



Il diritto digitale

Temi di informatica giuridica

a cura di

Monica Palmirani, Giovanni Sartor
Federico Galli, Salvatore Sapienza

Bologna
University Press

IL DIRITTO DIGITALE

Temi di informatica giuridica

a cura di
Monica Palmirani, Giovanni Sartor
Federico Galli, Salvatore Sapienza

Bologna
University Press

Title: LEGAL DESIGN AND DATA SCIENCE FOR EXPLICABLE AI IN LEGAL DOMAIN

Acronym: LEDS 4 XAIL

n. GPA: 101085576

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Education and Culture Executive Agency (EACEA). Neither the European Union nor the granting authority can be held responsible for them.



Co-funded by the
European Union



LEDS4XAIL

Fondazione Bologna University Press

Via Saragozza 10, 40123 Bologna

tel. (+39) 051 232 882

www.buonline.com

e-mail: info@buonline.com

Quest'opera è pubblicata sotto licenza Creative Commons CC BY-4.0

ISBN 979-12-5477-771-8

ISBN on line 979-12-5477-772-5

DOI 10.30682/9791254777725

Questo volume è stato realizzato a partire da un impaginato camera-ready in formato pdf fornito dai curatori

In copertina: Summit Art Creations/Shutterstock.com

Prima edizione: marzo 2026

INDICE

Introduzione	1
<i>Federico Galli, Monica Palmirani, Salvatore Sapienza, Giovanni Sartor</i>	

PARTE I – DATI

La protezione dei dati personali	11
<i>Federico Galli, Giovanni Sartor</i>	

Data Governance Act e Data Act nel quadro degli Spazi Comuni Europei dei Dati	37
<i>Salvatore Sapienza</i>	

L'uso secondario dei dati sanitari elettronici nella cornice dell'European Health Data Space	55
<i>Paola Aurucci</i>	

Open Government Data	75
<i>Monica Palmirani</i>	

Investigare i dati informatici: la <i>digital forensics</i> tra norme giuridiche, standard tecnici e innovazioni tecnologiche <i>Raffaella Brighi, Michele Ferrazzano</i>	97

PARTE II – STRUMENTI ABILITANTI

Identità e firme digitali <i>Chantal Bompreszi, Monica Palmirani</i>	121
Smart contract e blockchain <i>Chantal Bompreszi</i>	137

PARTE III – SISTEMI E PRODOTTI

La protezione dei beni informatici attraverso il diritto d'autore <i>Claudio Di Cocco</i>	161
La regolazione dell'Intelligenza Artificiale nell'UE: l'AI Act <i>Giuseppe Contissa, Marco Billi</i>	203
La decisione automatica e la sua spiegazione tra GDPR e AI Act <i>Francesca Lagioia, Giovanni Sartor</i>	221
Responsabilità e Intelligenza Artificiale <i>Chantal Bompreszi</i>	251

PARTE IV – MERCATI E SERVIZI

La regolazione dei mercati digitali: il Digital Markets Act <i>Federico Galli</i>	263
La regolazione degli intermediari di Internet: il Digital Service Act <i>Giuseppe Contissa</i>	287

La tutela del consumatore digitale <i>Federico Galli</i>	307

PARTE V – SICUREZZA

La Cybersicurezza nella trasformazione digitale <i>Raffaella Brighi</i>	341

Il diritto UE della Cybersicurezza: il quadro normativo <i>Pier Giorgio Chiara</i>	363

I reati informatici e la violazione dei diritti della persona in rete <i>Francesco Di Tano</i>	391

Il data breach e l'incidente di sicurezza <i>Juri Monducci</i>	409

PARTE VI – ETICA DEL DIGITALE

Etica dell'Intelligenza Artificiale <i>Giorgio Bongiovanni, Claudio Novelli</i>	435

Gli Autori	463

INTRODUZIONE

Il diritto digitale rappresenta oggi una delle aree più dinamiche dell'ordinamento giuridico. Esso è chiamato a confrontarsi con trasformazioni tecnologiche che ridefiniscono continuamente i confini tra pubblico e privato, tra libertà individuale e controllo sociale, tra innovazione e tutela dei diritti fondamentali. La pervasività delle tecnologie digitali nella vita quotidiana, l'onnipresenza dei dati come risorsa economica e strumento di potere, l'emergere di nuovi attori globali capaci di esercitare un'influenza senza precedenti sui mercati e sulla sfera pubblica, la diffusione di sistemi di Intelligenza Artificiale che automatizzano decisioni che, fino a meno di pochi anni fa, erano riservate esclusivamente al giudizio umano: tutti questi fenomeni richiedono risposte giuridiche adeguate, in grado di bilanciare esigenze spesso contrapposte e governare una realtà in continua evoluzione.

Per comprendere la natura e i contorni del diritto digitale, è necessario ripercorrere le tappe fondamentali che hanno segnato l'evoluzione di questa disciplina, delineando al contempo le aree che ne costituiscono oggi il nucleo fondante.

Il diritto digitale odierno affonda le proprie radici negli anni Settanta e Ottanta del Novecento, quando l'informatica cominciò a porsi come oggetto di attenzione per la scienza giuridica in modo specifico e autonomo rispetto ad altri metodi e saperi. In quel periodo, il fenomeno tecnologico dell'elaborazione automatica dei dati si presentava ancora come una realtà settoriale, confinata prevalentemente in ambito aziendale, amministrativo e scientifico.

Questa prima fase, che definiamo come "diritto dell'informatica", si caratterizzava per un approccio prevalentemente reattivo: il giurista – legislatore o interprete – interveniva per risolvere problemi specifici estendendo o reinterpretando categorie giuridiche tradizionali – quali la proprietà intellettuale, la responsabilità civile, la tutela della riservatezza o le fattispecie penali – a fenomeni nuovi, senza mettere in discussione l'architettura complessiva dell'ordinamento,

ma sforzandosi di applicare norme generali e astratte all'emergere di tecnologie informatiche.

In questo senso, una delle prime questioni affrontate ha riguardato la protezione giuridica del software. La natura ibrida del programma per elaboratore, opera dell'ingegno dotata al contempo di una funzione tecnica e di una dimensione espressiva, sollevava interrogativi sul regime giuridico applicabile. Il dibattito oscillava tra la brevettabilità e la tutela autorale: quest'ultima opzione ha prevalso nella maggior parte degli ordinamenti occidentali, anche sotto la spinta delle convenzioni internazionali e delle direttive europee, in particolare la Direttiva 91/250/CEE, poi sostituita dalla Direttiva 2009/24/CE.

Un'altra fondamentale linea di sviluppo ha riguardato l'emersione del "dato" informatico come bene giuridico, divenendo oggetto di studio soprattutto nell'ottica della tutela di una identità personale "datificata", senza tuttavia tralasciare la natura del dato quale risorsa economica, strumento di potere e, al contempo, potenziale minaccia per altri diritti fondamentali. La protezione dei dati personali, le cui origini risalgono agli anni Settanta, rappresenta storicamente il primo ambito in cui il dato ha assunto dignità giuridica autonoma.

Il progressivo riconoscimento dell'autodeterminazione informativa come diritto fondamentale autonomo rispetto al diritto alla vita privata ha costituito un passaggio cruciale: ogni individuo ha il diritto di decidere sulla raccolta, l'uso e la comunicazione dei propri dati personali. Questo approccio si è riflesso nella Direttiva 95/46/CE, che ha armonizzato la protezione dei dati personali nell'Unione europea introducendo principi quali la limitazione delle finalità del trattamento, la minimizzazione dei dati e la necessità del consenso o di altra base giuridica, e ha trovato piena consacrazione nel *General Data Protection Regulation* (GDPR, Regolamento Generale sulla Protezione dei Dati) del 2016.

In questa fase, e specialmente dopo l'approvazione della Carta dei diritti fondamentali del 2000, la giurisprudenza della Corte di Giustizia ha svolto un ruolo essenziale nel dare forma concreta ai principi della protezione dei dati personali, affermando con forza il primato dei diritti fondamentali attraverso sentenze come *Google Spain* (2014), che ha riconosciuto il diritto all'oblio nei confronti dei motori di ricerca, e *Schrems I e II* (2015, 2020), che hanno invalidato gli accordi sui trasferimenti internazionali di dati tra Unione europea e Stati Uniti.

Il GDPR ha ulteriormente rafforzato il diritto alla protezione dei dati personali, introducendo un diritto all'oblio generalizzato e alla portabilità dei dati. Il regolamento ha altresì imposto il principio di *accountability*, secondo cui i soggetti che determinano mezzi e modalità del trattamento dei dati – ossia i titolari del trattamento, come le imprese o le pubbliche amministrazioni – devono dimo-

strare attivamente la conformità e prevenire eventuali violazioni dei meccanismi di tutela dei dati personali. Sul piano della *governance*, il GDPR ha istituito meccanismi di cooperazione tra le autorità nazionali per garantire un'applicazione uniforme nell'Unione.

Accanto alla tutela dei dati personali, già negli anni Novanta emerse la necessità di tutelare le prerogative proprietarie sulle raccolte di dati. L'Unione europea ha riconosciuto il valore economico degli investimenti nelle banche dati con la Direttiva 96/9/CE, che ha introdotto un sistema a doppio binario: tutela autorale per le banche dati originali e un diritto *sui generis* che protegge gli investimenti sostanziali nella costituzione, verifica o presentazione di banche dati, anche non originali. Questo diritto esclusivo consente al costituente di impedire l'estrazione o il reimpiego non autorizzato della totalità o di parti sostanziali del contenuto.

Progressivamente, e sempre più negli ultimi anni, si è sentita l'esigenza, diametralmente opposta rispetto alla protezione dei dati personali, di favorire la circolazione e il riuso dei dati, anche e soprattutto non personali. Il movimento degli *open data*, promosso per i dati detenuti dalle pubbliche amministrazioni, si fonda sull'idea che i dati raccolti con risorse pubbliche debbano essere accessibili in formati aperti per favorire la trasparenza dell'attività amministrativa e innovazione a partire dal patrimonio comune rappresentato dai dati pubblici. Questo percorso è stato inaugurato dalla Direttiva (UE) 2019/1024 ma, più di recente, il Data Governance Act del 2022 e il Data Act del 2023 hanno introdotto un quadro organico per favorire ulteriormente la circolazione dei dati oltre che la loro semplice diffusione. Il primo promuove la condivisione volontaria attraverso intermediari affidabili, il secondo disciplina l'accesso ai dati generati da dispositivi IoT introducendo diritti di portabilità e obblighi di condivisione tra imprese. Si delinea così una governance dei dati fondata su disponibilità, portabilità, interoperabilità e riuso, che ambisce a trasformare i dati in un bene comune strategico, superando la visione esclusivamente difensiva e creando spazi comuni europei dei dati in settori strategici quali sanità, agricoltura, energia e mobilità.

Insieme alla crescente valorizzazione del dato, la fine degli anni Novanta si è caratterizzata dalla diffusione di Internet, dalla liberalizzazione delle telecomunicazioni e dall'esplosione del commercio elettronico. L'Unione europea ha assunto un ruolo di primo piano nella costruzione di un diritto dell'informatica di stampo europeo, un *corpus* normativo trasversale che regola le comunicazioni

elettroniche, il commercio online, la firma digitale e la responsabilità degli intermediari.

La Direttiva sul commercio elettronico (2000/31/CE) ha introdotto principi fondamentali quali la libera prestazione dei servizi della società dell'informazione e il regime di responsabilità limitata per gli intermediari tecnici, bilanciamento che ha garantito per due decenni lo sviluppo della Rete e l'accesso ad essa da parte degli utenti.

Nell'ultimo periodo, è emerso un approccio più cauto: gli intermediari e le piattaforme online hanno raggiunto dimensioni economiche e capacità di influenza senza precedenti. Motori di ricerca, social network e piattaforme di e-commerce si sono imposti come attori protagonisti, la cui posizione di dominio deriva dalla natura stessa dei mercati digitali, caratterizzati da forti economie di scala e di rete, asimmetrie informative strutturali e tendenze alla concentrazione. Il controllo su grandi quantità di dati (*big data*) con le conseguenti capacità di estrarne profitto costituisce una fonte di potere economico e sociale senza precedenti, con asimmetrie che incidono non solo sulla concorrenza, ma anche sulla libertà di scelta individuale, sulla formazione dell'opinione pubblica e sull'esercizio dei diritti fondamentali.

L'Unione europea ha inizialmente risposto in modo piuttosto frammentato, utilizzando strumenti consolidati del diritto *antitrust*, della tutela dei consumatori e del diritto d'autore. Procedimenti antitrust contro Google e Amazon, la Direttiva Omnibus del 2019 e la Direttiva sul diritto d'autore nel mercato unico digitale hanno rappresentato primi tentativi di regolamentazione, rivelatisi però insufficienti.

Un approccio più organico si è consolidato con l'adozione del Digital Markets Act e del Digital Services Act (2022), due regolamenti che hanno ridefinito profondamente le regole del gioco.

Il Digital Markets Act ha introdotto obblighi *ex ante* per i cosiddetti "gatekeeper", ovvero coloro che controllano l'accesso ai mercati digitali, imponendo condizioni di equità contrattuale, interoperabilità, portabilità dei dati e divieto di pratiche di *self-preferencing*, con l'obiettivo di ripristinare condizioni di concorrenza effettiva nei mercati digitali.

Il Digital Services Act, invece, ha aggiornato e ampliato il regime di responsabilità degli intermediari, sostituendo le regole della Direttiva sul commercio elettronico del 2000, introducendo obblighi di diligenza sulla moderazione dei contenuti, differenziati a seconda delle dimensioni e del ruolo svolto, imponendo trasparenza algoritmica, meccanismi di reclamo, valutazioni del rischio sistemico e cooperazione con le autorità pubbliche.

Parallelamente, per garantire certezza alle interazioni tra soggetti digitali, il Regolamento eIDAS ha riconosciuto validità giuridica alle firme elettroniche e ai documenti informatici, ricostruendo la fiducia nel contesto digitale attraverso meccanismi crittografici e infrastrutture di autenticazione. Questo modello, fondato su autorità centralizzate di certificazione, si è successivamente confrontato con l'emergere di tecnologie distribuite quali la *blockchain*, che propongono paradigmi alternativi di *trust* basati su consenso distribuito e immutabilità crittografica, sollevando nuove questioni giuridiche relative al valore probatorio delle transazioni registrate su registri distribuiti, alla qualificazione giuridica degli *smart contract* e alla compatibilità tra principi di protezione dei dati (quali il diritto alla cancellazione) e caratteristiche tecniche di immutabilità della *blockchain*.

La frontiera più recente del diritto digitale è rappresentata dall'automazione dei processi decisionali, resa possibile dai progressi nell'intelligenza artificiale e nel *machine learning*. Sistemi di IA vengono impiegati in ambiti sempre più delicati, dalla diagnosi medica all'individuazione di sospetti in indagini penali, dalla gestione dei lavoratori all'accesso a servizi essenziali, sollevando interrogativi profondi sulla trasparenza, sulla spiegabilità e sulle responsabilità connesse all'utilizzo di tali sistemi. La decisione automatizzata si caratterizza spesso per la sua opacità intrinseca: molti sistemi algoritmici funzionano come *black box*, entrando in tensione con principi giuridici fondamentali quali il diritto al contraddittorio, il diritto di difesa e il principio di non discriminazione.

Il GDPR aveva già riconosciuto all'articolo 22 il diritto di non essere sottoposti a decisioni basate unicamente su trattamenti automatizzati, introducendo al contempo un diritto alla spiegazione, la cui portata effettiva è stata a lungo oggetto di dibattito. Il Regolamento sull'Intelligenza artificiale (AI Act), adottato nel 2024, ha ulteriormente sviluppato questo quadro, introducendo requisiti di trasparenza, robustezza, sicurezza e sorveglianza umana per i sistemi ad alto rischio.

In questo ambito, il diritto viene a configurarsi sempre più come architettura del rischio tecnologico: l'approccio *risk-based regulation* è al cuore dell'AI Act, che classifica i sistemi in base al livello di rischio e applica regimi normativi differenziati. Le pratiche a rischio inaccettabile sono vietate, mentre i sistemi ad alto rischio sono sottoposti a requisiti stringenti e quelli a rischio limitato o minimo hanno obblighi meno stringenti. Il controllo umano costituisce un principio cardine posto a garanzia che il potere ultimo di decisione rimanga nelle mani delle persone.

La regolazione *ex ante* dell'IA non ha eliminato le questioni riguardanti la responsabilità giuridica per danni causati da sistemi automatizzati. Nel 2022 l'Unione europea ha proposto due direttive rilevanti: la prima, una revisione

della Direttiva sulla responsabilità per danno da prodotti difettosi, è stata approvata nel 2024 (Direttiva (UE) 2024/2853) estendendo il regime di responsabilità oggettiva ai software e ai sistemi di IA; la seconda, sulla responsabilità civile per l'IA, si proponeva di introdurre ulteriori presunzioni di causalità e nesso di colpa, creando un regime complementare a quello della responsabilità da prodotto. Tale direttiva, tuttavia, è stata ritirata dopo l'adozione dell'AI Act.

La gestione del rischio riguarda anche e sempre più un'altra area cruciale del diritto digitale contemporaneo: la protezione delle infrastrutture e dei sistemi digitali. La sicurezza informatica è progressivamente emersa come prerequisito essenziale per l'esercizio dei diritti fondamentali e per il funzionamento dell'economia e dei rapporti sociali.

I primi fenomeni di criminalità informatica rendevano evidente l'inadeguatezza di alcune categorie penali tradizionali, spingendo gli ordinamenti nazionali a introdurre fattispecie penali *ad hoc* e avviando tentativi di coordinamento internazionale culminati nella Convenzione di Budapest del 2001. Nel frattempo, nel campo dell'informatica del diritto, la *digital forensics* cominciava a configurarsi come area di indagine autonoma, affrontando le delicate questioni di autenticità, integrità e ammissibilità processuale delle prove informatiche.

Ma è negli ultimi anni che l'Unione europea, nel settore della cybersicurezza, ha progressivamente costruito un quadro normativo organico: la Direttiva NIS (*Network and Information Security*) del 2016, poi sostituita dalla Direttiva NIS2 del 2022, ha introdotto obblighi di sicurezza per gli operatori di servizi essenziali e per i fornitori di servizi digitali; il Cybersecurity Act del 2019 ha istituito un quadro europeo di certificazione; il Cyber Resilience Act del 2024 estende gli obblighi di sicurezza ai prodotti con elementi digitali. La sicurezza e la resilienza diventano così concetti complementari: mentre la sicurezza mira a prevenire incidenti, la resilienza si riferisce alla capacità di resistere, assorbire, adattarsi e riprendersi da eventi avversi. La resilienza richiede un approccio olistico che integri aspetti tecnici, organizzativi, procedurali e umani, con cooperazione tra settore pubblico e privato e coordinamento tra Stati membri.

Accanto alle dimensioni giuridiche e tecniche, emerge con forza anche la dimensione etica del digitale. L'innovazione tecnologica pone interrogativi etici che richiedono una riflessione più ampia sui valori, sui fini e sulle conseguenze sociali delle scelte tecnologiche. L'Unione europea ha promosso un approccio *human-centric* all'intelligenza artificiale, fondato sul rispetto dei diritti fondamentali, della democrazia e dello stato di diritto.

L'etica del digitale risponde a precise ragioni teoriche e pratiche: essa svolge molteplici funzioni nell'ecosistema normativo. In primo luogo, può contribuire a dare contenuto alle leggi: i principi etici costituiscono spesso il fondamento e la giustificazione delle scelte normative. In secondo luogo, l'etica può condurre alla modifica di una legge: le trasformazioni tecnologiche sollevano nuove questioni morali che spingono verso revisioni normative. In terzo luogo, fornisce un modello interpretativo della legge: di fronte a disposizioni ambigue, i principi etici forniscono criteri interpretativi. Infine, può richiedere più di quanto necessario giuridicamente e imporre meno di quanto consentito: l'etica opera come standard di comportamento che va oltre il diritto positivo, particolarmente importante in contesti di rapida evoluzione tecnologica dove la *soft law*, i codici di condotta volontari e le *best practices* svolgono un ruolo cruciale.

Il percorso delineato testimonia una trasformazione profonda, non solo dell'oggetto della regolazione, ma della stessa natura del diritto. Il diritto digitale non è una branca settoriale, ma un diritto trasversale e sistemico che attraversa tutte le tradizionali partizioni disciplinari. Il passaggio da un "diritto dell'informatica" al "diritto digitale" segna un cambiamento di prospettiva: mentre il primo si concentrava sugli strumenti tecnologici forieri di problematiche giuridiche, il secondo assume le tecnologie digitali come dimensione costitutiva della realtà contemporanea e del fenomeno giuridico. Il suo scopo non è soltanto quello di *regolare* l'uso di computer e reti, ma di *governare* ecosistemi complessi in cui tecnologie, dati, algoritmi, piattaforme, individui e istituzioni interagiscono dinamicamente.

I contorni del diritto digitale sono tracciati da atti normativi che spesso condividono definizioni, attori e processi comuni, e sono accomunati da tecniche regolatorie ricorrenti, squisitamente preventive: trasparenza, regolazione *by design*, *accountability*, valutazione di impatto, certificazione e standardizzazione. La regolazione *by design*, in particolare, costituisce l'elemento più evidente che contraddistingue il diritto digitale: mentre il diritto tradizionale interviene prevalentemente *ex post*, la regolazione *by design* ambisce a prevenire i problemi incorporando vincoli normativi nella struttura stessa della tecnologia e dei suoi ecosistemi. Questo approccio richiede una stretta collaborazione tra giuristi e informatici, e mette in evidenza il legame inscindibile tra diritto digitale e informatica giuridica, che diviene dunque componente essenziale della stessa produzione normativa.

Un altro elemento costitutivo del diritto digitale è la centralità dell'Unione europea. L'adozione del GDPR nel 2016 ha segnato l'abbandono del modello della direttiva a favore del regolamento, strumento direttamente applicabile senza necessità di recepimento. L'UE, forse in virtù della limitata competitività

dell'industria del digitale rispetto a Stati Uniti e Cina, ha fatto della regolazione la propria leva strategica, costruendo un modello di *governance* digitale fondato sulla promozione dell'innovazione e sul rispetto dei valori e dei diritti fondamentali. Questo modello ha una dimensione interna, finalizzata alla costruzione di uno spazio giuridico comune, e una dimensione esterna, spesso definita come “sovranità digitale europea”, che sfrutta il cosiddetto “effetto Bruxelles”: le imprese globali, per accedere al mercato europeo, devono conformarsi alle norme europee, che tendono a divenire *de facto* standard globali. GDPR, DMA, DSA e AI Act rappresentano tappe di questa strategia i cui risultati restano tuttavia ancora incerti.

L'importanza dell'Unione europea non riduce la rilevanza della dimensione nazionale. Le specificità di implementazione e le questioni non armonizzate chiamano costantemente in causa gli ordinamenti degli Stati membri. La *governance* del digitale è multilivello, articolata su una pluralità di attori istituzionali che operano a livello europeo, nazionale e locale. Numerosi atti accompagnano e integrano la legislazione europea: si pensi alla legge italiana sull'intelligenza artificiale del 2025. Le autorità nazionali di protezione dei dati, le autorità di settore, le corti nazionali e la Corte di Giustizia costituiscono una rete complessa che coopera, si coordina e talvolta entra in tensione, dando vita a un sistema di *checks and balances* caratteristico del costituzionalismo europeo nell'era digitale.

Il presente manuale offre una panoramica aggiornata delle principali aree del diritto digitale. La struttura riflette la complessità di una materia che ha raggiunto una propria sistematicità. La *Parte I* è dedicata ai dati, la *Parte II* agli strumenti abilitanti, la *Parte III* ai sistemi e prodotti, la *Parte IV* ai mercati e servizi digitali, la *Parte V* alla sicurezza, la *Parte VI* alla dimensione etica. Questa articolazione riflette una scelta metodologica precisa: non isolare i singoli ambiti, ma evidenziarne le interconnessioni.

Il manuale adotta una metodologia pienamente interdisciplinare tesa ad integrare aspetti informatici e giuridici alla luce della filosofia del diritto e delle tecnologie.

Ringraziamo tutti gli Autori per il contributo alla realizzazione del volume, per la qualità scientifica dei testi e per la collaborazione nei lavori.

Un grazie speciale va al Prof. Giorgio Bongiovanni che ha contribuito in modo determinante all'avanzamento del progetto seguendone lo sviluppo e offrendo indicazioni preziose per la definizione e il consolidamento dell'impianto dell'opera.

F. Galli, M. Palmirani, S. Sapienza, G. Sartor

PARTE I – DATI

LA PROTEZIONE DEI DATI PERSONALI*

Federico Galli, Giovanni Sartor

SOMMARIO: 1. Privacy e protezione dei dati: origine e sviluppi. 2. Il Regolamento generale sulla protezione dei dati. 2.1. L'ambito di applicazione materiale. 2.2. L'ambito di applicazione territoriale. 3. La definizione di "dato personale". 3.1. Pseudonimizzazione e anonimizzazione. 4. Principi generali sul trattamento. 5. Le condizioni di liceità del trattamento. 5.1. Categorie particolari di dati (dati sensibili). 5.2. Il consenso dell'interessato. 5.3. Il legittimo interesse. 6. I diritti dell'interessato. 6.1. Il diritto alla cancellazione (diritto all'oblio). 7. Gli obblighi del titolare del trattamento. 7.1. Il titolare e il responsabile del trattamento. 7.2. Gli obblighi del titolare del trattamento. 7.3. *Data protection by design* e *by default*. 7.4. Valutazione di impatto sulla protezione dei dati e il *Data Protection Officer*. 8. Il Garante per la protezione dei dati personali. 9. La tutela giurisdizionale. 10. L'applicazione del GDPR nel contesto europeo (cenni).

1. Privacy e protezione dei dati: origine e sviluppi

La protezione dei dati ha origini dalla confluenza di diverse esigenze di protezione giuridica.

Una prima esigenza attiene alla protezione rispetto alla diffusione non autorizzata di informazioni sulla vita privata dei singoli (che include non solo i comportamenti che l'individuo tiene nel proprio domicilio, al di fuori dello sguardo altrui, ma anche quelli che non rilevano per ruoli o funzioni di interesse pubblico). Era questo il tema affrontato nel famoso saggio che aprì il dibattito statunitense sul "diritto alla privacy" alla fine del XIX secolo¹.

La stessa esigenza di tutela è stata affermata dalla nostra Corte di Cassazione nella sentenza n. 2129 del 27 maggio 1975, che riguardava la pubblicazione, da parte di un settimanale, di fotografie e dettagli sulla vita privata della principessa Soraya, ex moglie dello Scià di Persia. Nel sanzionare tale comportamento, la Corte riconosceva l'esistenza di un autonomo diritto alla riservatezza, qualificandolo come un diritto della personalità tutelato dall'ordinamento, ricollegandolo agli articoli 2 e 3 della Costituzione.

Una seconda esigenza di tutela attiene alla garanzia della libertà dell'individuo nella propria vita privata, quale sfera sottratta alle intrusioni dello Stato,

* Il presente contributo è un risultato del progetto ERC-Advanced "CompuLaw" (Grant Agreement No 833647).

¹ S. WARREN, L. BRENDIS, *The Right to Privacy*, in *Harvard L. Rev.*, 1890, pp. 193-220.

un'esigenza fortemente sentita in Europa dopo l'esperienza dei regimi totalitari (caratterizzati dalla tendenziale negazione di ogni dimensione privata). Questa esigenza è alla base del diritto alla protezione della vita privata, affermato nell'articolo 12 della Dichiarazione Universale dei Diritti Umani:

Nessun individuo potrà essere sottoposto ad interferenze arbitrarie nella sua vita privata, nella sua famiglia, nella sua casa, nella sua corrispondenza, né a lesione del suo onore e della sua reputazione. Ogni individuo ha diritto ad essere tutelato dalla legge, contro tali interferenze o lesioni.

La Convenzione europea dei diritti dell'uomo (1950) ha seguito l'esempio, nell'articolo 8 della Convenzione che recita:

1. Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza. 2. Non vi sarà alcuna ingerenza da parte di un'autorità pubblica nell'esercizio di tale diritto, salvo quella prevista dalla legge e necessaria in una società democratica nell'interesse della sicurezza nazionale, della pubblica sicurezza o del benessere economico del Paese, per la prevenzione di disordini o crimini, per la protezione della salute o della morale, o per la protezione dei diritti e delle libertà altrui.

Il diritto alla protezione della vita privata comprende due aspetti. Da un lato vi è la così detta "privacy decisionale", cioè la libertà dell'individuo nelle scelte che riguardano la sua sfera intima (per esempio, la dimensione sessuale, affettiva o familiare). Dall'altro lato, vi è la così detta "privacy informazionale", che riguarda invece il diritto a limitare l'accesso alle informazioni che riguardano quella stessa sfera. Questo secondo aspetto è specificamente rilevante ai nostri fini.

Una terza esigenza di tutela emersa più recentemente attiene invece alla protezione dell'individuo dai rischi che derivano dalla raccolta ed elaborazione sistematica dei dati che lo riguardano, in particolare mediante sistemi informatici. Tale esigenza di protezione ha un ambito più esteso rispetto a quello della "privacy informazionale" quale aspetto della tutela della vita privata: riguarda ogni tipo di dato personale, anche al di là degli aspetti "privati" (pensiamo ad esempio, alle informazioni raccolte dai datori di lavoro sui dipendenti, dallo stato sui cittadini a fini fiscali o previdenziali, dalle imprese per l'invio di pubblicità mirata, ecc.).

Nel costruire una disciplina giuridica che risponda a questa così ampia esigenza di protezione bisogna però considerare che vi sono interessi importanti – pubblici e privati – che possono giustificare la raccolta e l'elaborazione dei dati personali. Si pensi a come dati sugli individui siano necessari per la gestione del

personale nelle imprese, per l'erogazione dei servizi da parte degli enti pubblici, per l'erogazione del credito da parte delle banche, per la fornitura di prestazioni sanitarie da parte di strutture pubbliche e private, per pagamenti e consegne nel commercio elettronico, ecc. Per rispondere a tali esigenze è necessario consentire la raccolta e l'elaborazione dei dati personali per scopi legittimi, regolando però tale elaborazione in modo da minimizzare i rischi che ne derivino per gli individui interessati.

Affrontare quei rischi è oggi necessario poiché tecnologie sempre più potenti consentono di sorvegliare le persone e di tracciarne la vita in ogni aspetto (gli spostamenti, gli acquisti, le interazioni sociali, le condizioni di salute, ecc.). I dati raccolti possono essere poi elaborati per inferire caratteristiche, attitudini, interessi e vulnerabilità degli interessati, e quindi per adottare decisioni (possibilmente ingiuste o discriminatorie) che li riguardano, o per cercare di influenzarne il comportamento nella sfera economica o anche in quella politica. In questo contesto non solo la riservatezza o la vita privata, ma le libertà civili e politiche (libertà di espressione, di associazione, di informazione, diritto al lavoro, ecc.) sono minacciate e lo stesso assetto democratico della società è in discussione.

Per affrontare questi rischi si è sviluppata la disciplina della “protezione dei dati”, che, ricoprendo ogni elaborazione sistematica di dati personali (non solo di quelli che attengono alla dimensione intima o privata), si affianca e sovrappone alla tutela della riservatezza e alla tutela della vita privata. Lo scopo di tale disciplina non è la protezione dei dati stessi ma piuttosto la protezione degli individui dai rischi che derivano dal trattamento dei loro dati personali, protezione che richiede una regolazione dei processi mediante i quali i dati sono raccolti ed elaborati.

Il diritto alla protezione dei dati si configura quindi come il diritto dell'interessato a controllare il trattamento dei propri dati, e più in generale, ad essere protetto dai rischi che derivano dall'elaborazione di quei dati. La protezione si attua mediante diritti garantiti all'interessato (es., all'informazione, l'accesso, e la rettifica), mediante obblighi imposti a chi effettua i trattamenti e grazie alla supervisione da parte di autorità indipendenti.

Tale diritto è infatti così caratterizzato dall'articolo 8 della Carta dei Diritti Fondamentali dell'Unione europea.

1. Ogni persona ha diritto alla protezione dei dati personali che la riguardano.
2. Tali dati devono essere trattati lealmente per finalità specifiche e sulla base del consenso dell'interessato o di un'altra base legittima prevista dalla legge. Ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica.

3. Il rispetto di queste regole è soggetto al controllo di un'autorità indipendente.

Nell'Unione Europea la protezione dei dati è oggi disciplinata dal Regolamento 679/2016 sulla protezione dei dati, cui si fa spesso riferimento con l'acronimo GDPR (*General Data Protection Regulation*).

Tale regolamento ha abrogato la precedente disciplina rappresentata dalla direttiva 95/46 che costituiva il principale riferimento europeo in materia di tutela dei dati personali, fissando principi comuni per tutti gli Stati membri tesi ad armonizzare le legislazioni nazionali in materia.

In Italia tale direttiva era stata trasposta con la legge 31 dicembre 1996, n. 675 (la prima disciplina organica della protezione dei dati nel nostro Paese), poi riorganizzata all'interno del Codice in materia di protezione dei dati personali, detto anche Codice privacy (d.lgs. 30 giugno 2003, n. 196).

Dopo l'entrata in vigore del Regolamento, il Codice privacy non è stato abrogato (sebbene molte delle sue disposizioni siano state superate dalla nuova normativa europea), ma è stato pesantemente modificato dal d.lgs. 10 agosto 2018, n. 101. Tale decreto ha abrogato le disposizioni incompatibili con il GDPR e ha introdotto norme integrative per le materie lasciate alla competenza degli Stati membri, come il trattamento dei dati in ambito giudiziario, la protezione dei dati dei minori e le sanzioni amministrative.

Il Codice privacy è stato successivamente ulteriormente modificato. Si ricorda in particolare il d.l. 8 ottobre 2021, n. 139 (cosiddetto "decreto Capienze"), che ha inciso in modo significativo su vari articoli del Codice, ridefinendo, tra l'altro, il ruolo delle basi giuridiche per i trattamenti effettuati da soggetti pubblici, chiarendo l'ambito applicativo dell'art. 2-ter e introducendo modifiche anche in materia di trattamento per finalità di interesse pubblico, semplificazioni procedurali e coordinamento con il GDPR.

2. Il Regolamento Generale sulla Protezione dei Dati

Il Regolamento UE 2016/679 è stato adottato nel 2016 ed è entrato in vigore il 25 maggio 2018². Il GDPR è stato concepito per uniformare le leggi sulla protezione dei dati in tutta Europa, per proteggere e potenziare la privacy dei

² Si ricorda che il GDPR è stato proposto nel cosiddetto Pacchetto Protezione Dati accanto alla così detta Direttiva Polizia, relativa alla protezione dei dati nel corso delle indagini di polizia e dell'applicazione del diritto penale (Direttiva (UE) 2016/680), che protegge i dati personali nelle forze dell'ordine, e al Regolamento sulla libera circolazione dei dati non personali (Regolamento (UE) 2018/1807). Inoltre, il pacchetto ha proposto il regolamento sulla privacy elettronica, che si sarebbe concentrato sulla riservatezza delle comunicazioni elettroniche e avrebbe sostituito la direttiva sulla privacy elettronica del 2002, che tuttavia non è mai stato approvato.

dati di tutti i cittadini dell'UE e per rimodellare il modo in cui le organizzazioni affrontano la privacy dei dati.

In particolare, l'oggetto è così specificato nell'articolo 1:

1. Il presente regolamento stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali e norme relative alla libera circolazione dei dati personali.
2. Il presente regolamento tutela i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali.
3. La libera circolazione dei dati personali all'interno dell'Unione non è limitata né vietata per motivi connessi alla protezione delle persone fisiche con riguardo al trattamento dei dati personali.

2.1. L'ambito di applicazione materiale

L'ambito di applicazione materiale del GDPR è definito dall'articolo 2 del Regolamento e determina i casi in cui le norme sulla protezione dei dati personali si applicano o meno.

In linea generale, il GDPR si applica al trattamento dei dati personali che riguardano persone fisiche identificate o identificabili, effettuato, totalmente o parzialmente, con mezzi automatizzati, nonché al trattamento non automatizzato di dati contenuti in un archivio o destinati a figurarvi.

Ciò significa che il Regolamento copre una vasta gamma di attività, che spaziano dalla gestione di banche dati digitali alle raccolte cartacee strutturate di informazioni personali, purché destinate a essere organizzate o consultate sistematicamente. L'elemento determinante, come vedremo sotto, è dunque l'identificabilità della persona fisica, diretta o indiretta, attraverso elementi come nome, numero di identificazione, dati relativi all'ubicazione, identificatori online o altri fattori specifici relativi all'identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale dell'interessato.

L'articolo 2, paragrafo 2, elenca in modo espresso alcune esclusioni dall'ambito di applicazione, tra cui i trattamenti effettuati: a) nell'esercizio di attività non rientranti nell'ambito di applicazione del diritto dell'Unione; b) dagli Stati membri quando esercitano attività rientranti nell'ambito della politica estera e di sicurezza comune; c) da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico; d) dalle autorità competenti per finalità di prevenzione, indagine, accertamento o perseguimento di reati o per l'esecuzione di sanzioni penali, disciplinate dalla Direttiva (UE) 2016/680.

2.2. L'ambito di applicazione territoriale

L'articolo 3 del GDPR definisce l'ambito di applicazione territoriale del Regolamento, stabilendo che esso riguarda le attività di trattamento dei dati personali effettuate da titolari o responsabili stabiliti nell'Unione europea, indipendentemente dal luogo in cui il trattamento viene materialmente svolto³. La nozione di "stabilimento" è interpretata in senso funzionale e sostanziale, secondo la giurisprudenza della Corte di giustizia, e richiede la presenza di un'attività reale ed effettiva, anche se minima, esercitata tramite un'organizzazione stabile.

Il GDPR si applica inoltre ai trattamenti effettuati da soggetti non stabiliti nell'UE quando tali trattamenti riguardano l'offerta di beni o servizi a interessati che si trovano nell'Unione, oppure il monitoraggio del loro comportamento, nella misura in cui tale comportamento avvenga all'interno del territorio dell'Unione. Questa clausola, introdotta dall'articolo 3, paragrafo 2, ha un ruolo centrale nel contrastare fenomeni di delocalizzazione opportunistica dei trattamenti (al fine di godere di una disciplina meno rigorosa): non è dunque determinante la sede giuridica del titolare, ma l'effettiva incidenza delle sue attività sugli interessati nell'UE.

L'estensione extraterritoriale del GDPR ha ampliato in modo significativo il numero di soggetti obbligati a conformarsi alla disciplina europea. Una società con sede negli Stati Uniti o in un Paese terzo che offra servizi a utenti europei, oppure che tracci il loro comportamento mediante cookie, identificatori online o altre tecniche di profilazione, è tenuta a rispettare il GDPR e a designare un rappresentante nell'Unione, salvo eccezioni. In questo modo si assicura che i diritti degli interessati nell'UE siano tutelati anche quando il trattamento è effettuato da entità situate al di fuori del territorio europeo.

Questa portata extraterritoriale ha contribuito a ciò che è stato definito "effetto Bruxelles"⁴. Il GDPR, attraverso i suoi standard elevati e la sua capacità di incidere sulle pratiche di attori globali, ha influenzato normative e politiche aziendali in tutto il mondo. Molte imprese multinazionali hanno scelto di adottare modelli di conformità uniformi a livello globale, estendendo le tutele del GDPR a tutti i loro utenti, non solo a quelli residenti nell'UE.

³ Articolo 3, paragrafo 1 del GDPR.

⁴ A. BRADFORD, *The Brussels Effect: How the European Union Rules the World*, Oxford: Oxford University Press, 2020.

3. La definizione di “dato personale”

Ai sensi dell'articolo 4, paragrafo 1, del GDPR, per dati personali si intende qualsiasi informazione relativa a una persona fisica identificata o identificabile, cioè del “soggetto interessato” (in inglese *data subject*). Tali informazioni includono identificatori come il nome, il numero di identificazione, i dati relativi all'ubicazione e gli identificatori online⁵, nonché fattori specifici dell'identità fisica, fisiologica, genetica, mentale, economica, culturale o sociale.

Entro la categoria generale di dato personale, il GDPR distingue una sottocategoria di informazioni che, per la loro natura, richiedono una tutela rafforzata: le categorie particolari di dati personali, comunemente dette dati sensibili. Sono quei dati che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché il trattamento di dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale e all'orientamento sessuale della persona.

Come vedremo sotto, il trattamento di tali dati è vietato in linea di principio (dunque viene invertita la regola generale rispetto al trattamento dei dati comuni, consentito qualora vi sia una base giuridica), salvo che ricorra una delle eccezioni tassativamente previste dallo stesso articolo 9, paragrafo 2.

Tornando alla definizione generale di dato personale, la questione interpretativa più delicata della definizione di dato personale è la misura in cui le informazioni possono essere considerate relative a una “persona fisica identificabile”.

Il GDPR stabilisce che per valutare se una persona è identificabile, si devono considerare tutti i mezzi ragionevolmente utilizzabili, come l'individuazione, da parte del responsabile del trattamento o di un'altra persona. Ciò include la considerazione di fattori quali il costo e la quantità di tempo necessari per l'identificazione, considerando la tecnologia disponibile al momento del trattamento e qualsiasi progresso tecnologico futuro⁶.

⁵ Si ricorda, in questo caso, la sentenza *Breyer* (C-582/14, 19 ottobre 2016), con la quale la Corte di giustizia dell'Unione europea ha stabilito che un indirizzo IP dinamico può costituire un dato personale qualora il titolare del trattamento disponga di mezzi legittimi e ragionevoli per identificare l'interessato mediante informazioni aggiuntive detenute da terzi, come il fornitore di accesso a Internet. La Corte ha chiarito che, per valutare l'identificabilità di una persona, occorre considerare non solo i mezzi effettivamente a disposizione del titolare, ma anche quelli che potrebbero essere utilizzati da altri soggetti, purché l'identificazione non richieda sforzi sproporzionati. Tale pronuncia conferma un'interpretazione ampia e funzionale del concetto di “dato personale”, coerente con il considerando 26 del GDPR, e rafforza l'approccio contestuale fondato sul rischio di re-identificazione.

⁶ Considerando 26.

Questo aspetto è particolarmente problematico se si considerano le numerose tecnologie che consentono la re-identificazione dei dati. Tecniche come il *data mining*, l'apprendimento automatico e l'analisi dei big data possono incrociare i set di dati anonimizzati con altre fonti di dati, rivelando potenzialmente le identità personali. Anche informazioni apparentemente innocue, se combinate con altri dati, possono portare all'identificazione di individui.

Tale sviluppo ha portato alcuni autori a ritenere che oggi il diritto alla protezione dei dati rischia di diventare un «diritto sull'informazione in quanto tale»⁷, cioè che potrebbe estendersi ipoteticamente a qualsiasi informazione che, anche solo potenzialmente, possa contribuire all'identificazione di un individuo, diretta o indiretta. Tale sviluppo, se da un lato estende l'ambito delle garanzie, rischia di sminuire la specificità e la funzione originaria del diritto alla protezione dei dati, trasformandolo in una clausola generale di controllo su qualsiasi flusso informativo.

3.1. Pseudonimizzazione e anonimizzazione

Per comprendere appieno la nozione di dato personale e dunque i confini di applicazione del Regolamento, occorre introdurre anche la distinzione tra pseudonimizzazione e anonimizzazione

La pseudonimizzazione è definita all'articolo 4, paragrafo 5, del GDPR come «il trattamento dei dati personali in modo tale che i dati non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, purché tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative atte a garantire che non siano attribuite a una persona fisica identificata o identificabile».

In altri termini, la pseudonimizzazione è una tecnica di sicurezza che riduce il rischio di identificazione, ma non elimina il carattere personale del dato: i dati pseudonimizzati restano infatti «dati personali», in quanto l'identità dell'interessato può essere ricostruita tramite informazioni ausiliarie in possesso del titolare o di terzi. Ciò è stato ribadito dal Considerando 26 del GDPR, secondo cui «i dati personali che sono stati sottoposti a pseudonimizzazione, e che potrebbero essere attribuiti a una persona fisica mediante l'utilizzo di informazioni supplementari, devono essere considerati informazioni su una persona fisica identificabile».

La qualificazione dei dati pseudonimizzati come dati personali implica che essi restano soggetti a tutte le disposizioni del Regolamento, inclusi i principi di

⁷ N. PURTOVA, *The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law*, in *Law, Innovation and Technology*, 2018 (1), pp. 40-81.

liceità, minimizzazione, limitazione della conservazione e sicurezza del trattamento. Tuttavia, la pseudonimizzazione rappresenta una misura di garanzia significativa, in quanto riduce i rischi per gli interessati e può essere considerata un mezzo di conformità ai sensi dell'articolo 25 (protezione dei dati fin dalla progettazione e per impostazione predefinita) e dell'articolo 32 (sicurezza del trattamento).

La giurisprudenza ha confermato questo approccio in più occasioni. In particolare, nella sentenza “Deloitte” del 26 ottobre 2023 (Causa C-319/22), la Corte di giustizia dell'Unione europea (CGUE) ha chiarito che i dati pseudonimizzati restano dati personali anche se il destinatario del trattamento non dispone direttamente delle chiavi di ricodifica, qualora il titolare originario o un altro soggetto abbia i mezzi per risalire all'identità della persona. Secondo la Corte, la valutazione dell'identificabilità deve essere effettuata tenendo conto non solo dei mezzi del soggetto che detiene i dati, ma anche di quelli potenzialmente accessibili ad altri soggetti che collaborano o possono accedere alle informazioni aggiuntive. La decisione Deloitte ha così ristretto l'ambito del “dato personale” escludendone i dati pseudonimizzati qualora trasmessi ad un terzo che non ha la capacità di procedere alla reidentificazione dei soggetti interessati.

L'anonimizzazione, invece, si distingue dalla pseudonimizzazione per il fatto che comporta un trattamento irreversibile, attraverso il quale le informazioni non possono più essere ricondotte, neppure indirettamente o tramite tecniche avanzate, a una persona fisica identificata o identificabile. I dati anonimizzati non rientrano più nell'ambito di applicazione del GDPR, poiché perdono la loro natura di dato personale. Tuttavia, l'anonimizzazione completa è difficile da garantire nella pratica, specialmente, come detto, alla luce delle tecniche moderne di re-identificazione e dell'integrazione di dataset eterogenei.

Un aspetto particolarmente controverso nel dibattito contemporaneo riguarda i dati sintetici, ossia dati generati artificialmente mediante algoritmi (spesso di intelligenza artificiale) che riproducono le caratteristiche statistiche dei dati reali senza corrispondere a persone effettive. La questione centrale è se tali dati possano essere considerati “anonimi” o se, a causa del loro processo di generazione basato su dati personali, possano comunque implicare un rischio di re-identificazione indiretta. L'assenza di una posizione univoca da parte del legislatore o delle autorità di controllo europee rende l'inquadramento dei dati sintetici ancora oggetto di dibattito dottrinale e giurisprudenziale: mentre alcuni ritengono che essi debbano essere esclusi dal campo di applicazione del GDPR, altri sostengono che, se la generazione sintetica consente la ricostruzione o inferenza di dati riferibili a individui reali, tali dati dovrebbero continuare a essere trattati come dati personali.

4. Principi generali sul trattamento

L'articolo 5 del GDPR delinea i principi per il trattamento dei dati personali:

- Liceità, correttezza e trasparenza: i dati devono essere trattati in modo legale, corretto e trasparente, garantendo la conformità alle regole del GDPR, equità nel trattamento e chiara comunicazione sull'uso dei dati agli interessati.
- Limitazione delle finalità: i dati personali devono essere raccolti per finalità determinate, esplicite e legittime e non devono essere ulteriormente trattati in modo incompatibile con tali finalità.
- Minimizzazione dei dati: devono essere trattati solo i dati adeguati, pertinenti e limitati a quanto necessario per le finalità previste.
- Esattezza: i dati personali devono essere esatti e aggiornati; devono essere adottate misure per correggere o eliminare informazioni inesatte.
- Limitazione della conservazione: i dati personali non devono essere conservati più a lungo del necessario per le finalità per cui sono trattati.
- Integrità e riservatezza: i dati personali devono essere trattati in modo sicuro, proteggendoli da trattamenti non autorizzati o illeciti, perdita accidentale, distruzione o danni.

Tutti i principi elencati all'articolo 5 costituiscono le fondamenta del regime di protezione dei dati personali, poiché vi delineano i criteri ai quali ogni trattamento deve conformarsi perché sia una lecita e proporzionata interferenza con il diritto fondamentale alla protezione dei dati personali. Essi non sono meri obblighi formali, ma regole di condotta sostanziali che orientano l'intero ciclo di vita del dato personale, dalla raccolta, all'utilizzo, fino alla conservazione e cancellazione.

Secondo il principio di responsabilizzazione (*accountability*, art. 5, par. 2), il titolare del trattamento, cioè colui che stabilisce le finalità e i mezzi del trattamento, non solo è tenuto a rispettare i principi di cui al paragrafo 1, ma deve anche essere in grado di dimostrarne la conformità. Ciò segna un'evoluzione fondamentale rispetto alla disciplina previgente: la protezione dei dati non è più basata su un modello meramente autorizzativo o formale, bensì su un sistema di responsabilità proattiva, in cui il titolare deve adottare misure tecniche, organizzative e documentali idonee a garantire e comprovare la conformità al Regolamento.

Vi sono due principi che rispondono in modo particolarmente diretto ai principi di necessità e proporzionalità, espressione del bilanciamento tra tutela dei diritti fondamentali e libertà economiche: la limitazione della finalità e la minimizzazione dei dati.

Il principio di limitazione della finalità impone che i dati personali siano raccolti per scopi determinati, espliciti e legittimi, e che ogni successivo trattamento sia compatibile con tali scopi originari. Ciò serve a evitare che i dati vengano utilizzati in modo arbitrario o per finalità ulteriori non previste al momento della raccolta. La valutazione di compatibilità deve tener conto, secondo il considerando 50 del GDPR, di elementi quali il nesso tra la finalità originaria e quella del trattamento successivo, il contesto in cui i dati sono stati raccolti, la natura dei dati e le possibili conseguenze per gli interessati.

Il principio di minimizzazione dei dati, invece, rappresenta la traduzione più diretta del principio di necessità: i dati personali devono essere «adeguati, pertinenti e limitati a quanto necessario» rispetto alle finalità perseguite. Tale principio impone una valutazione preventiva di proporzionalità del trattamento, in modo da evitare la raccolta e conservazione di informazioni eccedenti o non indispensabili. Esso si collega strettamente anche al principio di protezione dei dati fin dalla progettazione (*privacy by design*, art. 25), che obbliga il titolare a configurare i sistemi informativi e i processi aziendali in modo da limitare per quanto possibile la quantità e la portata dei dati trattati.

Nel complesso, i principi di limitazione della finalità e di minimizzazione dei dati costituiscono l'espressione operativa della proporzionalità nel trattamento dei dati personali: garantiscono che l'azione del titolare sui dati personali dell'interessato sia limitata nella misura strettamente necessaria al raggiungimento di scopi legittimi, preservando al contempo l'essenza del diritto alla protezione dei dati sancito dagli articoli 7 e 8 della Carta dei diritti fondamentali dell'Unione europea.

5. Le condizioni di liceità del trattamento

L'articolo 6 del GDPR specifica le condizioni per il trattamento legale dei dati, chiamate anche "basi legali". Queste sono le uniche condizioni che rendono legittimo il trattamento dei dati personali.

Le condizioni sono:

- **Consenso:** l'interessato ha dato il proprio consenso al trattamento dei propri dati personali per una o più finalità specifiche.
- **Necessità contrattuale:** il trattamento è necessario per l'esecuzione di un contratto di cui l'interessato è parte, o per l'esecuzione di misure precontrattuali adottate su richiesta dello stesso.
- **Obbligo legale:** il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento.
- **Interessi vitali:** il trattamento è necessario per proteggere gli interessi vitali dell'interessato o di un'altra persona fisica.

- Esecuzione di un compito di interesse pubblico: il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento.
- Legittimo interesse: il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, salvo che su tali interessi prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali.

Per ciascuna delle condizioni sopra, è possibile fornire alcuni esempi ricorrenti nella pratica:

- Consenso: l'interessato acconsente a ricevere una newsletter promozionale iscrivendosi volontariamente tramite un modulo online.
- Necessità contrattuale: un'azienda di e-commerce tratta i dati dell'acquirente per spedire un prodotto acquistato e gestire il pagamento.
- Obbligo legale: un'azienda conserva i dati fiscali delle fatture per il periodo previsto dalla normativa tributaria.
- Interessi vitali: in caso di emergenza medica, i dati sanitari di un paziente vengono comunicati ai soccorritori per salvaguardarne la vita.
- Esecuzione di un compito di interesse pubblico: un ente pubblico tratta i dati dei cittadini per l'emissione della carta d'identità elettronica.
- Legittimo interesse: un'azienda installa un sistema di videosorveglianza per proteggere i propri locali da furti, nel rispetto dei principi di necessità e proporzionalità.

In ogni caso, spetta al titolare stabilire quale base giuridica sia applicabile al trattamento, prima di iniziare a trattare i dati, e documentare tale scelta in modo chiaro e motivato. La scelta della base di liceità non può essere modificata retroattivamente né “selezionata” in maniera opportunistica: il titolare deve individuare quella che rispecchia effettivamente la finalità perseguita e le circostanze del trattamento.

5.1. Categorie particolari di dati (dati sensibili)

Come abbiamo anticipato sopra, i dati sensibili (o, come definiti dall'art. 9 GDPR, categorie particolari di dati personali) sono quei dati che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché i dati genetici, i dati biometrici intesi a identificare in modo univoco una persona fisica, i dati relativi alla salute e i dati relativi alla vita sessuale o all'orientamento sessuale della persona.

La *ratio* di una disciplina rafforzata per queste categorie di dati risponde all'esigenza di graduare la protezione dei dati in base alla sensibilità e al rischio potenziale per i diritti e le libertà fondamentali dell'individuo. I dati sensibili, infatti, possono rivelare aspetti intimi e profondamente identitari della persona e, se divulgati o trattati in modo improprio, possono condurre a forme di discriminazione o stigmatizzazione sociale. La regola generale è che è vietato trattare tali dati (art. 9, par. 1 GDPR), salvo che ricorra una delle eccezioni previste dal paragrafo 2.

L'articolo 9, par. 2, delinea infatti requisiti specifici per il trattamento di categorie particolari di dati. Tali requisiti devono essere considerati come aggiuntivi rispetto all'art. 6(1) GDPR, cioè è necessario che sussista una base giuridica ordinaria per il trattamento (ad es. consenso, obbligo legale, interesse pubblico, interesse legittimo)⁸, e in più una delle condizioni speciali che giustificano il trattamento dei dati sensibili.

Queste includono, tra le altre, il consenso esplicito⁹ dell'interessato (lett. a); il trattamento di dati manifestamente resi pubblici dall'interessato (lett. e); il trattamento necessario per motivi di interesse pubblico rilevante (lett. g); il trattamento necessario per finalità di assistenza sanitaria o sociale (lett. h); il trattamento necessario per motivi di sanità pubblica (lett. i); e il trattamento necessario per finalità di archiviazione nel pubblico interesse, di ricerca scientifica o storica, o a fini statistici (lett. j)¹⁰.

5.2. Il consenso dell'interessato

Secondo l'art. 4, par. 11, il consenso dell'interessato è qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o

⁸ L'interesse legittimo non è applicabile al trattamento di categorie particolari di dati, salvo casi eccezionali nei quali il trattamento ricada in una delle basi dell'art. 9(2).

⁹ Secondo il Comitato europeo per la protezione dei dati, il termine "esplicito" si riferisce al modo in cui il consenso viene espresso dall'interessato e significa che l'interessato deve fornire una dichiarazione esplicita di consenso, come una dichiarazione scritta o, online, compilando un modulo elettronico, inviando un'e-mail, caricando un documento scansionato. Vedi *European Data Protection Board*, Linee guida 05/2020 sul consenso ai sensi del Regolamento 2016/679 Versione 1.1, adottate il 4 maggio 2020.

¹⁰ Il Comitato europeo per la protezione dei dati ha chiarito che, laddove le basi legali dell'articolo 9(2) siano meno protettive dell'articolo 6 (ad esempio, quando i dati sono manifestamente resi pubblici dall'interessato), l'articolo 6 dovrebbe applicarsi cumulativamente in questo contesto per garantire una protezione completa delle categorie particolari di dati. Ciò significa che anche se i dati sono resi pubblici, dovrebbero comunque essere trattati in modo legale, corretto e trasparente, mantenendo gli elevati standard di protezione dei dati richiesti dal GDPR.

azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento.

Innanzitutto, il consenso deve essere libero; cioè l'individuo deve avere una scelta genuina. Questo significa che, se l'interessato non può scegliere, è obbligato a dare il consenso o subirà conseguenze negative per non averlo dato, allora il consenso non è considerato libero.

In secondo luogo, il consenso deve essere specifico, in linea con il principio della limitazione delle finalità. Ogni finalità del trattamento dei dati deve avere il proprio consenso, permettendo all'interessato di accettare o rifiutare ogni finalità individualmente. Questa specificità può comprendere attività di trattamento separate se condividono la stessa finalità.

Inoltre, il consenso deve essere informato, aderendo al principio della trasparenza e al diritto all'informazione come delineato negli articoli 13 e 14 del GDPR. Gli elementi essenziali che devono essere comunicati includono l'identità del titolare del trattamento, le finalità del trattamento, le categorie di dati coinvolti, i diritti dell'interessato e qualsiasi processo decisionale automatizzato o trasferimento di dati.

Infine, il consenso deve essere affermativo, indicando chiaramente che l'interessato ha acconsentito all'attività di trattamento specifica. Questo può avvenire tramite una dichiarazione scritta o orale o un'altra azione positiva.

Relativamente al consenso, l'articolo 7(3) aggiunge che l'interessato ha sempre il diritto di revocare il consenso.

Il consenso è spesso considerato la condizione di liceità più protettiva. In effetti, esso riflette l'essenza stessa del diritto alla protezione dei dati personali poiché attribuisce all'individuo la possibilità di decidere autonomamente sull'uso dei propri dati personali.

Tuttavia, sono state sollevate crescenti critiche sull'efficacia del consenso, specialmente riguardo al trattamento dei dati in contesti online¹¹.

È stato osservato che il consenso risulta spesso non pienamente libero, poiché l'accesso a molti servizi online viene subordinato all'accettazione di trattamenti di dati non necessari alla loro effettiva erogazione¹². Inoltre, il design delle interfacce dei siti web può influenzare o coartare il consenso (ad es. tramite i

¹¹ Vedi, tra gli altri, B. CUSTERS ET AL., *Consent and Privacy*, in P. SCHABER, A. MÜLLER (eds.), *The Routledge Handbook of the Ethics of Consent*, Abingdon: Routledge, 2018 e F. ZUIDERVEEN BORGESIU, *Informed Consent: We Can Do Better to Defend Privacy*, in *IEEE Security & Privacy*, 2015 (2), pp. 103-107.

¹² In tali casi può rilevare l'Articolo 7, paragrafo 4, secondo cui, nel valutare se il consenso è stato liberamente prestato, occorre considerare in particolare se la conclusione o l'esecuzione di un contratto, inclusa la fornitura di un servizio, sia condizionata al consenso a trattamenti di dati personali non indispensabili per tale esecuzione.

cosiddetti “*tracking walls*”), con la pratica dei cosiddetti “*dark patterns*”¹³. Questi ultimi sono strategie di design utilizzate per manipolare gli utenti a fare scelte che potrebbero non essere nel loro miglior interesse o che potrebbero non aver fatto liberamente. Questi possono includere pulsanti ingannevoli, linguaggio confuso o opzioni di opt-out nascoste, che rendono difficile per gli utenti rifiutare o revocare il consenso o capire a cosa stanno acconsentendo.

Il consenso non è spesso specifico. In molti contesti online, agli utenti viene generalmente richiesto di dare un consenso generico, non potendo selettivamente accettare certe attività di trattamento mentre ne rifiutano altre, fornendo così un “consenso aggregato”.

Il consenso è anche spesso scarsamente informato. Molti utenti di Internet danno il consenso senza leggere o comprendere le informazioni sul trattamento dei dati, che sono talvolta presentate in modo vago e ambiguo. Gli utenti spesso non sanno chi tratterà i loro dati.

Infine, il consenso non è sempre inequivocabile. Potrebbe essere dato semplicemente cliccando su un banner o spuntando una casella, possibilmente insieme all'accettazione dei termini di servizio, senza chiara evidenza che questa azione rappresenti una scelta vera da parte dell'utente.

Vi è chi sostiene che occorrerebbe rafforzare il modello del consenso attraverso obblighi più stringenti per i titolari: informative più chiare e brevi, interfacce progettate in modo neutrale, divieto di pratiche manipolative, possibilità di negare il consenso senza perdere l'accesso ai servizi e meccanismi facilmente accessibili per revocarlo in qualsiasi momento.

D'altra parte, vi è chi ritiene invece che l'idea di un consenso genuino si debba abbandonare – almeno in molti contesti digitali – a favore di modelli normativi che responsabilizzino maggiormente i titolari del trattamento, spostando l'onere della protezione dei dati dalle spalle dell'individuo a quelle dell'organizzazione, come nel caso del legittimo interesse.

5.3. Il legittimo interesse

Il legittimo interesse rappresenta una delle basi giuridiche più flessibili e, al tempo stesso, più controverse del GDPR. Ai sensi dell'articolo 6, par. 1, lett. f), il trattamento è lecito quando è «necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi», a meno che su tali interessi non prevalgano «gli interessi o i diritti e le libertà fondamentali dell'interessato».

¹³ J. LUGURI, L.J. STRAHILEVITZ, *Shining a Light on Dark Patterns*, in *Journal of Legal Analysis*, 2021 (13,1), pp. 43-109.

Questa base giuridica non è disponibile per le autorità pubbliche nell'esecuzione dei loro compiti istituzionali e, in generale, richiede l'esistenza di un interesse reale, attuale e sufficientemente concreto, che il titolare deve essere in grado di dimostrare.

Il Comitato europeo per la protezione dei dati ha chiarito che il ricorso al legittimo interesse richiede un'analisi strutturata (spesso definita test di bilanciamento o LIA, cioè *Legitimate Interest Assessment*) composta da tre fasi:

1. Il titolare deve identificare un interesse proprio o di terzi che sia effettivo e non meramente ipotetico. Esempi ricorrenti includono la sicurezza dei sistemi informatici, la prevenzione delle frodi, la protezione del patrimonio aziendale o il miglioramento di servizi già richiesti dagli utenti.
2. Il trattamento deve essere necessario per perseguire tale interesse e non devono esistere modalità alternative, meno invasive rispetto ai diritti dell'interessato, che permettano di ottenere il medesimo risultato.
3. Occorre valutare se i diritti, le aspettative ragionevoli e le libertà fondamentali dell'interessato prevalgano sull'interesse perseguito dal titolare. Per esempio, un trattamento può risultare sproporzionato quando incide significativamente sulla sfera privata dell'interessato o quando avviene in modo inatteso rispetto al contesto della raccolta dei dati.

Il test di bilanciamento deve essere documentato e, quando appropriato, reso disponibile all'interessato, in linea con il principio di trasparenza (art. 5 GDPR). Inoltre, quando si fa affidamento sul legittimo interesse, il titolare deve garantire che l'interessato possa esercitare il diritto di opposizione previsto dall'articolo 21, salvo la presenza di motivi cogenti che prevalgano sui diritti dell'interessato.

Il legittimo interesse, se correttamente applicato, consente un trattamento proporzionato e coerente con finalità legittime del titolare, senza tuttavia indebolire le tutele riconosciute agli individui. Se applicato in modo improprio, rischia invece di diventare una base "di comodo" per il titolare del trattamento, che può sottostimare i rischi del trattamento, in contrasto con i principi del GDPR e con le aspettative degli interessati.

6. I diritti dell'interessato

I diritti dell'interessato costituiscono uno dei pilastri fondamentali del GDPR. Essi rappresentano gli strumenti attraverso i quali la persona fisica può esercitare il controllo sui propri dati personali, verificare che il trattamento avvenga nel rispetto dei principi di liceità, correttezza e trasparenza, e reagire a eventuali violazioni.

Il Regolamento non si limita a elencare tali diritti, ma impone anche al titolare del trattamento obblighi specifici per garantirne l'effettivo esercizio¹⁴, come la predisposizione di canali di comunicazione adeguati, la risposta entro termini certi e la gratuità delle operazioni (salvo richieste manifestamente infondate o eccessive).

I diritti riconosciuti all'interessato dagli articoli 13-22 del GDPR sono:

- Il diritto di essere informato (articoli 13 e 14): il diritto di ricevere informazioni chiare, comprensibili e facilmente accessibili sul trattamento, sia quando i dati sono raccolti presso il soggetto interessato, sia quando provengono da terzi. Tale diritto, nella pratica, porta alla redazione delle cosiddette "informative privacy" che, secondo i contenuti del GDPR, devono contenere, tra gli altri, l'identità del titolare del trattamento, le finalità del trattamento dei dati, le categorie di dati personali trattati, i destinatari o le categorie di destinatari dei dati, il periodo per il quale i dati saranno conservati, l'esistenza dei diritti dell'interessato e qualsiasi processo decisionale automatizzato coinvolto nel trattamento dei dati.
- Il diritto di accesso (articolo 15): il diritto di ottenere una conferma sul trattamento dei dati personali e di ottenere informazioni su come vengono trattati, inclusa una copia dei dati stessi.
- Il diritto di rettifica (articolo 16): il diritto di far correggere dati personali inesatti o completare dati incompleti.
- Il diritto alla cancellazione (articolo 17): conosciuto anche come diritto all'oblio (si veda nel dettaglio sotto), consente agli interessati di richiedere la cancellazione dei propri dati personali in determinate condizioni.
- Il diritto di limitazione del trattamento (articolo 18): il diritto di limitare il trattamento dei propri dati personali in determinate circostanze.
- Il diritto alla portabilità dei dati (articolo 20): il diritto di ricevere i propri dati personali in un formato strutturato, di uso comune e leggibile da dispositivo automatico e di trasmetterli a un altro titolare del trattamento.
- Il diritto di opposizione (articolo 21): il diritto di opporsi al trattamento dei propri dati personali per determinate finalità, inclusi i fini di marketing diretto.
- Il diritto a non essere soggetto a una decisione basata unicamente su un trattamento automatizzato, compresa la profilazione (articolo 22): il di-

¹⁴ Articolo 12 del Regolamento.

ritto a non essere soggetto a una decisione basata unicamente su un trattamento automatizzato, compresa la profilazione, che produca effetti giuridici o incida significativamente sulla persona.

6.1. Il diritto alla cancellazione (diritto all'oblio)

Il diritto all'oblio, disciplinato dall'articolo 17 del GDPR, rappresenta una delle innovazioni più rilevanti introdotte dal Regolamento. Esso riconosce all'interessato la possibilità di ottenere la cancellazione dei propri dati personali quando ricorrono determinate condizioni, riflettendo l'idea che i dati non debbano essere conservati o resi disponibili oltre il tempo necessario rispetto alle finalità per le quali sono stati raccolti.

Le principali situazioni in cui l'interessato può chiedere la cancellazione sono:

- i dati non sono più necessari rispetto alle finalità originarie del trattamento;
- l'interessato revoca il consenso e non sussiste altra base giuridica per il trattamento;
- l'interessato si oppone al trattamento basato sul legittimo interesse del titolare e non prevalgono motivi legittimi per proseguire;
- i dati sono stati trattati illecitamente;
- i dati devono essere cancellati per adempiere a un obbligo legale;
- i dati sono stati raccolti relativamente all'offerta di servizi della società dell'informazione ai minori.

Il diritto all'oblio non è tuttavia assoluto. L'art. 17, par. 3, individua una serie di eccezioni, tra cui l'esercizio del diritto alla libertà di espressione e di informazione; l'adempimento di obblighi legali o l'esecuzione di compiti di interesse pubblico; motivi di interesse pubblico nel settore della sanità pubblica; finalità di archiviazione nel pubblico interesse, di ricerca scientifica o storica, o a fini statistici; l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Il diritto all'oblio è divenuto particolarmente rilevante nel contesto online, dove la persistenza delle informazioni può avere effetti duraturi sulla reputazione personale. La giurisprudenza della Corte di giustizia, a partire dalla sentenza *Google Spain* del 2014¹⁵, ha riconosciuto che gli interessati possono richiedere ai motori di ricerca la deindicizzazione dei risultati che li riguardano, quando le informazioni siano inadeguate, non pertinenti, non più pertinenti o eccessive rispetto alle finalità della pubblicazione.

¹⁵ CGUE, C-131/12, *Google Spain v AEPD and Mario Costeja González*.

È importante distinguere tra cancellazione dei dati alla fonte e deindicizzazione: nel primo caso si tratta dell'eliminazione dei dati presso il titolare del trattamento; nel secondo, invece, i dati rimangono disponibili sul sito originario, ma non sono più facilmente reperibili tramite ricerche nominative.

Il diritto all'oblio, pur essendo uno strumento potente di tutela, richiede un equilibrio con altri diritti fondamentali, primo tra tutti la libertà di informazione. Per questo motivo, la valutazione delle richieste di cancellazione o deindicizzazione deve essere svolta caso per caso, alla luce del contesto, del ruolo pubblico dell'interessato e della rilevanza sociale dell'informazione.

7. Gli obblighi del titolare del trattamento

7.1. Il titolare e il responsabile del trattamento

Il titolare del trattamento è la persona fisica o giuridica che determina le finalità e i mezzi del trattamento dei dati personali (articolo 4, par. 7). In quanto tale, il titolare ha la responsabilità primaria di garantire che le attività di trattamento dei dati siano conformi ai principi del GDPR. Ciò include la definizione dei motivi per cui i dati personali vengono raccolti, le modalità di utilizzo e la garanzia che vengano adottate misure adeguate per la protezione dei dati.

Per contro, un responsabile del trattamento, ai sensi dell'articolo 4, paragrafo 8, è la persona fisica o giuridica che tratta i dati per conto del titolare del trattamento. Il ruolo del responsabile dunque è più operativo, in quanto gestisce le attività di trattamento dei dati sulla base delle istruzioni fornite dal titolare del trattamento.

L'articolo 28 del GDPR prevede che il titolare e il responsabile del trattamento formalizzino il loro rapporto attraverso un contratto. Questo contratto deve stabilire le istruzioni specifiche per il trattamento dei dati, la natura e lo scopo del trattamento, il tipo di dati personali coinvolti e gli obblighi di entrambe le parti.

Una sfida significativa si presenta quando i titolari del trattamento hanno più potere contrattuale e influenza dei titolari del trattamento. In tali scenari, i responsabili potrebbero dettare condizioni che limitano la capacità del titolare del trattamento di applicare pienamente la conformità al GDPR, creando uno squilibrio di potere che potrebbe compromettere gli sforzi di protezione dei dati.

L'articolo 26 affronta anche il caso di contitolarità, cioè quando due o più entità determinano congiuntamente le finalità e i mezzi del trattamento dei dati personali. In tal caso entrambe tali entità sono titolari del trattamento e dovranno, attraverso l'accordo di contitolarità, definire chiaramente le rispettive responsabilità in relazione al trattamento.

L'attuazione pratica del controllo congiunto può essere complessa¹⁶. Determinare l'esatta natura del controllo e della responsabilità può essere impegnativo, con conseguenti difficoltà nel classificare se un'entità è un contitolare del trattamento o un semplice responsabile del trattamento. Questa ambiguità può complicare la responsabilità e la conformità, rendendo essenziale per le entità coinvolte in attività di trattamento congiunto documentare accuratamente i propri ruoli e responsabilità.

7.2. Gli obblighi del titolare del trattamento

Il GDPR enfatizza la responsabilità del titolare del trattamento richiedendo implementare misure tecniche e organizzative adeguate a garantire e dimostrare la conformità in base al rischio del trattamento per i diritti e le libertà dei soggetti interessati.

Questo è il nucleo del “principio di responsabilizzazione” alla base della filosofia del GDPR¹⁷. Il Regolamento riconosce la complessità e la varietà delle attività di trattamento dei dati e la difficoltà di definire misure universali applicabili a tutte le situazioni. Inoltre, il titolare del trattamento è considerato la persona più competente per valutare i rischi e implementare misure preventive. Questo cambiamento sottolinea il ruolo dei titolari del trattamento e la responsabilità proattiva, spostandosi da prescrizioni dettagliate a un “impegno per la conformità”.

La misura chiave di responsabilità è il rischio delle operazioni di trattamento dei dati rispetto al diritto alla protezione dei dati¹⁸. Ciò significa che i titolari del trattamento devono valutare i rischi specifici posti dalle loro attività di trattamento, considerando sia la probabilità di occorrenza sia l'impatto potenziale sugli interessati. Devono quindi implementare misure tecniche e organizzative proporzionate a questi rischi, garantendo che il trattamento dei dati sia effettuato in conformità ai principi del GDPR.

7.3. Data protection by design e by default

Il principio di responsabilizzazione è accompagnato dall'idea di favorire una “privacy by design”.

¹⁶ C. MILLARD, *At This Rate, Everyone Will Be a [Joint] Controller of Personal Data*, in *International Data Privacy Law*, 2019 (4), pp. 217-219.

¹⁷ T. KARJALAINEN, *All Talk, No Action? The Effect of the GDPR Accountability Principle on the EU Data Protection Paradigm*, in *Eur. Data Prot. L. Rev.*, 2022 (1).

¹⁸ In questo senso, si può dire che il GDPR adotti un “approccio basato sul rischio” alla protezione dei dati.

Il concetto di protezione dei dati *by design* e *by default* può essere fatto risalire all'idea di "*privacy by design*", introdotta negli anni '90 da Ann Cavoukian, allora Commissario per l'informazione e la privacy dell'Ontario, Canada.

I principi alla base di questo concetto includono la prevenzione dei problemi piuttosto che la loro correzione, il che significa che i problemi dovrebbero essere valutati durante la fase di progettazione e l'applicazione dovrebbe prevenire il verificarsi dei rischi. La privacy dovrebbe essere l'impostazione predefinita, quindi non dovrebbe essere obbligatorio compilare un campo del modulo quando la fornitura dei dati è facoltativa. La privacy dovrebbe anche essere incorporata nel design, ad esempio utilizzando tecniche come la pseudonimizzazione o la minimizzazione dei dati. È essenziale mantenere la piena funzionalità, rispettando tutte le esigenze e respingendo false dicotomie come più privacy equivale a meno sicurezza. La sicurezza deve essere garantita per tutto il ciclo di vita del prodotto o servizio. La visibilità e la trasparenza del trattamento sono cruciali; tutte le fasi operative dovrebbero essere trasparenti per verificare la protezione dei dati. Infine, l'utente deve essere al centro, con i suoi diritti rispettati e risposte tempestive e chiare fornite alle sue richieste di controllo sui dati personali.

Ispirandosi a questi criteri, il principio della data protection by design e by default previsto all'art. 25 del GDPR richiede ai titoli del trattamento di implementare misure tecniche e organizzative adeguate sia al momento di determinare i mezzi per il trattamento (letteralmente "*by design*") sia durante il trattamento stesso. Queste misure, come la pseudonimizzazione, dovrebbero integrare efficacemente i principi di protezione dei dati come la minimizzazione dei dati e garantire le necessarie salvaguardie per soddisfare i requisiti del GDPR e proteggere i diritti degli interessati.

7.4. Valutazione di impatto sulla protezione dei dati e il Data Protection Officer

L'articolo 35 richiede ai titolari del trattamento di condurre una Valutazione di Impatto sulla Protezione dei Dati (*Data Protection Impact Assessment* o DPIA) quando il trattamento è probabilmente destinato a comportare un rischio elevato per i diritti e le libertà degli individui¹⁹.

¹⁹ Secondo il Gruppo di lavoro Articolo 29 (ovvero l'odierno Comitato europeo per la protezione dei dati), il rischio elevato può essere indicato, tra l'altro, da uno o più di questi fattori: trattamento valutativo o di scoring, compresa la profilazione per valutare aspetti come la performance professionale e la situazione economica, come un'azienda biotecnologica che offre test genetici direttamente ai consumatori; decisioni automatizzate che producono effetti giuridici significativi, come assunzioni, concessione di prestiti o sottoscrizione di polizze assicurative; monitoraggio si-

Una DPIA è una procedura strutturata per valutare i rischi connessi al trattamento dei dati. Deve includere: a) una descrizione sistematica delle operazioni di trattamento previste e delle finalità del trattamento; b) una valutazione della necessità e della proporzionalità delle operazioni di trattamento in relazione alle finalità; c) una valutazione dei rischi per i diritti e le libertà degli interessati; e d) le misure previste per affrontare i rischi.

Gli articoli 37-39 richiedono la designazione di un Responsabile della Protezione dei Dati (*Data Protection Officer*, abbreviato DPO) in condizioni specifiche. Il DPO ha il compito di supervisionare la strategia di protezione dei dati e garantire la conformità ai requisiti del GDPR. Il ruolo del DPO include informare e consigliare il titolare o il responsabile del trattamento e i loro dipendenti sui loro obblighi in materia di protezione dei dati, monitorare la conformità al GDPR e cooperare con l'autorità di controllo.

8. Il Garante per la protezione dei dati personali

Il GDPR stabilisce un sistema di controllo incentrato sul ruolo delle autorità di controllo nazionali. Queste sono incaricate di monitorare i titolari e i responsabili del trattamento e di far rispettare la conformità al Regolamento.

Come noto, nel nostro ordinamento tale ruolo è esercitato dall'Autorità Garante per la protezione dei dati personali, istituita con la legge n. 675/1996 e oggi disciplinata dal Codice della privacy come modificato dal d.lgs. 101/2018.

L'Autorità, con sede a Roma, è composta da quattro membri, nominati per sette anni non rinnovabili: due eletti dalla Camera dei deputati e due dal Senato della Repubblica, con maggioranze qualificate. Il Collegio elegge al proprio interno il Presidente, che ha la rappresentanza dell'Autorità e ne coordina l'attività. La struttura operativa è supportata da un Ufficio composto da dirigenti, funzionari e personale tecnico-amministrativo.

Al fine di monitorare l'applicazione del Regolamento il Garante dispone di ampi poteri investigativi, correttivi, autorizzativi e consultivi, come previsto dagli articoli 57 e 58 del GDPR. In particolare, l'Autorità può condurre indagini e ispezioni, anche avvalendosi della Guardia di Finanza; effettuare audit e richiedere informazioni e documenti a titolari e responsabili; ottenere accesso a qualsiasi sede in cui avvenga il trattamento dei dati; adottare avvertimenti, ammonimenti e reprimende; ingiungere al titolare di conformarsi al GDPR, compresa

stematico, come la videosorveglianza in luoghi pubblici; trattamento di dati sensibili, giudiziari o altamente personali, come opinioni politiche, dati di geolocalizzazione o dati finanziari, ecc. Vedi Art. 29 WP, Linee guida sulla Valutazione di Impatto sulla Protezione dei Dati (DPIA) e Determinazione di quando il trattamento è «probabilmente destinato a comportare un rischio elevato» ai sensi del Regolamento 2016/679, 9-11.

la limitazione o il divieto del trattamento; autorizzare determinati trattamenti quando previsto dalla legge; emettere pareri su atti normativi e schemi di regolamento che incidono sulla protezione dei dati personali.

In caso di non conformità, il Garante può imporre sanzioni amministrative pecuniarie, che possono essere particolarmente rilevanti. Il GDPR prevede un sistema sanzionatorio graduato, con importi che possono raggiungere fino a 20 milioni di euro o il 4% del fatturato annuo mondiale del gruppo nel precedente esercizio, scegliendo il valore più elevato. La determinazione dell'importo dipende da una serie di fattori, tra cui natura, gravità e durata della violazione; grado di responsabilità del titolare o del responsabile; eventuali precedenti violazioni; modalità con cui l'Autorità è venuta a conoscenza dell'illecito; misure correttive adottate dal titolare; qualunque fattore aggravante o attenuante pertinente.

9. La tutela giurisdizionale

Il GDPR prevede un sistema di tutela giurisdizionale articolato e coerente con i principi di effettività e accessibilità della protezione. L'interessato può attivare diversi rimedi quando ritenga che il trattamento dei suoi dati personali violi il Regolamento, sia nei confronti dei titolari o responsabili del trattamento, sia nei confronti dell'autorità di controllo.

In primo luogo, il soggetto interessato può presentare un reclamo al Garante in funzione dell'articolo 77, che riconosce il diritto di presentare un reclamo all'Autorità di controllo competente. Il reclamo rappresenta un rimedio amministrativo attraverso il quale l'interessato può denunciare eventuali violazioni e sollecitare l'intervento correttivo o sanzionatorio dell'Autorità.

L'articolo 78 del GDPR prevede inoltre la possibilità di proporre ricorso contro le decisioni dell'autorità di controllo o contro la sua inerzia, nel caso in cui non si sia pronunciata sul reclamo entro i termini dovuti. In Italia, la competenza a conoscere tali ricorsi è attribuita al tribunale ordinario del luogo in cui risiede l'interessato, secondo quanto stabilito dagli articoli 152 e seguenti del Codice della privacy. Le pronunce del tribunale sono impugnabili dinanzi alla Corte d'Appello e, in ultima istanza, alla Corte di Cassazione.

Accanto alla tutela di fronte al Garante, l'articolo 79 GDPR attribuisce all'interessato la possibilità di proporre un ricorso giurisdizionale nei confronti del titolare o del responsabile del trattamento dinanzi al giudice competente, qualora ritenga che il trattamento violi le disposizioni del Regolamento. Nel nostro ordinamento, tale ricorso va effettuato dinnanzi al giudice civile ed è finalizzato sia ad accertare l'illiceità del trattamento sia, eventualmente, ad adottare misure

idonee a rimuovere la violazione, incluse, ad esempio, l'interruzione del trattamento o la cancellazione dei dati.

In questo caso è sempre ammessa la possibilità di richiedere il risarcimento del danno patito dal soggetto interessato.

Tale ipotesi è confermata dall'articolo 82 del GDPR che introduce un regime particolarmente ampio, volto a garantire un risarcimento effettivo a chiunque abbia subito un danno – materiale o immateriale – causato da una violazione del Regolamento. Il titolare o il responsabile del trattamento rispondono del danno, salvo che riescano a dimostrare che l'evento non è loro imputabile. Il danno risarcibile può consistere non solo in una perdita economica, ma anche in un pregiudizio morale, come la lesione della reputazione, lo stress, l'ansia o altre forme di sofferenza derivanti dall'illecito trattamento.

Ove più titolari o responsabili siano coinvolti nel medesimo trattamento, il GDPR prevede un regime di responsabilità solidale, che assicura all'interessato la possibilità di ottenere l'integrale ristoro del danno da uno qualsiasi dei soggetti coinvolti, lasciando poi a questi ultimi l'onere di rivalersi tra loro in funzione del grado di responsabilità.

Il rapporto tra i rimedi giurisdizionali e quelli amministrativi è caratterizzato da complementarità: il reclamo al Garante consente un intervento rapido e specializzato sul piano amministrativo, mentre il ricorso al giudice permette di ottenere una valutazione piena della responsabilità e un eventuale risarcimento del danno. L'interessato, pertanto, dispone di un ventaglio di strumenti che possono essere attivati parallelamente o in alternativa, in funzione della natura della violazione e del tipo di tutela ricercata.

10. L'applicazione del GDPR nel contesto europeo (cenni)

L'applicazione del GDPR avviene in un quadro europeo complesso caratterizzato da una combinazione di norme direttamente applicabili, competenze condivise tra Stati membri e meccanismi di cooperazione istituzionale. Sebbene il Regolamento abbia l'obiettivo di garantire un livello uniforme di protezione dei dati personali in tutta l'Unione, la sua attuazione pratica mostra significative differenze tra i vari ordinamenti, dovute sia alle norme nazionali di integrazione sia alle prassi delle singole autorità di controllo.

Un ruolo centrale è svolto dal Comitato europeo per la protezione dei dati (*European Data Protection Board*), l'organismo che riunisce le autorità di controllo degli Stati membri e il Garante europeo della protezione dei dati. Il Comitato adotta linee guida, raccomandazioni e pareri che contribuiscono all'interpretazione uniforme del Regolamento e assicura il funzionamento del meccanismo di coerenza previsto dal Capo VII del GDPR. Attraverso questo meccanismo,

L'EDPB interviene per garantire che le autorità nazionali applichino il Regolamento in modo convergente, in particolare nei casi transfrontalieri.

Nei trattamenti che coinvolgono più Stati membri, trova applicazione il principio del *one-stop-shop*, che individua un'unica autorità capofila (*lead supervisory authority*) competente a coordinare il procedimento, riducendo la frammentazione e assicurando una risposta più efficiente nei confronti delle grandi piattaforme digitali e dei soggetti che operano su scala europea.

Nonostante questi strumenti di armonizzazione, persistono differenze rilevanti nelle modalità con cui gli Stati membri applicano il GDPR. Ciò riguarda tanto la struttura e le risorse delle singole autorità di controllo, quanto la disciplina nazionale relativa alle materie rimesse alla competenza statale, come il trattamento dei dati in ambito lavorativo, la sanità, la ricerca scientifica o i trattamenti effettuati per finalità di sicurezza pubblica. Queste differenze possono incidere sull'effettiva uniformità della protezione offerta dal Regolamento.

Un tentativo di ridurre le divergenze nelle modalità applicative, almeno nei procedimenti transfrontalieri, è stato fatto con il Regolamento (EU) 2025/2518 del 26 novembre 2025 che stabilisce norme procedurali supplementari relative all'applicazione del GDPR. Questo nuovo strumento mira a rafforzare il funzionamento del meccanismo dello *one-stop-shop*, a migliorare la cooperazione tra autorità di controllo e a rendere più prevedibili e tempestivi i procedimenti, contribuendo così a una più omogenea e coerente applicazione del Regolamento all'interno dell'Unione.

DATA GOVERNANCE ACT E DATA ACT NEL QUADRO DEGLI SPAZI COMUNI EUROPEI DEI DATI

Salvatore Sapienza

SOMMARIO: 1. Cenni introduttivi. 2. Gli Spazi Comuni Europei Dei Dati. 3. Il Data Governance Act. 3.1. Servizi di intermediazione dei dati: definizione. 3.2. Servizi di intermediazione dei dati: titolari dei dati e utenti dei dati. 3.3. Servizi di intermediazione dei dati: titolari dei dati e utenti dei dati. 4. Il Data Act. 4.1 Data Act e prodotti connessi: definizioni essenziali. 4.2 Data Act e prodotti connessi: regime giuridico. 4.3 Data Act e condivisione di dati su richiesta delle autorità. 5. Spazi di dati.

1. Cenni introduttivi

La circolazione delle informazioni è ritenuta uno degli elementi essenziali dell'economia dei dati. L'Unione Europea si è posta, a più riprese e conclusivamente nella Strategia europea dei dati del 2020¹, l'obiettivo strategico di creare un mercato unico dei dati in cui le informazioni, personali e non, possano circolare liberamente tra settori diversi e Stati membri. Gli elementi essenziali di tale circolazione possono essere rinvenuti nella definizione di un quadro normativo che abbia tre obiettivi:

a) rimuovere gli ostacoli che possano limitare la circolazione delle informazioni all'interno dell'Unione e massimizzare il valore dei dati, specie in relazione ad altri obiettivi dell'Unione, come il cambiamento climatico o la trasformazione digitale;

b) definire regole per i soggetti giuridici che operano nel mercato dei dati, con l'obiettivo di identificare un quadro giuridico di riferimento in grado di dare certezza, stabilità e credibilità alle organizzazioni che condividono informazioni;

c) incentivare la concorrenza nel mercato dei dati, mitigando le posizioni di monopolio o di oligopolio che caratterizzando l'economia dei dati;

Vale la pena rimarcare come questi obiettivi vadano, nell'ottica dell'Unione, sempre bilanciati con il rispetto dei diritti garantiti dalla Carta Europea dei Di-

¹ Commissione europea, Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni: Una strategia europea per i dati (Bruxelles, 19 febbraio 2020) COM(2020) 66 final. V. anche Commissione europea, '1.3 Definitions' JRC Data spaces Knowledge Base (7 giugno 2023).

ritti Fondamentali, su tutti i diritti alla riservatezza e alla tutela dei dati personali². Questa operazione di bilanciamento e di preminenza dei diritti fondamentali caratterizza la regolamentazione rispetto ad altre esperienze normative, su tutte quella statunitense e cinese. Alla luce di questa considerazione, vale la pena porre l'accento su due importanti regolamenti europei, già discussi congiuntamente in dottrina³, il *Data Governance Act*⁴ e il *Data Act*⁵, letti in relazione ad alcune importanti iniziative in tema di Spazi Europei dei Dati.

2. Gli Spazi Comuni Europei Dei Dati

Al centro della visione strategica europea si collocano gli “Spazi comuni europei dei dati” (o, come più comunemente noti, Common European Data Spaces), ecosistemi giuridici e tecnico-organizzativi in cui informazioni eterogenee possono fluire ed essere condivise in modo efficiente e sicuro. In buona sostanza, tali spazi dati mirano a favorire la circolazione dei dati all'interno dell'UE preservando il controllo in capo alle imprese, alle organizzazioni e agli individui che li producono. Nella strategia originaria del 2020 la Commissione UE individuò inizialmente nove ambiti strategici (mobilità, sanità, agricoltura, energia, manifattura, finanza, pubblica amministrazione, pubblica utilità, e open data), poi estesi a quattordici complessivi. Questi spazi (per es. mobilità, salute, finanziario, pubblico, manifatturiero, ecc.) costituiranno i pilastri del futuro mercato unico europeo dei dati. Essi non sono scevri, tuttavia, di elementi di criticità che vale la pena analizzare al fine di identificare, nella pratica, gli strumenti giuridici introdotti dall'Unione per far fronte ad essi.

In primo luogo, uno “Spazio di dati” è inteso come «un vero e proprio mercato unico dei dati in cui i dati personali e non personali, compresi i dati sensibili aziendali, siano sicuri e le imprese abbiano facile accesso a dati industriali di

² M. PALMIRANI, *La Mediazione Digitale e nuove forme tecnologiche di discriminazione*, in *La mediazione interculturale*, Bologna: Bononia University Press, 2021, pp. 63-75; G. SARTOR, *The way forward for better regulation in the EU – better focus, synergies, data and technology*, Bruxelles: European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs, 2022; G. PASCUZZI, *Il diritto dell'era digitale* (6ª ed.), Bologna: Il Mulino, 2025.

³ C. DUCUING, *The Regulation of Data in the European Union: the Data Governance Act and the Data Act*, in C. AKIN, S. KLIMBACHER, G. ZICCARDI (a cura di), *Smart Cities, Artificial Intelligence and Digital Transformation Law: a Handbook for Students and Professionals*, Milano: Milano University Press, 2024, pp. 63-89.

⁴ Regolamento (UE) 2022/868 del Parlamento Europeo e del Consiglio del 30 maggio 2022 relativo alla governance europea dei dati e che modifica il regolamento (UE) 2018/1724 (Regolamento sulla governance dei dati).

⁵ Regolamento (UE) 2023/2854 del Parlamento Europeo e del Consiglio del 13 dicembre 2023 riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo e che modifica il regolamento (UE) 2017/2394 e la direttiva (UE) 2020/1828 (Regolamento sui dati).

alta qualità, incentivando la crescita e creando valore»⁶. Una caratteristica essenziale di un *data space* è la presenza di un'architettura tecnologica implementata secondo un principio di interoperabilità by design. I *data space* sono intesi come sistemi robusti che permettono di raccogliere un ampio volume di dati (Big Data) e concepiti per consentire la fruizione diretta di cataloghi di dati appartenenti ad un partecipante al *data space*, che avviene secondo protocolli e ontologie condivise.

I *data space* possono presentarsi secondo tre modelli, riportati schematicamente nella Fig. 1

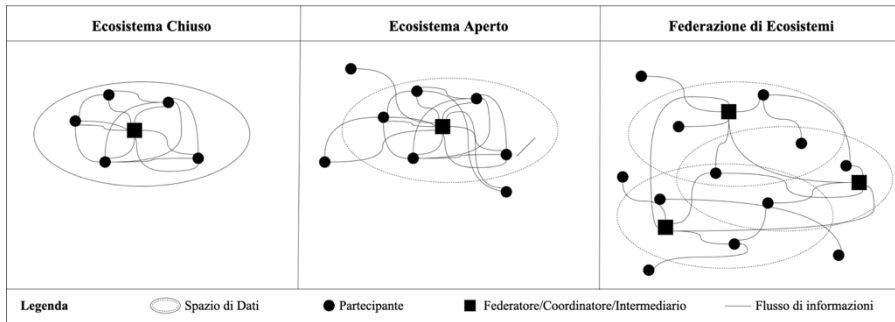


Figura 1: Modelli di Data Space

In primo luogo, un *data space* può consistere in un ecosistema *chiuso*. In questo modello, tutti i partecipanti operano all'interno di un perimetro ben definito, in cui accesso e condivisione dei dati sono riservati esclusivamente a soggetti autorizzati preventivamente. È prevista la presenza di un federatore o coordinatore centrale, incaricato di mantenere traccia delle attività e delle responsabilità dei partecipanti e assicurare che i dati rimangano confinati all'interno dell'ecosistema. Tale configurazione garantisce elevati livelli di sicurezza e controllo, ma limita fortemente le possibilità di interazione e collaborazione con attori esterni. In secondo luogo, il *data space* può costituirsi come un ecosistema *aperto*, in cui i confini risultano più permeabili rispetto al modello chiuso. Nuovi partecipanti possono essere ammessi con maggiore facilità, purché si conformino a un insieme condiviso di regole (tecniche e giuridiche) e standard di interoperabilità. Se, da un lato, questo modello facilita la crescita rapida e l'ampliamento della rete di partecipanti, dall'altro esso comporta anche maggiori sfide in termini di sicurezza e garanzia della qualità delle informazioni condivise. Infine, il modello

⁶ E. FARRELL. ET AL., *European Data Spaces – Scientific Insights into Data Sharing and Utilisation at Scale*, JRC Research Reports JRC129900, Joint Research Centre, 2023.

di un *data space* può assumere la forma di una *federazione di ecosistemi*. A differenza degli altri, questa struttura non si fonda sulla presenza di un unico gruppo di partecipanti, bensì su una pluralità di ecosistemi autonomi, ciascuno con proprie regole e politiche di governance. I rispettivi federatori comunicano e collaborano tra loro, condividendo metadati e informazioni che garantiscono l'interoperabilità tra sistemi. Ciò consente ai diversi ecosistemi di mantenere la propria autonomia gestionale pur beneficiando della cooperazione tra federazioni. In Europa, questo modello è considerato particolarmente strategico per i *data space*, poiché consente di coniugare la salvaguardia della sovranità sui dati con la creazione di reti collaborative in grado di garantire efficienza e qualità nello scambio di informazioni.

A prescindere dal modello in uso, i *data spaces* si fondano su tre componenti essenziali. In primo luogo, il nucleo informativo costituito da dati personali, non personali o misti, accompagnati dai relativi metadati, che ne descrivono origine, formato, condizioni di utilizzo e diritti associati. I dati non personali costituiscono tutti i dati diversi da quelli personali⁷, mentre quelli misti sono definiti come la presenza, all'interno dello stesso insieme di informazioni, di dati personali e non personali. Se l'insieme di dati personali e non personali è logicamente separabile, ciascun sottoinsieme segue il suo regime⁸. Altrimenti, tutte le informazioni sono considerate personali e il GDPR trova applicazione su tutto l'insieme.

In secondo luogo, è essenziale la presenza di fornitori e utilizzatori dei dati, ossia i soggetti attivamente o passivamente coinvolti nella condivisione di informazioni. Non vanno dimenticati, tuttavia, i fruitori dei benefici derivanti dalla loro condivisione, tra cui rientrano anche le pubbliche amministrazioni e gli individui in generale, quanto meno nella visione europea.

Infine, le misure di *data governance* (ossia di definizione delle procedure di indirizzo e attuazione dello scambio di dati), possibilmente ispirate anche a principi etici (sicurezza, sovranità dei dati, trasparenza, concorrenza, etc.), rappresentano il terzo elemento essenziale. Esse realizzano in pratica la sintesi, da un lato, delle misure tecniche che consentono materialmente lo scambio di dati e, dall'altro, delle norme relative allo scambio di dati. Ai *data spaces* è quindi, inevitabilmente, applicabile una *compliance* interdisciplinare capace di integrare esigenze normative, standard tecnologici e principi nel rispetto del quadro delineato dalla normativa europea, in particolare GDPR, Data Governance Act e Data

⁷ L'art. 3(1), del Regolamento (UE) 2018/1807 definisce i dati (non personali) come “i dati diversi dai dati personali definiti all'articolo 4, punto 1, del regolamento (UE) 2016/679”.

⁸ L'art. 2(2), del Regolamento (UE) 2018/1807 stabilisce che, se insiemi di dati contengono sia dati personali che non personali e questi non possono essere separati (“indissolubilmente legati”), si applica il GDPR all'intero insieme.

Act. Vale la pena, dunque, analizzare in che modo gli ultimi due Regolamenti interagiscono con gli spazi dei dati europei.

3. Il Data Governance Act

Il Data Governance Act (DGA) è un regolamento dell'UE, entrato in vigore nel settembre 2023, che istituisce le fondamenta normative per la condivisione dei dati nell'Unione. Il DGA persegue l'obiettivo di accrescere la fiducia nella condivisione volontaria dei dati tra cittadini e imprese e di rimuovere ostacoli tecnici e normativi al riutilizzo dei dati⁹. Tra le sue principali misure si annoverano quelle relative:

- a) al riutilizzo di dati pubblici protetti: facilita l'accesso e il riutilizzo di categorie di dati detenuti da enti pubblici (anche sensibili o coperti da segreto industriale) che non possono essere resi disponibili in formati aperti (Capo II DGA);
- b) ai servizi di intermediazione dei dati, ossia alla disciplina dei c.d. *data intermediaries*, operatori neutrali che facilitano lo scambio di dati fra chi li possiede (individui o aziende) e chi li utilizza (Capo III DGA);
- c) alle organizzazioni per l'altruismo dei dati, che favoriscono la creazione di enti che raccolgono dati donati volontariamente da persone fisiche e giuridiche per fini di interesse generale (Capo IV DGA);
- d) all'introduzione dell'*European Data Innovation Board* (EDIB), che consiste in un comitato di esperti per consigliare la Commissione e gli Stati membri su norme tecniche comuni e ulteriori misure di innovazione nei dati (Capo VI DGA).

3.1. Servizi di intermediazione dei dati: definizione

L'art. 2(11) del DGA definisce il servizio di intermediazione dei dati (SID) come un servizio volto a instaurare, tramite strumenti tecnici o giuridici, relazioni commerciali per la condivisione di dati tra un numero indeterminato di *interessati al trattamento* o *titolari di dati*, da un lato, e di *utenti dei dati*, dall'altro. In sostanza, il SID è un servizio (ma, in genere, una piattaforma, come i *data space*) o un "mercato di dati" (*data marketplace*) che mette in contatto soggetti che offrono dati (imprese, istituti di ricerca, cittadini) e soggetti che li richiedono o li

⁹ F. BRAVO, *Intermediazione di dati personali e servizi di data sharing dal GDPR al Data Governance Act*, in *Contratto e impresa Europa*, 2021, pp. 199-256; G. CAROVANO, M. FINCK, *Regulating data intermediaries: The impact of the Data Governance Act on the EU's data economy*, in *Computer Law & Security Review*, 2023; D. POLETTI, *Data Intermediaries*, in *European Journal of Privacy Law & Technologies*, 2022, p. 45.

utilizzano. Il DGA prevede che possano costituirsi come fornitori di SID anche entità che intendono favorire l'esercizio dei diritti degli interessati sui dati personali¹⁰.

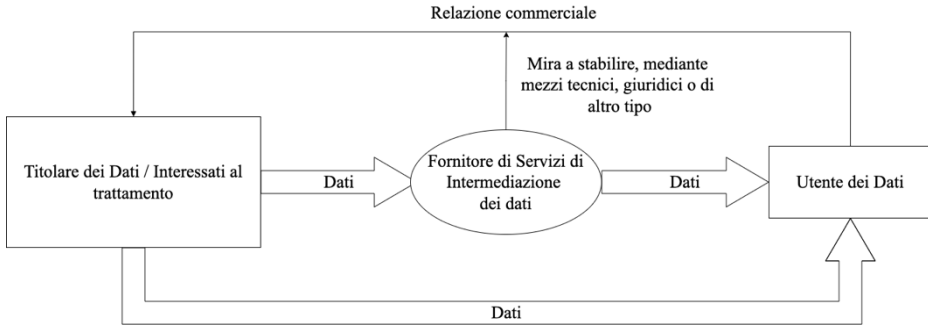


Figura 2: Servizi di Intermediazione dei Dati

Gli elementi chiave della definizione di SID sono, dunque, quattro:

- Il fornitore di SID deve porsi l'obiettivo di stabilire una relazione commerciale, ossia un rapporto economico tra due parti (titolare del dato o interessato al trattamento, da un lato, e utente del dato, dall'altro)¹¹ fondato su elementi quantificabili economicamente¹². Un prezzo di accesso al servizio è un chiaro indicatore della natura economica della relazione;
- La relazione commerciale deve essere primariamente finalizzata a condividere i dati. Sebbene, il rapporto possa presentare finalità ulteriori, ossia quelle perseguite dalle parti, la finalità primaria della relazione deve essere quella di condividere dati. La condivisione del dato può avvenire sia direttamente tra i soggetti intermediati che, indirettamente, ossia tramite le strutture del fornitore del SID.
- Il fornitore di SID deve offrire il suo servizio ad un numero indeterminato di interessati al trattamento o titolari di dati non personali. In altri termini, tra i modelli di *data space* discussi supra, un SID si presuppone come un sistema

¹⁰ D. POLETTI, *Il quadro normativo del "Data Governance Act": l'esercizio dei diritti dell'interessato nell'attività di intermediazione dei dati*, in *Le Nuove leggi civili commentate*, 2024, pp. 533-548.

¹¹ L. PASERI, *Il governo dei dati. Interesse pubblico, altruismo e partecipazione*, in *Memorie del Dipartimento di Giurisprudenza dell'Università degli Studi di Torino*, Torino: Giappichelli, 2025.

¹² Cfr. le sentenze della Corte di Giustizia Europea *Falco Privatstiftung e Thomas Rabitsch c. Gisela Weller-Lindhorst* (C-533/07, ECLI:EU:C:2009:257) §29, §30, §31, §41, §44; §58.1; v. anche *la causa Granarolo SpA/Ambrosi Emmi France SA* (C-196/15, ECLI:EU:C:2016:559), §37, §40, §41. Sul tema, S. SAPIENZA, M. PALMIRANI, S. GRECO, *Data Sharing Governance in Digital Twins and Smart Cities: The European Data Strategy*, in *Lecture Notes in Computer Science*, 2024, pp. 184-197.

necessariamente aperto. L'indeterminatezza del numero di potenziali fornitori di dati si concretizza nell'assenza di barriere a priori all'accesso al SID.

- Il fornitore di SID deve predisporre mezzi tecnici, giuridici o di altro tipo finalizzati ad instaurare la relazione commerciale. Mezzi tecnici possono consistere, ad esempio, nel predisporre l'infrastruttura che materialmente consente lo scambio di dati, mentre quelli giuridici possono consistere nella predisposizione dei contratti e delle licenze che regolano la condivisione di informazioni.

Rientrano esplicitamente (Art. 10 DGA) nella definizione di SID i servizi che pongono in relazione titolari e utilizzatori di dati, attraverso piattaforme o infrastrutture che favoriscono lo scambio, la creazione di mercati e l'uso condiviso dei dati. Vi rientrano, inoltre, i servizi che consentono alle persone fisiche di mettere a disposizione i propri dati personali, in particolare quelli che consentono l'esercizio dei diritti degli interessati previsti dal GDPR. Infine, sono ricompresi anche i modelli di condivisione organizzati in forma collettiva, come le cooperative di dati¹³, che permettono a gruppi di soggetti di gestire in modo congiunto la condivisione delle informazioni.

Al contrario, ai sensi dell'Art. 2(11) del DGA, non rientrano nella nozione di servizi di intermediazione quei servizi che, pur ricevendo dati dai titolari, li aggregano, arricchiscono o trasformano in modo da crearne una versione con valore aggiunto, ceduta poi agli utenti senza che vi sia un rapporto diretto con i titolari originari; restano altresì esclusi i servizi dedicati in via principale all'intermediazione di contenuti protetti dal diritto d'autore. Non sono considerati intermediari, inoltre, i servizi utilizzati esclusivamente dal titolare per permettere l'uso dei propri dati o impiegati all'interno di gruppi chiusi di titolari/utenti, ad esempio nei rapporti con fornitori, clienti o partner contrattuali, spesso connessi alla funzionalità di dispositivi IoT. Infine, restano fuori dalla disciplina i servizi di condivisione dei dati messi a disposizione da enti pubblici che non hanno come scopo l'instaurazione di rapporti commerciali.

3.2. Servizi di intermediazione dei dati: titolari dei dati e utenti dei dati

Ai sensi del DGA, un *titolare* dei dati è una persona giuridica o una persona fisica (diversa dall'interessato) che, conformemente al diritto dell'Unione o nazionale applicabile, ha il diritto di concedere l'accesso o la condivisione di determinati dati (siano essi personali o non personali) che sono sotto il suo controllo (Art. 2(8) DGA). Tale prerogativa può nascere, ad esempio, dalla

¹³ F. BRAVO, *EU data cooperatives. L'ingresso delle cooperative di dati nell'ordinamento europeo*, Torino, Giappichelli, 2024.

titolarità su una banca dati. Gli *utenti* dei dati sono persone fisiche o giuridiche che hanno accesso legittimo ai dati (personali o non personali) e sono autorizzati a utilizzarli (Art. 2(9) DGA), a seconda delle condizioni imposte dai titolari e, generalmente, condivise con i fornitori di SID. Nonostante il DGA distingua chiaramente le figure di titolare e utente dei dati, occorre porre attenzione alla sovrapposizione terminologica tra “titolare dei dati” (DGA) e “titolare del trattamento dei dati personali” (GDPR). Il DGA non ridefinisce né sostituisce i meccanismi del GDPR. Qualora dati personali siano oggetto di trattamento all’interno di un SID, il GDPR si applica senza pregiudizi e prevale sul DGA (Art. 1(3) DGA). Pertanto, tutti i soggetti coinvolti devono continuare a garantire i diritti degli interessati (le persone fisiche a cui i dati si riferiscono), come il diritto all’informazione, al consenso (ove necessario), alla rettifica, cancellazione, ecc. Questa regola di preminenza del GDPR vale, inoltre, nel caso in cui il SID sia un servizio che consente agli interessati ad altri trattamenti di esercitare i propri diritti.

3.3. Servizi di intermediazione dei dati: requisiti

I fornitori di SID devono operare come terze parti neutrali poste tra fornitori e utenti dei dati. Possono chiedere un compenso per facilitare gli scambi, ma non possono utilizzare direttamente i dati intermediati per trarre un proprio profitto (ad es. vendendoli o sviluppando prodotti basati su di essi). Non possono, inoltre, interferire direttamente con il valore economico o informativo del dato (ad es. aggregando le informazioni o generando inferenze a partire da esse). A tutela della loro terzietà tra le parti e neutralità rispetto al dato, devono inoltre garantire una separazione strutturale fra il servizio di intermediazione dati e qualsiasi altra attività economica da essi condotta. In altri termini, il servizio di intermediazione deve essere fornito da una persona giuridica distinta e i termini economici (prezzi, condizioni) non devono dipendere dall’utilizzo di altri servizi del medesimo fornitore.

I fornitori conformi ai requisiti del DGA possono iscriversi in un registro pubblico dell’Unione e utilizzare il titolo di “fornitore di servizi di intermediazione dei dati riconosciuto nell’Unione”. Una volta notificato il servizio all’autorità nazionale competente¹⁴ (o nominato un rappresentante legale in caso di operatore extra-UE), il fornitore può operare in tutti gli Stati membri senza ulteriori licenze nazionali. In questo modo il DGA rende possibile che *data inter-*

¹⁴ Il DGA è stato recepito in Italia tramite il Decreto Legislativo 144/2024, pubblicato in Gazzetta Ufficiale il 7 ottobre 2024. Il D.L. adegua la normativa italiana al Regolamento, identificando l’Agenzia per l’Italia Digitale (AgID) come l’autorità competente per l’applicazione del DGA.

mediaries europei, regolamentati e affidabili, alimentino gli spazi dei dati con le informazioni necessarie al loro funzionamento.

4. Il Data Act

Il regolamento Data Act (DA) copre un'ampia gamma di obiettivi strategici dell'UE nell'ambito della generazione e condivisione di dati¹⁵. La lista di finalità normative è, pertanto, relativamente corposa. Da una prospettiva generale, esso può dirsi finalizzato a garantire un accesso più equo e trasparente ai dati, promuovere la condivisione tra imprese, pubbliche amministrazioni e individui in un contesto di fiducia, sicurezza e affidabilità. Le sue norme mirano, infatti, a rimuovere gli ostacoli (tecnici, giuridici ed economici) che limitano l'utilizzo dei dati generati da dispositivi connessi e nell'ambito dei servizi digitali, nell'ottica di assicurare che i benefici economici e sociali derivanti dal loro sfruttamento siano distribuiti in modo più proporzionato e meno asimmetrico tra tutti gli attori della società dell'informazione. Per rimuovere le barriere alla circolazione dei dati, il DA stabilisce regole per la portabilità e l'utilizzo dei dati, rafforzando i diritti degli utenti e favorendo la nascita di nuovi modelli economici basati su un più ampio e innovativo utilizzo delle informazioni.

Naturalmente, come già osservato a proposito del DGA, l'applicazione del DA non deve confliggere con l'osservanza della disciplina in materia di tutela dei dati personali e della vita privata. Pertanto, anche in questa circostanza, il GDPR prevale automaticamente in caso di contrasto (Art. 1(5) DA).

Il Data Act è diviso in 6 Capi. Facendo seguito al primo Capo, destinato a definire lo scopo oggettivo del regolamento e le definizioni, alcune porzioni del testo normativo meritano attenzione specifica:

Il Capo II, disciplina l'accesso e l'utilizzo dei dati generati da prodotti connessi o dai relativi servizi, imponendo obblighi di trasparenza e accessibilità verso l'utente finale. Garantisce, inoltre, il diritto dell'utente a condividere tali dati con terzi, introduce diritti e doveri per titolari, utenti e terzi coinvolti.

Il Capo III definisce le condizioni per rendere disponibili i dati quando previsto dalla normativa UE. Esso comprende norme che regolano l'equo compenso per l'ottenimento dei dati, le misure di protezione tecnica contro gli utilizzi non autorizzati dei dati, e la risoluzione di controversie relative ai trasferimenti dei dati¹⁶.

¹⁵ F. CASOLARI, C. BUTTABONI, L. FLORIDI, *The EU Data Act in context: a legal assessment*, in *International Journal of Law and Information Technology*, 2023, pp. 399-412.

¹⁶ L. PASERI, S.G. VERHULST, *Unpacking B2G data sharing mechanism under the EU Data Act*, in *BioLaw Journal – Rivista di BioDiritto*, 2025, pp. 259-273.

Il Capo IV affronta i contratti tra imprese, vietando l'imposizione unilaterale di clausole contrattuali inique che possano compromettere l'accesso o l'uso dei dati, tutelando le piccole e medie imprese e la concorrenza nel mercato.

Il Capo V regola la messa a disposizione di dati non personali (e, se necessario, anche personali anonimizzati) a enti pubblici e istituzioni UE in situazioni eccezionali (es. emergenze, pandemie), delineando le modalità di richiesta, di compensazione per i titolari dei dati e l'utilizzo ed eventuale condivisione con enti di ricerca.

Il Capo VIII introduce requisiti per garantire l'interoperabilità dei dati, dei meccanismi di condivisione, dei servizi e degli Spazi Comuni Europei dei dati e comprende norme sugli standard per *smart contracts* che eseguono accordi di condivisione dei dati.

La disamina che segue introduce alcuni aspetti essenziali alla comprensione di importanti fenomeni informatico-giuridici relativi agli spazi di dati.

4.1 Data Act e prodotti connessi: definizioni essenziali

Prima di entrare nel merito della disciplina, è opportuno chiarire il perimetro applicativo del Capo II. Per farlo, è necessario identificare alcune importanti definizioni contenute al Capo I.

Un *prodotto connesso* è un dispositivo fisico che ottiene, genera o raccoglie dati in relazione al proprio funzionamento, all'uso che ne viene fatto o all'ambiente in cui è collocato. Rientrano in questa categoria, ad esempio, gli oggetti dell'Internet of Things, come veicoli, elettrodomestici intelligenti o macchinari industriali. I *dati del prodotto* sono i dati generati dal funzionamento o dall'utilizzo del prodotto connesso, oppure ottenuti attraverso sensori e altri meccanismi integrati nello stesso dispositivo. Questi dati possono riguardare sia l'oggetto in sé, sia le condizioni di utilizzo e l'ambiente circostante. Un *servizio correlato* è un servizio digitale, tipicamente un software o un'applicazione, che interagisce con il prodotto connesso per abilitare funzionalità aggiuntive, migliorarne le prestazioni o consentire servizi di supporto. Esempi possono essere app (o altri software) di controllo remoto, sistemi di diagnostica o piattaforme di monitoraggio del dispositivo. Infine, i *dati di un servizio correlato* sono i dati generati o acquisiti attraverso l'uso del servizio correlato da parte dell'utente, spesso in combinazione con il prodotto connesso. Tali dati riflettono sia l'interazione dell'utente con il software, sia le informazioni elaborate a partire dal prodotto e dal suo contesto operativo.

La definizione di *dato personale* ha lo stesso significato attribuito dal Regolamento (UE) 2016/679 (GDPR), ossia qualsiasi informazione riguardante una persona fisica identificata o identificabile (Art. 4 GDPR). Anche la categoria

dell'*interessato* al trattamento coincide con quella del GDPR, e individua la persona fisica alla quale i dati personali si riferiscono.

È *utente*, invece, la persona fisica o giuridica che possiede un prodotto connesso o a cui sono stati trasferiti contrattualmente diritti temporanei di utilizzo di tale prodotto connesso o che riceve un servizio correlato. Differisce dal GDPR (non senza sovrapposizione terminologica con quest'ultimo, in maniera non dissimile da quanto osservato rispetto al DGA), la definizione di *titolare dei dati* (nel GDPR, *titolare del trattamento*). Per il DA, questa figura è la persona fisica o giuridica, l'autorità pubblica, l'agenzia o altro organismo che ha il diritto o l'obbligo, in forza della legge o di un contratto, di utilizzare e mettere a disposizione determinati «dati del prodotto o di un servizio correlato che ha reperito o generato nel corso della fornitura di un servizio correlato»¹⁷. È, invece, *destinatario dei dati* la “persona fisica o giuridica, che agisce per fini connessi alla sua attività commerciale, imprenditoriale, artigianale o professionale, diversa dall'utente di un prodotto connesso o di un servizio correlato, a disposizione della quale il titolare dei dati mette i dati, e che può essere un terzo [...]”.

4.2. Data Act e prodotti connessi: regime giuridico

Il Capo II del Data Act stabilisce il regime giuridico dei dati generati dai prodotti connessi e dai servizi correlati. Gli utenti (siano essi persone fisiche o giuridiche) che possiedono, prendono in leasing o utilizzano un prodotto connesso hanno il diritto di accedere direttamente, facilmente, gratuitamente e in tempo reale ai dati generati dal prodotto, compresi i metadati necessari per interpretarli (Art. 4(1) DA). I dati devono essere forniti in formato completo, strutturato, di uso comune e leggibile da dispositivo automatico (Art. 3(1) DA) e, quando tecnicamente possibile, l'accesso deve essere garantito in forma diretta dal prodotto all'utente (Art. 3(2) DA), ossia tramite un'interfaccia prontamente disponibile.

Prima della conclusione di un contratto di acquisto, locazione o leasing, il fabbricante o fornitore deve informare l'utente sul tipo, formato e volume stimato dei dati generati, sulla possibilità di generazione in tempo reale, sulla destinazione di conservazione (locale o remota), nonché sulle modalità di accesso, recupero o cancellazione (Art. 3(3) DA).

L'utente ha inoltre il diritto di condividere i dati con terze parti di sua scelta, anche a fini di servizi post-vendita, fermo restando l'obbligo di rispettare gli accordi di riservatezza e il divieto per la terza parte di utilizzare i dati per lo sviluppo di prodotti concorrenti (Art. 6(2) e 6(3)(a) DA). Per garantire un equi-

¹⁷ *Infra* par. 4.3.

librio e maggiore concorrenza, il legislatore ha previsto che le micro, piccole e medie imprese siano esentate da alcuni obblighi più onerosi (Art. 7 DA).

La *ratio* del quadro giuridico così ricostruito può essere rintracciata nella necessità di prevenire fenomeni di *lock-in* tecnologico, ossia garantire che i dati generati dai prodotti connessi non restino confinati in un modello chiuso e proprietario, ma possano essere effettivamente accessibili e riutilizzabili a beneficio degli utenti e, più in generale, dell'innovazione dell'ecosistema digitale, ad esempio anche attraverso i *data spaces*. In particolare, il legislatore europeo sottolinea che i dati hanno un valore economico e sociale crescente, e che il loro utilizzo può stimolare la concorrenza, migliorare i servizi post-vendita e promuovere nuovi modelli di business (Cons. 5 e 6 DA).

La norma si fonda, inoltre, su un principio di riequilibrio contrattuale. L'utente, che è parte attiva e integrante nella generazione dei dati tramite l'uso del prodotto connesso o dei servizi ad esso correlati, deve poter esercitare un controllo effettivo su tali dati, superando le asimmetrie informative e di potere rispetto ai produttori (Cons. 14 DA). Allo stesso tempo, il DA non distoglie l'attenzione dagli interessi legittimi dei produttori, garantendo la protezione dei segreti commerciali e dei diritti di proprietà intellettuale (Cons. 28 e 29 DA).

4.3. Data Act e condivisione di dati su richiesta delle autorità

Il Capo V del Data Act istituisce un quadro armonizzato per permettere agli enti pubblici degli Stati membri e ad alcune istituzioni, agenzie e organi dell'UE di accedere ai dati personali o non personali detenuti da soggetti privati, in presenza di una necessità eccezionale, limitata nel tempo. L'art. 15(1) DA descrive due possibili fattispecie. La lett. a) riguarda i dati personali e si applica solo in presenza di una situazione eccezionale dichiarata ufficialmente (emergenze pubbliche, catastrofi, crisi di cybersicurezza), quando i dati siano indispensabili per affrontarla. La lett. b) invece riguarda i dati non personali e si applica in contesti non emergenziali, quando un compito di interesse pubblico non può essere svolto senza quei dati e l'autorità ha già esaurito tutti i mezzi alternativi.

Per le richieste *ex art.* 15(1)(a) DA concernenti dati personali, la ricorrenza di una necessità eccezionale avviene se alcuni elementi si verificano congiuntamente:

- il verificarsi di una situazione eccezionale, limitata nel tempo, come un'emergenza di sanità pubblica, un'emergenza derivante da calamità naturali, una grave catastrofe di origine antropica, compreso un grave incidente di cibersicurezza,
- un presumibile impatto negativo della situazione eccezionale sulla popolazione (dell'Unione o di uno Stato membro), con il possibile rischio di

ripercussioni gravi e durature sulle condizioni di vita o sulla stabilità economica, sulla stabilità finanziaria, o di un sostanziale e immediato degrado delle risorse economiche, e

- la determinazione o dichiarazione ufficiale da parte delle autorità nazionali o europee della situazione di crisi, in conformità alle norme applicabili,
- la necessità dei dati, da parte dell'ente pubblico o di un'altra istituzione, detenuti da un soggetto privato, non ottenibili con mezzi equivalenti.

Invece, *ex art. 15(1)(b) DA*, per ciò che attiene ai soli dati non personali e in situazioni diverse da quelle dell'emergenza pubblica, qualora un compito d'interesse pubblico non possa essere svolto dall'istituzione pubblica e quest'ultima abbia esaurito tutti gli altri mezzi a sua disposizione per ottenere tali dati, incluso l'acquisto sul mercato ai prezzi, il ricorso a norme o la predisposizione di altre misure che possano consentire il reperimento dei dati.

L'istituzione pubblica deve presentare una richiesta scritta al titolare dei dati e deve includere elementi quali i dati oggetto della richiesta, compresi i metadati pertinenti necessari per interpretare e utilizzare tali dati l'indicazione puntuale della necessità eccezionale per cui si richiedono i dati, lo scopo in concreto della richiesta e il termine entro il quale soddisfarla. La richiesta deve essere scritta in maniera chiara e comprensibile al titolare, e presentare carattere di proporzionalità rispetto alla granularità e il volume dei dati richiesti. La richiesta deve essere notificata all'autorità competente per la protezione dei dati personali se ad essere demandati sono anche dati personali (art. 17 DA)

Ai sensi dell'art. 18 DA, il titolare dei dati può formalmente rifiutarsi qualora a) non sia in possesso dei dati richiesti, b) ritenga che la richiesta sia stata reiterata, che la precedente sia stata soddisfatta e che il suo scopo non sia terminato, indicando la richiesta precedente o c) ritenga che la richiesta non soddisfi i requisiti di cui all'art. 17 appena discussi. L'istituzione pubblica può contestare il diniego della richiesta, sottoponendo la questione all'autorità competente designata dallo Stato Membro.

Le istituzioni che ricevono le informazioni possono utilizzare i dati unicamente per la finalità specifica indicata nella richiesta e non per scopi ulteriori o incompatibili, sono tenuti ad adottare misure tecniche e organizzative idonee a garantirne la riservatezza, l'integrità e la sicurezza, e hanno l'obbligo di cancellarli una volta che la finalità originaria sia stata raggiunta, salvo gli obblighi di conservazione derivanti dal diritto dell'Unione o nazionale in materia di trasparenza e accesso ai documenti. Inoltre, non è consentito impiegare tali dati, né le informazioni economiche o produttive ad essi connesse, per sviluppare o migliorare prodotti o servizi in concorrenza con quelli del titolare dei dati, né condividerli con terzi per tali scopi. La divulgazione di segreti commerciali è am-

messa soltanto nella misura strettamente necessaria alle finalità istituzionali della richiesta e deve essere accompagnata da garanzie adeguate, incluse clausole contrattuali e codici di condotta che ne assicurino la protezione. In ogni caso, la responsabilità ultima per la sicurezza dei dati rimane sempre in capo all'ente ricevente.

Ai sensi dell'art. 20 DA, nel rispondere alle richieste *ex art.* 15(1)(a), i titolari (ad eccezione delle microimprese e delle piccole imprese) devono mettere a disposizione i dati all'istituzione pubblica gratuitamente e "senza indebito ritardo, tenendo conto delle misure tecniche, organizzative e giuridiche necessarie". Invece, tutti i titolari dei dati hanno diritto a ricevere un compenso equo per la messa a disposizione dei dati ai sensi dell'art. 15(1)(b). Tale compenso deve coprire i costi tecnici e organizzativi sostenuti per evadere la richiesta, inclusi, se necessari, quelli relativi ad anonimizzazione, pseudonimizzazione, aggregazione e adeguamenti tecnici, nonché garantire un margine ragionevole.

Nell'adempire alla richiesta, qualora questa contenga dati personali, il titolare dei dati è tenuto ad anonimizzarli, salvo che la richiesta imponga la condivisione di dati personali. In tal caso, il titolare dei dati li pseudonimizza prima di condividerli (art. 18(4) DA).

4.4. Data Act e interoperabilità nei Data Spaces

Il Capitolo VII del Data Act mira ad una duplice finalità: da un lato, assicurare che i dati possano circolare senza ostacoli tecnici o giuridici attraverso diversi settori e Stati membri all'interno degli Spazi Comuni Europei dei dati; dall'altro, rafforzare la fiducia degli operatori che in essi condividono i dati, fornendo garanzie di trasparenza, qualità e sicurezza.

L'articolo 33 introduce in particolare i requisiti tecnici per i *data spaces*. Essi rispondono alla necessità, più volte sottolineata nei Considerando (Cons. 62–67 DA), di evitare la frammentazione tecnologica e semantica e di promuovere, al contrario, invece standard e pratiche uniformi per tutti gli attori coinvolti negli scambi di dati.

In primo luogo, chi mette a disposizione dati è tenuto a fornire una descrizione completa in formato *machine-readable*. Tale descrizione deve indicare, tra gli altri:

- il contenuto informativo dei *dataset*,
- le restrizioni all'uso dei dati che possono derivare dalle licenze applicabili ai dataset, diritti di proprietà intellettuale o esigenze di riservatezza, l
- a metodologia di raccolta dei dati,
- la valutazione della qualità dei dati e le eventuali lacune presenti.

La divulgazione di questi elementi non ha carattere meramente formale, ma funzionale a consentire valutazioni affidabili da parte dei potenziali nuovi utilizzatori, a rafforzare la fiducia negli scambi e a favorire la riduzione delle asimmetrie informative (Cons. 64 DA).

Accanto a questo obbligo di trasparenza, l'art. 33 DA impone anche la pubblicazione delle strutture dei dati e dei metadati: i fornitori devono rendere note le architetture informative adottate, i formati utilizzati, i vocabolari semantici, gli schemi di classificazione, e le tassonomie impiegate. La *ratio* della disposizione è quella di permettere agli attori coinvolti nello scambio di dati e, in particolare, agli utenti, di comprendere come i dati sono strutturati e organizzati, assicurando compatibilità semantica e riducendo i costi di adeguamento alla nuova struttura del dataset. In questo modo, si realizza nella pratica l'obiettivo dei Considerando di garantire un "linguaggio comune" tra diversi settori e applicazioni (Cons. 63 DA).

Un ulteriore elemento di rilievo riguarda la descrizione dei mezzi tecnici di accesso. I titolari dei dataset devono rendere noto in che modo i dati possano essere effettivamente ottenuti, indicando, ad esempio, le API (*Application Programming Interfaces*), i protocolli di *query* (interrogazione del database), le piattaforme e gli altri strumenti messi a disposizione degli utenti.

Devono, inoltre, essere resi noti i relativi termini e condizioni d'uso, affinché gli utenti sappiano in anticipo quali siano le modalità di accesso e le eventuali limitazioni all'uso dei dati. L'articolo specifica che, ove tecnicamente possibile, deve essere consentito sia il download in blocco (*batch* o *bulk download*) sia l'accesso in tempo reale, rispondendo così a esigenze diverse: da un lato, consentendo l'analisi delle serie storiche di dati, dall'altro, facilitando l'alimentazione di servizi digitali dinamici che agiscono in tempo reale.

L'ultimo aspetto disciplinato riguarda la interoperabilità degli strumenti per l'esecuzione degli accordi di condivisione dei dati. L'art. 33 prevede infatti che, ove applicabile, siano forniti mezzi che assicurino la compatibilità tecnica degli strumenti impiegati per dare attuazione agli accordi che accompagnano la condivisione dei dati. Ciò include anche strumenti basati su tecnologie innovative come gli *smart contracts*, che consentono l'automazione delle condizioni di accesso e uso dei dati, garantendo tracciabilità, sicurezza e verificabilità delle transazioni¹⁸.

La *ratio* complessiva del Capitolo VII si colloca dunque all'interno della più ampia strategia europea di sovranità digitale e di circolazione sicura dei dati. I Considerando chiariscono che, in assenza di regole comuni sui requisiti

¹⁸ C. BOMPRESZI, M. PALMIRANI, *Blockchain technology for legislation: preliminary considerations*, in *Comparazione e Diritto Civile*, 2024, pp. 83-99.

tecniche dei *data spaces*, si rischierebbe la proliferazione di standard proprietari e di soluzioni incompatibili, con il risultato di ostacolare l'emergere di un mercato unico dei dati. Stabilire un quadro armonizzato consente invece di ridurre i costi di transazione, incoraggiare la condivisione, sostenere la competitività delle imprese europee e stimolare l'innovazione in settori chiave come la sanità, i trasporti, l'energia e l'agricoltura e, più in generale, le aree di sviluppo dei *data spaces*.

5. Spazi di Dati e sfide aperte

Nel progetto europeo di mercato unico dei dati, DGA e DA svolgono funzioni complementari e progressive. Il DGA ha messo in piedi l'infrastruttura "fiduciaria" per la condivisione dei dati (riuso di dati pubblici protetti, intermediari neutrali e certificati, l'EDIB e i meccanismi di certificazione). D'altro canto, il DA è intervenuto a valle per rendere effettivo l'accesso e la portabilità dei dati, riequilibrare rapporti contrattuali a beneficio degli utenti dei prodotti connessi, e fissare requisiti di interoperabilità per la circolazione dei dati.

Sinergicamente, i due Regolamenti compongono il binomio fiducia-operatività: il primo crea le regole per l'identificazione di attori affidabili, in grado di assicurare neutralità; il secondo impone diritti, obblighi e standard tecnici perché lo scambio avvenga anche tra settori diversi e oltre i confini nazionali, alimentando così gli obiettivi prefissati dal DGA.

La buona riuscita del tentativo di realizzare gli Spazi Comuni Europei dei Dati necessita di questa complementarità in concreto. Il DGA dovrebbe abilitare gli attori e i processi di governance che possono "alimentare" i *data spaces* con asset informativa affidabili; il DA obbliga i partecipanti ai *data spaces* a descrivere *dataset* e metadati in formati leggibile da macchina, a pubblicare strutture, ontologie e modalità di accesso (API, query, bulk download e accesso real time), e a garantire la compatibilità tecnica degli strumenti che eseguono gli accordi di condivisione (inclusi gli *smart contracts*). Insieme, i regolamenti prevengono frammentazioni semantiche e tecniche, riducono i costi di integrazione e creare un "linguaggio comune" (DA) tra operatori che operano sotto regole comuni e certificati (DGA), naturalmente nel rispetto delle norme a tutela dei dati personali (GDPR). In parallelo, lo sviluppo degli spazi settoriali avanza: lo European Health Data Space (EHDS) ha completato l'iter legislativo con pubblicazione in Gazzetta nel Marzo 2025, aprendo la fase di attuazione che costituisce un banco di prova per interoperabilità, *governance* e

riuso secondario dei dati sanitari, ambiti trazionalmente “critici” nel vasto panorama regolamentare europeo sulla materia¹⁹.

Proprio dagli spazi di dati emergono le sfide aperte che determineranno il successo del quadro. Dal punto di vista giuridico, le sfide emergenti per il prossimo futuro possono essere riassunte in alcuni punti essenziali. In primo luogo, sarà essenziale l'identificazione di modelli di *business* sostenibili per gli operatori (intermediari, federatori, fornitori di strumenti) coinvolti nello scambio, considerati i costi di allineamento e mantenimento della *compliance*; secondariamente, una sfida cruciale è posta dalla necessaria convergenza applicativa tra DGA e DA, da un lato, e normative orizzontali (GDPR, tutela giuridica delle banche dati, etc.), dall'altro; inoltre, la capacità tecnica di abilitare accesso in tempo reale e *bulk download* non dovrà sacrificare sicurezza e riservatezza, che minerebbero non solo gli sforzi di compliance (si pensi ai costi legati alle sanzioni comminate in conseguenza di un *data breach*), ma anche quelli della credibilità generale degli istituti del DGA e del DA.

L'Europa ha inteso costruire una catena normativa volutamente coerente: il DGA istituisce la fiducia e i ruoli per condividere; il DA vincola a condividere secondo criteri di equità e interoperabilità; i *data spaces* sono il campo di gioco dove questa catena deve funzionare. La stagione normativa che si apre richiederà uno sforzo coordinato di implementazione: linee guida e standard tecnici, registrazione e vigilanza effettiva degli intermediari, *governance* trasparente, strumenti e rimedi contrattuali dovranno lavorare sinergicamente. Se questo accadrà, i *data spaces* potranno realmente coniugare sovranità dei dati, concorrenza e innovazione, trasformando regole astratte in valore aggiunto per imprese, PA e cittadini.

¹⁹ G. BINCOLETTI, *Scientific research processing health data in the European Union: data protection regime vs. open data*, in *Journal of Open Access Law*, 2023, p. 1.

L'USO SECONDARIO DEI DATI SANITARI ELETTRONICI NELLA CORNICE DELL'*EUROPEAN HEALTH DATA SPACE*

Paola Aurucci

SOMMARIO: 1. Introduzione. 2. Stato dell'arte: le barriere normative al riutilizzo dei dati sanitari per finalità di ricerca biomedica nel quadro giuridico europeo. 3. Evoluzione normativa: la disciplina dell'uso secondario dei dati sanitari elettronici nello Spazio europeo dei dati sanitari. 4. Problematiche attuali: criticità giuridiche e rischi di arretramento della tutela nell'EHDS. 5. Conclusioni.

1. Introduzione

L'11 febbraio 2025 è stato approvato il Regolamento (UE) 2025/327 sullo Spazio europeo dei dati sanitari, meglio conosciuto con l'acronimo inglese di *European Health Data Space*, "EHDS"¹, la cui proposta risale al 2022². L'EHDS rappresenta il primo atto normativo di attuazione di quanto previsto dalla Commissione nella Strategia europea dei dati del 2020³, con riferimento all'istituzione di spazi comuni e interoperabili di dati a livello dell'Unione⁴ in settori economici specifici e ambiti di interesse pubblico⁵. Tali spazi mirano a promuovere la circolazione e il riuso dei dati, attraverso il combinato disposto di strumenti tecnici, infrastrutture sicure, norme comuni, procedure standardizzate e meccanismi di *governance* affidabili⁶. L'obiettivo ultimo è che gli spazi europei dei dati di ambiti specifici – tra cui, oltre a quello sanitario, si annoverano, a titolo esemplificativo e non esaustivo, quelli finanziario, manifatturiero, della

¹ Regolamento (UE) 2025/327 del Parlamento europeo e del Consiglio, dell'11 febbraio 2025, sullo Spazio europeo dei dati sanitari (European Health Data Space – EHDS), GU L 327 del 21.2.2025, pp. 1–96.

² Proposta di regolamento del Parlamento europeo e del Consiglio sullo Spazio europeo dei dati sanitari (European Health Data Space – EHDS), COM (2022) 197 final, 3.5.2022, pp. 1-105.

³ Commissione europea, Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni: Una strategia europea per i dati (Bruxelles, 19 febbraio 2020) COM (2020) 66 final, pp.1-38.

⁴ *Ibid.*, p. 19.

⁵ *Ibid.*, p. 24.

⁶ *Ibid.*

mobilità, dell'energia e della pubblica amministrazione⁷ – confluiscono nel loro insieme in un unico spazio europeo, dove dati personali e no, possano circolare liberamente tra settori diversi e Stati membri, configurando un autentico mercato unico digitale⁸. Questi spazi sono quindi destinati a costituire gli assi portanti di un'economia europea dei dati improntata al pieno rispetto dei valori e del diritto dell'Unione, in particolare alla normativa in materia di protezione dei dati personali, tutela dei consumatori e diritto della concorrenza⁹.

La politica europea dei dati si distingue, in tal senso, tanto dall'approccio statunitense, caratterizzato dalla centralità delle dinamiche di mercato e dell'iniziativa privata, sia da quello cinese, di impronta statale e funzionale alla preservazione del potere politico, orientandosi invece verso un bilanciamento tra sviluppo tecnologico e tutela dei diritti fondamentali¹⁰ così da «preservare le strutture democratiche della società e garantire un'equa distribuzione dei benefici dell'economia digitale»¹¹.

Nella programmazione strategica europea, il settore sanitario ha assunto fin da subito un rilievo prioritario¹². Nell'ottica del legislatore europeo la crescente digitalizzazione dei dati sanitari e l'accesso sicuro alle cartelle cliniche elettroniche, sia da parte dei singoli, sia degli operatori medici, sono destinati a migliorare l'assistenza clinica, garantendo al contempo la continuità delle cure in caso di mobilità transfrontaliera, e a favorire il perseguimento di obiettivi di medicina personalizzata¹³. Inoltre, lo scambio e il riutilizzo sicuro di dati sanitari elettro-

⁷ Nella «Strategia europea per i dati» del 2020 la Commissione europea ha individuato nove spazi comuni dei dati riferiti ad ambiti settoriali specifici. Nei successivi documenti di attuazione della Strategia, il numero degli spazi è stato progressivamente ampliato fino a quattordici. *Staff Working Document on the implementation of the European data strategy*, SWD(2022) 45 final, Bruxelles, 23 febbraio 2022, pp. 1–35; Commissione europea, *Staff Working Document on the implementation of the European data strategy – Common European Data Spaces*, SWD(2023) 45 final, Bruxelles, 1 febbraio 2023, pp. 1–38.

⁸ L. PASERI, *Il governo dei dati. Interesse pubblico, altruismo e partecipazione*, Torino: Giappichelli, 2025.

⁹ Commissione europea, *Common European Data Spaces*, reperibile online sul sito: <https://digital-strategy.ec.europa.eu/en/policies/data-spaces>.

¹⁰ U. PAGALLO, *The politics of data in EU law: Will it succeed?*, in *Digital Society*, 2002 (1, 3), pp. 1–20.

¹¹ A. BRADFORD, *Digital Empires. The Global Battle to Regulate Technology*, Oxford: OUP, 2023.

¹² La priorità attribuita dal Consiglio europeo alla creazione di uno spazio europeo dei dati sanitari trova fondamento nell'esperienza pandemica del COVID-19, che ha evidenziato la necessità di un accesso tempestivo e della condivisione transfrontaliera dei dati sanitari elettronici per finalità di cura, contenimento dell'emergenza sanitaria e ricerca. Si veda COM (2022) 197, p. 1.

¹³ Nell'ambito della «Strategia europea dei dati», la medicina personalizzata è intesa come un modello di assistenza fondato sull'uso sistematico dei dati sanitari, che consente di “adeguare la strategia terapeutica giusta alle esigenze della persona giusta al momento giusto [...] determinare la predisposizione alla malattia e [...] attuare una prevenzione mirata e tempestiva”. Cfr. COM(2020) 66 final, p. 3.

nici per finalità di ricerca, innovazione e *policy making*, favoriscono lo sviluppo di sistemi diagnostici, terapie, tecnologie e politiche di sanità pubblica efficaci e sostenibili.

Per sbloccare tale potenziale, l'EHDS istituisce uno spazio digitale comune per la raccolta e la condivisione in tutta Europa dei dati sanitari elettronici, necessari all'erogazione di prestazioni sanitarie nei confronti delle persone fisiche. Nell'ambito di questo tipo trattamento, definito «uso primario» dei dati, il nuovo Regolamento rafforza il controllo delle persone fisiche sui propri dati sanitari, potenziando i diritti di accesso e portabilità¹⁴, oltre che intervenendo sull'organizzazione e sull'interoperabilità dei sistemi sanitari digitali. Parallelamente, l'EHDS rende disponibili a ricercatori, decisori politici e altri soggetti sia pubblici che privati tali dati, o altri raccolti appositamente a fini di studio e innovazione, per «uso secondario», cioè per il loro riutilizzo per finalità diverse da quelle originarie ma legate all'interesse della società nel suo complesso, tra cui la ricerca scientifica¹⁵. Un altro obiettivo dell'EHDS è favorire la creazione «di un autentico mercato unico per i servizi e i prodotti di sanità digitale»¹⁶ a garanzia della competitività globale dell'Unione.

Il Regolamento segna così un cambio di paradigma nella politica europea dei dati, avviato dalla Commissione nel 2020, nel quale al primato assiologico e normativo della protezione dei dati personali si affiancano, con pari dignità, le esigenze di accesso, condivisione e riutilizzo dei dati¹⁷, in una logica di complementarità tra il controllo individuale sui flussi informativi sanitari e la massimizzazione del valore pubblico della salute¹⁸.

¹⁴ W. LI, P. QUINN, *The European Health Data Space: An expanded right to data portability?*, in *Computer Law & Security Review*, 2024 (52), art. 105913.

¹⁵ Il fulcro dell'EHDS o è costituito dalla disciplina dell'uso primario e secondario dei dati sanitari elettronici, contenuta nei Capi III e IV, ed è funzionale alla costruzione di un vero e proprio ecosistema europeo dei dati sanitari. Tale obiettivo, inserito nel più ampio progetto della European Health Union (cd. EHU), mira a introdurre una regolazione uniforme a livello dell'Unione, volta a superare le barriere geografiche che ostacolano la libera circolazione dei dati e delle persone. Cfr. P. SCANGA, *Dal soggetto frammentato all'etica della cura. Per una diversa gestione dei dati sanitari*, in *Notizie di Politeia*, 2025 (XLI, 158), pp. 60-72.

¹⁶ Cons. 110, EHDS.

¹⁷ I. RAPISARDA, *Sul costituendo spazio europeo dei dati sanitari*, in *Responsabilità Medica*, 2023 (4), pp. 413-425; G. RESTA, *Health Data in Europe at the Crossroads of Data Protection and Data Sharing*, in M. CATANZARITI ET AL. (eds.), *Data Privacy, Data Property and Data Sharing. An Interdisciplinary Perspective for Post-pandemic Transnational Scientific Research*, Boca Raton: CRC Press, 2025, pp. 211-224.

¹⁸ La salute si configura come valore primario, strumentale alla tutela di una pluralità di situazioni giuridiche soggettive nella sua dimensione individuale e, al contempo, come interesse di natura superindividuale, la cui protezione risponde a esigenze di sanità pubblica e di tutela della collettività. Per un approfondimento, si veda S. RODOTÀ, *Il diritto di avere diritti*, Roma-Bari: Laterza, 2012.

Tale ricalibratura non implica tuttavia un arretramento delle garanzie esistenti. Nella prospettiva del legislatore europeo, l'uso secondario dei dati sanitari deve essere regolato nel pieno rispetto del quadro normativo vigente, e in particolare del GDPR, attraverso soluzioni idonee a realizzare il miglior contemporaneo possibile tra diritti individuali, interessi collettivi e dinamiche di mercato¹⁹. Si tratta di un equilibrio particolarmente delicato, che comporta anche un riassetto del regime della ricerca biomedica²⁰, in cui amministrazioni pubbliche, pazienti, ricercatori e attori privati sono chiamati a cooperare in schemi composti di *governance*²¹.

Il presente capitolo si propone di esaminare le caratteristiche, la portata innovativa e le criticità della disciplina dell'uso secondario dei dati sanitari introdotta dall'EHDS, con particolare attenzione alla finalità di ricerca scientifica. L'analisi prende avvio dal quadro normativo europeo in materia di protezione dei dati personali, al fine di evidenziare come il GDPR, pur riconoscendo uno statuto speciale alla ricerca scientifica, presenti limiti strutturali rispetto alle esigenze di riutilizzo e condivisione dei dati sanitari. Su tale base, l'indagine si concentra sul complesso sistema tecnico-organizzativo e normativo previsto dall'EHDS, con particolare attenzione alla disciplina dell'uso secondario dei dati e del nuovo diritto di esclusione (c.d. *opt-out*) per valutare se il nuovo assetto regolatorio sia in grado di superare le incertezze applicative e la frammentazione normativa esistenti, garantendo al contempo un elevato livello di tutela dei diritti fondamentali e una promozione efficace del progresso scientifico, dell'innovazione e della competitività economica delle imprese europee.

2. Stato dell'arte: le barriere normative al riutilizzo dei dati sanitari per finalità di ricerca biomedica nel quadro giuridico europeo

La ricerca biomedica contemporanea comporta la raccolta, l'utilizzo, la condivisione, il trasferimento, il confronto e la conservazione di ingenti quantità di dati²², anche personali e sensibili, provenienti da fonti eterogenee²³. L'approccio

¹⁹ L. MARELLI ET AL., *The European Health Data Space: Too big to succeed?*, in *Health Policy*, 2023 (135), pp. 1–4.

²⁰ S. SLOKENBERGA, *Scientific research regime 2.0? Transformations of the research regime and the protection of the data subject that the proposed EHDS regulation promises to bring along*, in *Technology and Regulation*, 2022, pp. 135–147; G. GORGONI, *Lo spazio europeo dei dati sanitari e il buon cittadino europeo: fare di virtù necessità?*, in *Notizie di Politeia*, 2025 (XLI, 158), pp. 18–30.

²¹ M. CATANZARITI, *Verso una nuova epistemologia dei dati sanitari: le promesse mancate del secondary use*, in *Notizie di Politeia*, 2025 (XLI, 158), pp. 31–44.

²² P. GUARDA, *Il regime giuridico dei dati della ricerca scientifica*, Napoli: ESI, 2021.

²³ S. LEONELLI, *La ricerca scientifica nell'era dei Big Data*, Milano: Meltemi, 2018; S. SHILO ET AL., *Axes of a Revolution: Challenges and Promises of Big Data in Healthcare*, in *Nature Medicine*, 2020 (26, 1), pp. 29–38.

data-intensive, reso possibile da capacità computazionali sempre più elevate²⁴ e alla disponibilità di infrastrutture digitali, è indispensabile tanto per il conseguimento di scoperte rilevanti ai fini della cura delle malattie, quanto per lo sviluppo di tecnologie digitali, in particolare di sistemi di intelligenza artificiale, la cui operatività è «strutturalmente dipendente dai Big Data»²⁵, necessari per addestrare, validare e far funzionare gli algoritmi. L'ampia adozione di tecnologie digitali nel contesto assistenziale promette di migliorare la prevenzione, la diagnosi e gli esiti clinici per i pazienti²⁶ e di rendere i sistemi sanitari più sostenibili²⁷ dal punto di vista finanziario. Ne discende il ruolo strategico della ricerca quale volano di efficientamento, crescita economica e competitività dell'Unione europea.

Le esigenze della ricerca orientata allo sviluppo di soluzioni tecnologiche complesse, fortemente dinamiche, mettono sotto pressione l'architettura tradizionale del diritto europeo della protezione dati, orientata al contenimento dei flussi informativi²⁸. In particolare, i principi di minimizzazione e di limitazione della finalità di cui all'art. 5 GDPR appaiono sempre meno compatibili con pratiche di ricerca basate sul riutilizzo pervasivo, continuo e potenzialmente illimitato di dati personali, in contesti in cui il valore scientifico dei dati e le finalità di studio non sono sempre pienamente predeterminabili, alimentando un dibattito che ha ormai travalicato l'ambito dottrinale per investire anche la sfera politica²⁹.

Nonostante l'innegabile sforzo compiuto dal legislatore eurounitario volto a garantire, attraverso il GDPR, una disciplina uniforme e, al contempo, volta a conciliare la tutela della persona fisica con riferimento alle informazioni sensibili che la riguardano con l'esigenza di circolazione dei dati per finalità di interesse collettivo³⁰, il quadro normativo risultante ha finito, in alcuni casi, per produrre

²⁴ M. DURANTE, *Potere computazionale: dalle informazioni ai dati*, in M. DURANTE e U. PAGALLO (a cura di) *La politica dei dati. Il governo delle nuove tecnologie tra diritto, economia e società*, Sesto San Giovanni: Mimesis, 2022; L. TRAPANI, *La circolazione dei dati sanitari per uso secondario e la riduzione dei divari*, in *Italian Papers on Federalism*, 2025 (3), pp. 156–175.

²⁵ G. FIORIGLIO, *Trattamento dei dati sanitari e ricerca medica: profili informatico-giuridici e istituzionali nel contesto europeo*, in *Jura Gentium*, 2025 (2), pp. 1–30.

²⁶ Commissione europea, *L'intelligenza artificiale nella salute*, disponibile su: <https://digital-strategy.ec.europa.eu/it/policies/artificial-intelligence-health> (ultimo accesso: 30 gennaio 2026).

²⁷ U. PAGALLO, *Il dovere alla salute. Sul rischio di sottoutilizzo dell'intelligenza artificiale in ambito sanitario*, Sesto San Giovanni: Mimesis, 2022.

²⁸ G. RESTA, *Health Data in Europe at the Crossroads of Data Protection and Data Sharing*, in M. CATTANZARITI ET AL. (eds.), *Data Privacy, Data Property and Data Sharing. An Interdisciplinary Perspective for Post-pandemic Transnational Scientific Research*, cit., pp. 211–224.

²⁹ M. DRAGHI, *The Future of European Competitiveness. Part B: In-depth Analysis and Recommendations*, Rapporto per la Commissione europea, 2024.

³⁰ Il considerando 4 del GDPR sancisce che il diritto alla protezione dei dati personali non costituisce una «prerogativa assoluta», ma deve essere «considerato alla luce della sua funzione so-

effetti opposti rispetto agli obiettivi perseguiti. Nel contesto della ricerca biomedica, oggi prevalentemente multicentrica e globale, caratterizzata dal «trattamento ulteriore» di dati personali raccolti anche al di fuori dei contesti tradizionali di cura o di ricerca e dal crescente coinvolgimento di attori privati portatori di interessi prevalentemente economici³¹, il GDPR ha finito per frenare lo scambio e il trattamento di questi dati da parte dei ricercatori, senza tuttavia riuscire a contrastare in modo pienamente efficace usi distorti, manipolativi o meramente commerciali³² di dati «che concorrono indefettibilmente»³³ alla costruzione dell'identità fisica e sociale dell'interessato. Tale esito appare riconducibile, da un lato, all'incapacità, solo parzialmente giustificata³⁴, del GDPR di prevedere la portata trasformativa dei sistemi di intelligenza artificiale, idonei a «riconfigurare le possibilità epistemiche del patrimonio informativo preesistente»³⁵.

Dall'altro lato il GDPR è andato incontro, a delle criticità strutturali, a iniziare dall'architettura giuridica particolarmente articolata sottesa al trattamento dei dati genetici e relativi alla salute che rientrano nelle «categorie particolari di dati» (Art. 9, par. 1, GDPR). Il Regolamento prevede un divieto generale di trattamento per questi dati, salvo che ricorra una delle deroghe elencate all'art. 9, par. 2. Un ricercatore che intenda condurre uno studio fondato sull'utilizzo di dati sanitari personali, che comporta il trattamento congiunto di dati personali comuni e di categorie particolari di dati³⁶, è tenuto a individuare una base giuridica ai sensi dell'art. 6, par. 1 del GDPR e un'eccezione al divieto di trattamento prevista dall'art. 9, par. 2 del GDPR. In caso di trasferimenti di dati extra EU è

ciale e temperato con altri diritti fondamentali» nel rispetto del principio di proporzionalità di cui all'art. 52, par. 1, della Carta dei diritti fondamentali dell'Unione europea.

³¹ Sebbene il regolamento sia stato elaborato in una fase storica in cui la portata trasformativa dei sistemi di intelligenza artificiale non era ancora pienamente manifesta, già al momento della sua adozione erano noti fenomeni quali la profilazione avanzata, l'inferenza di informazioni ulteriori e l'estrazione di conoscenza dai dati, idonei a mettere in discussione una concezione meramente statica del trattamento del patrimonio informativo. P. AURUCCI, *Salute e scienza*, in M. DURANTE e U. PAGALLO (a cura di), *La politica dei dati. Il governo delle nuove tecnologie tra diritto, economia e società*, Sesto San Giovanni: Mimesis, 2022, pp. 15–36.

³² A. BUSACCA, *I beni digitali nella tassonomia dei beni giuridici*, Bari: Cacucci, 2023; G. RESTA, *Health Data in Europe at the Crossroads of Data Protection and Data Sharing*, cit.

³³ M. GRANIERI, *Il trattamento di categorie particolari di dati personali nel Reg. UE 2016/679*, in *Le nuove leggi civili commentate*, 2017 (I), pp. 165–190.

³⁴ P. AURUCCI, *Il trattamento dei dati personali nella ricerca biomedica. Problematiche etico-giuridiche*, Napoli: Edizioni Scientifiche Italiane, 2022.

³⁵ G. FIORIGLIO, *Trattamento dei dati sanitari e ricerca medica: profili informatico-giuridici e istituzionali nel contesto europeo*, cit.

³⁶ G. BINCOLETTO, *Health Data Sharing for Scientific Research: Closing Data “As Necessary” and Opening it “As Possible”*, in *Data Privacy, Data Property, and Data Sharing. An Interdisciplinary Perspective for Post-pandemic Transnational Scientific Research*, a cura di F. CATANZARITI, F. INCARDONA, G. RESTA, A. SÖNNERBORG, Boca Raton: CRC Press, 2025, pp. 225–254.

poi necessario rispettare una delle condizioni elencate agli artt. 44–49 del GDPR. Tra le condizioni di liceità previste per il trattamento delle categorie particolari di dati, una è dedicata espressamente alla finalità di ricerca scientifica (art. 9, par. 2, lett. j) GDPR), la cui operatività è tuttavia rimessa al diritto dell'Unione o degli Stati membri, chiamati a individuare in una disposizione normativa *ad hoc* delle «misure appropriate e specifiche a tutela dei diritti fondamentali e degli interessi dell'interessato», a cui assoggettare questi trattamenti, che si aggiungono a quelle tecniche e organizzative richieste direttamente dal GDPR all'art. 89, par. 1³⁷, che richiama espressamente il ricorso alla pseudonimizzazione dei dati, quando l'uso di dati anonimi o anonimizzati non permette di raggiungere gli scopi della ricerca.

La possibilità di introdurre una base giuridica normativa specifica per i trattamenti a fini di ricerca scientifica non è stata sfruttata da oltre la metà degli Stati membri, che hanno preferito fare stretto affidamento alle basi giuridiche direttamente previste dal GDPR, ricorrendo in particolare al consenso esplicito dell'interessato, per procedere con il riutilizzo dei dati personali ai fini della ricerca scientifica. Questa scelta, tuttavia, non favorisce il riutilizzo dei dati per finalità di ricerca, poiché la riacquisizione del consenso per nuovi scopi scientifici via via identificati risulta spesso impraticabile e, anche in ragione della sua revocabilità, può introdurre distorsioni idonee a compromettere la continuità dello studio e l'affidabilità dei risultati scientifici.

La predilezione del consenso quale base giuridica per il riutilizzo dei dati dipende dalla centralità assegnata a livello europeo alla protezione dei dati personali, già richiamata in apertura. La tutela dei dati personali a livello europeo è caratterizzata da un approccio prevalentemente individualistico anche con riguardo ad ambiti come la ricerca scientifica, in cui il valore conoscitivo deriva dal trattamento sistematico di grandi insiemi di dati e, spesso, in assenza di una reale possibilità per il titolare del trattamento di ricondurre il singolo dato a una persona identificabile. Sotto un profilo sostanziale, il dato relativo alla salute, per la natura delle informazioni che veicola e per gli interessi sottesi al suo utilizzo, non appare pienamente riconducibile a un paradigma privatistico fondato sul consenso, ma si colloca piuttosto all'interno di una dimensione solidaristico-pubblicistica, funzionale alla tutela della salute collettiva, al progresso scientifico e all'efficienza dei sistemi sanitari.

³⁷ In virtù del *favor* del GDPR per la ricerca scientifica, i trattamenti ad essa finalizzati sono subordinati all'adozione di «garanzie adeguate», tra cui misure tecniche e organizzative volte a garantire il rispetto dei principi del Regolamento, con un'attenzione particolare al principio di minimizzazione, per cui è suggerito l'uso di dati anonimi o anonimizzati e, in via residuale, la pseudonimizzazione.

Un'altra criticità del GDPR che ha finito per ostacolare l'utilizzo secondario dei dati personali per finalità di ricerca riguarda la vaghezza di alcune disposizioni normative e lo scarso coordinamento tra *considerando* e articoli, che ha condotto ad un'interpretazione restrittiva da parte delle due autorità garanti europee³⁸. Sulla base del principio di limitazione della finalità, è stabilito in termini generali che i dati personali siano raccolti per finalità determinate, esplicite e legittime e successivamente trattati in modo compatibile con tali finalità. L'art. 5, par. 1, lett. b) GDPR introduce una «presunzione di non incompatibilità» per l'ulteriore trattamento a fini di ricerca scientifica, apparentemente attenuando l'obbligo, previsto dall'art. 6, par. 4, di svolgere un test di compatibilità caso per caso. Secondo l'orientamento del Garante europeo, il test di compatibilità resta opportuno quando i dati siano stati raccolti per finalità molto diverse dalla ricerca e se usati in studi biomedici. Analoghe interpretazioni restrittive emergono in relazione alla possibilità di sfruttare per il riutilizzo dei dati sanitari le condizioni di liceità che hanno consentito la raccolta iniziale (considerando 50, GDPR), in particolare quella connessa alle finalità di cura (art. 9, par. 2, lett. h) GDPR). L'acquisizione legittima di dati sanitari per scopi assistenziali non può legittimare il successivo trattamento per finalità di ricerca scientifica. Quest'ultima richiede una base normativa specifica, sia essa europea o nazionale, ai sensi del già visto art. 9, par. 2, lett. j) o dell'art. 9, par. 2, lett. g) (trattamenti necessari per motivi di interesse pubblico rilevante). Inoltre, il GDPR fa riferimento alla possibilità per gli interessati di prestare il proprio consenso a determinati ambiti di ricerca scientifica, se al momento della raccolta dei dati non è possibile individuare le finalità specifiche (considerando 33 GDPR). Tale possibilità, tuttavia, resta confinata dall'interpretazione dell'EDPB³⁹ a ipotesi residuali ed è subordinata all'adozione di garanzie ulteriori, in particolare alla raccolta progressiva di consensi specifici per le finalità del trattamento via via individuate nell'ambito dello stesso progetto o di progetti connessi, nel rispetto dei requisiti di specificità e granularità del consenso di cui all'art. 4, n. 11, e all'art. 6, par. 1, lett. a), GDPR. Infine, il ruolo attribuito dal GDPR al legislatore nazionale nel determinare il punto di bilanciamento tra tutela dei diritti degli interessati ed esigenze della ricerca scientifica ha prodotto un elevato grado di frammentazione normativa. In particolare, soluzioni eterogenee a livello nazionale sono dipese sia dalla facoltà riconosciuta agli Stati membri di mantenere o

³⁸ European Data Protection Board (EDPB) e European Data Protection Supervisor (EDPS).

³⁹ EDPB, *Linee guida 5/2020 sul consenso ai sensi del regolamento (UE) 2016/679*, par. 7.2, note 152- 162, pp. 33-35; EDPB, *Documento del Comitato europeo per la protezione dei dati sulla risposta alla domanda di chiarimenti della Commissione europea in merito all'applicazione coerente del GDPR, con un'attenzione particolare alla ricerca in campo sanitario*, par. 4, note 25-31, pp. 7-9.

introdurre ulteriori condizioni, comprese limitazioni, al trattamento dei dati genetici e di quelli relativi alla salute (art. 9, par. 4, GDPR), sia dalla possibilità di limitare l'esercizio di taluni diritti degli interessati nei trattamenti per finalità di ricerca scientifica (art. 89, par. 2, GDPR). Ne risulta un quadro normativo frammentato che crea barriere burocratiche e costi aggiuntivi per i ricercatori e costituisce un ostacolo allo svolgimento di studi multicentrici e internazionali.

3. Evoluzione normativa: la disciplina dell'uso secondario dei dati sanitari elettronici nello Spazio europeo dei dati sanitari

L'articolato impianto normativo sopra delineato, pur formalmente orientato al perseguimento dell'obiettivo dell'Unione di istituire uno Spazio europeo della ricerca in cui «i ricercatori, le conoscenze scientifiche e le tecnologie circolino liberamente»⁴⁰, non ha sino ad oggi favorito un effettivo riutilizzo dei dati sanitari, finendo anzi per ostacolarne la circolazione per finalità scientifiche⁴¹. L'EHDS punta a superare tali criticità, mettendo a disposizione di soggetti pubblici e privati (cons. 61, EHDS) che operano nell'UE un *pool* massivo di dati sanitari digitali⁴², inserito in uno spazio interoperabile comune, dedicato alla ricerca e per una pluralità di finalità di interesse generale. Tale obiettivo è perseguito attraverso una struttura giuridica «ibrida», che si pone l'obiettivo di superare il modello di riutilizzo e *data sharing* adottato sotto l'egida del GDPR. Secondo alcuni studiosi, si assisterebbe a una vera e propria riqualificazione giuridica dei dati sanitari, pur restando, almeno nelle intenzioni dichiarate, integralmente conforme alla disciplina del GDPR⁴³. Per chiarire i termini del problema, è opportuno rilevare che il nuovo Regolamento si inserisce nel più ampio assetto delineato dal Data Governance Act⁴⁴ e dal Data Act⁴⁵, rispetto ai quali si comporta come *lex specialis* per il settore sanitario⁴⁶, volto a rendere operativo⁴⁷

⁴⁰ Il considerando 159 del GDPR chiarisce che la nozione di «finalità scientifica» nel trattamento dei dati personali deve essere interpretata in senso ampio, alla luce dell'obiettivo dell'Unione di istituire uno Spazio europeo della ricerca, richiamando espressamente l'articolo 179, paragrafo 1, TFUE.

⁴¹ L. TRAPANI, *La circolazione dei dati sanitari per uso secondario e la riduzione dei divari*, cit.

⁴² S. THOBANI, *Verso il regolamento UE sullo spazio europeo dei dati sanitari (European Health Data Space)*, in *Persona e Mercato*, 2024 (4, 1), pp. 1393-1399.

⁴³ M. CATANZARITI, *Verso una nuova epistemologia dei dati sanitari*, cit.

⁴⁴ Regolamento (UE) 2022/868 del Parlamento europeo e del Consiglio, del 30 maggio 2022, relativo alla governance europea dei dati e che modifica il regolamento (UE) 2018/1724 (Data Governance Act), GU L 152 del 3.6.2022, pp. 1-44.

⁴⁵ Regolamento (UE) 2023/2854 del Parlamento europeo e del Consiglio, del 13 dicembre 2023, recante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo (Data Act), GU L 2854 del 22.12.2023, pp. 1-58.

⁴⁶ Data Act e Data Governance Act hanno portata generale e orizzontale: il primo rafforza la portabilità di alcune categorie di dati, potenzialmente anche sanitari, mentre il secondo «stabilisce

«un quadro coerente, affidabile ed efficiente per il riutilizzo dei dati sanitari in ambiti quali la ricerca, l'innovazione, l'elaborazione delle politiche e le attività normative» (cons. 110 EHDS).

Per queste «finalità di uso secondario» (cons. 63 EHDS), l'EHDS rinvia come propria base giuridica agli artt. 9, par. 2, lett. g) o j) del GDPR (v. *supra*). Su questa base giuridica, quindi il consenso individuale non appare requisito necessario per il trattamento legittimo dei dati sanitari: la legittimazione normativa va ricercata negli interessi pubblici in gioco e accompagnata da garanzie rafforzate.

Altra novità dell'EHDS riguarda un meccanismo comune di accesso e condivisione dei dati (cons. 52). Tale meccanismo si fonda sui diritti di accesso riconosciuti agli «utenti dei dati» secondo le condizioni definite dagli obblighi di condivisione stabiliti dall'art. 60 EHDS. Gli obblighi gravano sui «titolari dei dati» e organismi pubblici⁴⁸. Questi sono designati a livello statale⁴⁹, e decidono *inter alia*, sul rilascio di autorizzazioni amministrative all'accesso ai dati in spazi di trattamento sicuri (artt. 57, 68 e 73 EHDS)⁵⁰.

Per cogliere la portata di questo meccanismo comune di accesso e condivisione, è opportuno però delimitare l'ambito oggettivo di applicazione della disciplina dell'uso secondario dei dati sanitari. Quest'ultimo è definito dal Regolamento come il trattamento di dati sanitari elettronici «per finalità diverse da quelle per le quali essi sono stati originariamente raccolti o generati» (art. 2, par. 2, lett. e, EHDS). La nozione di dati sanitari elettronici adottata dall'EHDS esclude, sul piano semantico e normativo, i dati raccolti su supporto cartaceo. All'interno di tale perimetro, la categoria di uso secondario di dati nel caso dei dati sanitari risulta particolarmente ampia e comprende sia dati personali sia dati non personali (art. 2, par. 2, lett. a, EHDS). Quanto ai dati personali, il regolamento equipara, ai fini dell'applicazione della disciplina, i «dati relativi alla salute» e i «dati genetici»⁵¹. Un'impostazione che si discosta da quella del GDPR, il quale mantiene distinte le due categorie e riconosce la natura ipersensibile dei dati genetici, in ragione delle implicazioni che il loro trattamento comporta per una pluralità di diritti fondamentali⁵².

solo condizioni generiche per l'uso secondario dei dati nel settore pubblico senza creare un vero e proprio diritto all'uso secondario di tali dati»; cfr. Commissione europea, Proposta di regolamento sullo Spazio europeo dei dati sanitari, COM (2022) 197 final, 3 maggio 2022, p. 5.

⁴⁷ M. CATANZARITI, *Verso una nuova epistemologia dei dati sanitari*, cit.

⁴⁸ S. THOBANI, *Verso il regolamento UE sullo spazio europeo dei dati sanitari (European Health Data Space)*, cit.

⁴⁹ Chiamati «Organismi responsabili dell'accesso ai dati sanitari». Si v. Art. 55, EHDS.

⁵⁰ D. CORTI, *Consenso (a fasi progressive), interesse pubblico per l'LA, opt-out per l'uso secondario: le nuove regole per la ricerca scientifica sui dati sanitari*, in *BioLaw Journal – Rivista di BioDiritto*, 2024, p. ss.

⁵¹ EHDS rinvia espressamente alle definizioni del GDPR in materia di dati genetici e di dati relativi alla salute, di cui all'art. 4, nn. 13 e 15.

⁵² I dati genetici presentano caratteristiche peculiari, in quanto idonei a fornire informazioni non circoscritte al momento dell'analisi, ma rilevanti anche in una dimensione prospettica e di

La nozione di dati sanitari elettronici adottata dall'EHDS comprende pertanto sia dati raccolti nel contesto dell'uso primario (assistenza sanitaria)⁵³, sia dati generati o acquisiti direttamente per finalità di ricerca e innovazione, sia dati sanitari elettronici non personali, come nel caso di dati resi anonimi. Il risultato è, nelle intenzioni del legislatore, ampliare notevolmente l'ambito oggettivo del riutilizzo dei dati. Come si vedrà più approfonditamente nel prossimo paragrafo, la legittimità del trattamento dei dati sanitari ha sempre meno a che fare con la sfera personale degli interessati e più con un nuovo regime giuridico di dati destinati alla libera circolazione, sulla base dell'assunto, non privo di ambiguità, che l'anonimizzazione dei dati supporti in ogni caso una logica di valorizzazione economica⁵⁴.

Secondo gli auspici dell'EHDS, i dati sanitari elettronici possono essere messi a disposizione tanto di soggetti pubblici quanto di operatori privati, anche a fini di lucro, purché il trattamento sia ricondotto a finalità espressamente qualificate come legittime. Queste ultime finalità sono elencate all'art. 53 EHDS e comprendono, in particolare, le finalità di sanità pubblica e di medicina del lavoro, il sostegno alle attività di definizione delle politiche pubbliche, l'elaborazione di statistiche, le attività di istruzione e insegnamento, nonché il miglioramento e l'ottimizzazione delle prestazioni assistenziali (art. 53, par. 1, lett. a–d e f), EHDS). In questo quadro assume rilievo centrale la ricerca scientifica, a cui il legislatore europeo attribuisce una portata volutamente ampia (art. 53, par. 1, lett. e), EHDS). Essa comprende non solo la ricerca funzionale alla tutela della salute pubblica, ma anche quella volta alla valutazione delle tecnologie sanitarie e al miglioramento della qualità e della sicurezza dell'assistenza, dei medicinali e dei dispositivi medici, con un evidente potenziale di proiezione applicativa e commerciale dei risultati della ricerca. In questo ambito rientrano espressamente anche le attività di sviluppo e innovazione di prodotti e servizi, nonché l'addestramento, la sperimentazione e la valutazione di algoritmi, inclusi quelli impiegati in sistemi di intelligenza artificiale, dispositivi medici e applicazioni di sanità digitale.

lungo periodo, potenzialmente riferibili non solo all'individuo interessato, ma anche al suo gruppo biologico di appartenenza. Cfr. A.A. MOLLO, «Prime riflessioni sul Regolamento europeo sullo spazio europeo dei dati sanitari: l'uso secondario e il diritto di esclusione riguardo al trattamento dei dati sanitari elettronici personali», in *BioLaw Journal – Rivista di BioDiritto*, 2025 (3), pp. 11–29.

⁵³ Per «uso primario» si intende «il trattamento dei dati sanitari elettronici per la prestazione di assistenza sanitaria al fine di valutare, mantenere o ripristinare lo stato di salute della persona fisica cui si riferiscono tali dati, comprese la prescrizione, la dispensazione e la fornitura di medicinali e dispositivi medici, nonché i pertinenti servizi sociali, amministrativi o di rimborso». Cfr. Art. 2, par. 1, lett. e).

⁵⁴ C. STAUNTON ET AL., *Ethical and social reflections on the proposed European Health Data Space*, in *European Journal of Human Genetics*, 2024 (32, 5), p. 498–505.

A fronte dell'ampiezza delle finalità ammesse e dei rischi connessi alla circolazione di grandi volumi di dati sanitari, l'EHDS provvede ad un elenco di usi vietati (art. 54 EHDS). In particolare, l'uso secondario non può essere finalizzato all'adozione di decisioni che producano effetti giuridici o comunque pregiudizievoli nei confronti di persone fisiche o gruppi di persone (art. 54, lett. a) EHDS), incluse le decisioni discriminatorie in materia di occupazione, accesso a beni e servizi, condizioni assicurative o creditizie (art. 54, lett. b), EHDS). Sono altresì esclusi l'utilizzo dei dati per finalità di marketing o pubblicità (art. 54, lett. c), EHDS), lo sviluppo di beni o servizi suscettibili di arrecare danno alle persone, alla salute pubblica o alla società nel suo complesso (art. 54, lett. d), EHDS), nonché gli usi contrari all'ordine pubblico (art. 54, lett. e), EHDS)⁵⁵.

Tornando al meccanismo comune di accesso e condivisione messo a punto con il nuovo Regolamento, l'EHDS prevede tre categorie di soggetti: i titolari dei dati (art. 2, par. 2, lett. t), EHDS), gli utenti dei dati (art. 2, par. 2, lett. u), EHDS) e gli organismi responsabili dell'accesso ai dati sanitari (art. 55 EHDS). I titolari dei dati sanitari elettronici sono definiti in senso ampio dal Regolamento e comprendono non solo persone fisiche o giuridiche che erogano prestazioni sanitarie o assistenziali, ma anche soggetti che in questi settori sviluppano prodotti o servizi, svolgono attività di ricerca o, più in generale, trattano dati sanitari elettronici per le finalità previste dall'EHDS. Su tali soggetti, fatte salve le eccezioni previste per le persone fisiche e le microimprese (art. 50 EHDS), grava l'obbligo di messa a disposizione, per uso secondario, di un insieme minimo di categorie di dati in loro possesso. Gli utenti dei dati sanitari sono i soggetti autorizzati a richiedere l'accesso ai dati succitati per finalità di uso secondario. In questa categoria rientrano i ricercatori che hanno sempre più interesse a utilizzare i dati sanitari raccolti nei contesti assistenziali, per scopi scientifici che non hanno una ricaduta diretta sulla cura dell'interessato. Il rapporto tra titolari e utenti dei dati non è diretto, ma è mediato dagli organismi responsabili dell'accesso ai dati sanitari, designati a livello statale. In estrema sintesi, i titolari dei dati sono tenuti a mettere a disposizione, per uso secondario, un insieme minimo di categorie di dati (art. 51 EHDS). Gli utenti dei dati presentano le richieste di accesso agli organismi competenti (art. 67 EHDS), che valutano l'ammissibilità sulla base dei principi di finalità e minimizzazione (art. 66 EHDS) e rilasciano, se del caso, un'autorizzazione ai dati valida per finalità e

⁵⁵ Nel loro insieme, le disposizioni sulle finalità consentite e sui divieti delineano un modello di riutilizzo dei dati fortemente orientato alla tutela dell'interesse pubblico, nel quale la promozione della ricerca e dell'innovazione è accompagnata dall'esclusione di pratiche idonee a incidere negativamente sui diritti fondamentali, sull'eguaglianza sostanziale e sulla fiducia dei cittadini nei sistemi di condivisione dei dati. Cfr. G. RESTA, *Health Data in Europe at the Crossroads of Data Protection and Data Sharing*, cit.

durata determinate (art. 68 EHDS)⁵⁶. Il trattamento avviene esclusivamente in ambienti sicuri, senza trasferimento diretto dei dati agli utenti, e consente il rilascio all'esterno dei soli dati sanitari elettronici non personali, compresi i risultati in forma statistica anonimizzata (art. 73, par. 2), EHDS)⁵⁷. È fatto divieto di re-identificazione degli interessati (art. 61, par. 3), EHDS) ed è previsto l'obbligo di pubblicazione dei risultati dell'uso secondario (art. 61, par. 4), EHDS). Questa procedura standardizzata mira a prevenire modalità di accesso frammentate, ma non elimina del tutto le criticità legate alla natura ancora decentrata delle decisioni nei casi di accesso transfrontaliero, affidate ai singoli organismi nazionali competenti.

Poiché l'uso secondario di dati sanitari elettronici personali si configura come trattamento ulteriore di categorie particolari di dati, l'EHDS introduce una deroga specifica al divieto generale di trattamento, rendendo operative le basi giuridiche di cui all'articolo 9, paragrafo 2, lettere g) e j), del GDPR, che il nuovo regolamento integra e specifica mediante un articolato sistema di garanzie (cons. 52 EHDS). Per scongiurare il pericolo di un'applicazione disomogenea del nuovo Regolamento, al Considerando 52 si suggerisce agli Stati membri di non mantenere (o introdurre ulteriori) ostacoli o condizioni per il trattamento dei dati sanitari per uso secondario, in particolare, facendo leva sul principio del consenso e salvo l'adozione di garanzie più rigorose. In ogni caso, per gli utenti dei dati, rimane la necessità di individuare una valida base giuridica per il riuso dei dati ai sensi dell'articolo 6 del GDPR.

La riduzione della centralità del consenso nel meccanismo messo appunto dalla normativa è controbilanciata dall'introduzione del diritto di esclusione (c.d. *opt-out*), esercitabile in qualsiasi momento e senza obbligo di motivazione (art. 71, par. 1), EHDS). Questo diritto preclude l'ulteriore trattamento dei dati per uso secondario, fatti salvi i trattamenti già autorizzati prima del suo esercizio (art. 71, par. 3), EHDS).

Originariamente assente nelle prime versioni della proposta, il diritto di esclusione è stato oggetto di un lungo confronto interistituzionale sulla necessità di rafforzare il controllo degli interessati sull'utilizzo dei propri dati, all'interno di un regime di liceità fondato sulle basi giuridiche normative predisposte con l'art. 9, par. 2), lett. g) e j). L'*opt out* può qualificarsi come diritto potestativo dell'interessato che affianca e non si sovrappone ai diritti garantiti dal

⁵⁶ Al fine di agevolare l'uso secondario dei dati sanitari elettronici, il Regolamento prevede la pubblicazione, da parte degli organismi di accesso, di cataloghi delle serie di dati disponibili, predisposti sulla base delle informazioni fornite dai titolari ed eventualmente corredati da indicatori della qualità dei dataset (artt. 77–78 EHDS).

⁵⁷ Il Regolamento disciplina anche la condivisione verso Paesi terzi, prevedendo che l'accesso ai dati sanitari da parte di richiedenti stabiliti fuori dall'UE sia subordinato a condizioni di reciprocità accertate mediante un atto di esecuzione della Commissione (artt. 88–91 EHDS).

GDPR, in particolare il diritto di opposizione. La forma di tale diritto resta tuttavia rimessa alle scelte degli Stati membri, poiché, in deroga alla previsione generale, è espressamente stabilito che «uno Stato membro può prevedere nel proprio diritto nazionale un meccanismo per rendere disponibili i dati per i quali è stato esercitato il diritto di esclusione» (art. 71, par. 4), EHDS). Tale possibilità derogatoria è ammessa solo al ricorrere di condizioni stringenti ed è circoscritta a finalità specifiche, tra cui la «ricerca scientifica per importanti motivi di interesse pubblico» (art. 71, par. 4), lett. a) EHDS). In ogni caso, le norme nazionali che disciplinano l'attuazione di tali deroghe devono «rispettare l'essenza dei diritti e delle libertà fondamentali e costituire una misura necessaria e proporzionata in una società democratica per servire ragioni di interesse pubblico nel perseguimento di obiettivi scientifici e sociali legittimi» (art. 71, par. 5), EHDS; art. 52, par. 1, Carta dei diritti fondamentali dell'UE).

4. Problematiche attuali: criticità giuridiche e rischi di arretramento della tutela nell'EHDS

La ricostruzione del quadro normativo delineato dal regolamento sullo Spazio europeo dei dati sanitari consente di mettere in luce alcune criticità della disciplina dell'uso secondario dei dati sanitari. La prima riguarda l'effettivo coordinamento del nuovo Regolamento con la disciplina esistente, in particolare il rapporto con il GDPR. Le categorie minime di dati sanitari elettronici che i titolari sono tenuti a mettere a disposizione per l'uso secondario (v. *supra*, par. 3; art. 51 EHDS) devono essere lette in rapporto alle nozioni di «dati relativi alla salute» e di «dati genetici» del GDPR. Vi rientra un insieme eterogeneo e particolarmente ampio di dati provenienti da studi clinici, coorti di ricerca, registri di mortalità, registri di prodotti medicinali e dispositivi medici, biobanche e banche dati dedicate, nonché risultati di questionari e ricerche settoriali, che vanno ad aggiungersi ai dati genomici ed epigenomici, dati generati da applicazioni per il benessere e da dispositivi digitali, nonché riferiti a fattori solo indirettamente o astrattamente idonei a incidere sulla salute, quali i determinanti sociali e ambientali, sino a comprendere dati relativi allo status e alla formazione dei professionisti.

Nella *Joint Opinion* dell'EDPB e dell'EDPS del 2022, le osservazioni critiche delle due autorità europee, sebbene formulate con riferimento alla proposta iniziale della Commissione, sembrano in larga misura confermate dalle scelte adottate nel testo finale del Regolamento. Nello specifico riguardano l'introduzione di eccezioni alla regola del consenso per il trattamento dei dati sanitari, con un ampliamento delle deroghe agli obblighi informativi, incidendo in modo signifi-

cativo sull'effettività del controllo degli interessati sui propri dati personali⁵⁸. Abbiamo indugiato su questi problemi del Regolamento nei paragrafi precedenti di questo articolo.

D'altro canto, relativamente alla reale capacità dell'EHDS di istituire un quadro giuridico effettivamente uniforme per l'uso secondario dei dati sanitari, va menzionato che il regolamento fornisce una base giuridica per il riutilizzo dei dati sanitari elettronici personali a fini di ricerca, integrando e specificando le condizioni e le garanzie di cui all'art. 9, par. 2, lett. j) GDPR. Tale intervento, tuttavia, non incide sulla necessità che continua a gravare in capo al richiedente l'accesso ai dati anche in regime EDHS, di fondare la propria richiesta di trattamento a quei dati su una delle basi giuridiche previste dall'art. 6 GDPR. Il risultato è che il riutilizzo dei dati sanitari elettronici con riferimento al trattamento per finalità scientifiche dipendono ancora e nonostante tutto dalle normative nazionali che variano significativamente da Stato a Stato.

Potrebbe obbiettersi che il Considerando 53 suggerisce agli Stati membri di non mantenere né introdurre condizioni ulteriori per il trattamento dei dati sanitari a fini di uso secondario, comprese disposizioni che subordinino il trattamento al consenso dell'interessato. Al tempo stesso, però, il Regolamento consente espressamente l'adozione di misure più rigorose e di garanzie supplementari a livello nazionale, senza istituire uno standard uniforme per il regime di accesso e riutilizzo dei dati. L'impianto normativo così delineato rischia di alimentare nuove forme di frammentazione. In particolare, l'art. 51, par. 4, autorizza gli Stati membri a introdurre misure più stringenti e garanzie aggiuntive per certe categorie di dati, tra cui i dati genetici, genomici ed epigenomici, nonché quelli provenienti da applicazioni per il benessere e da biobanche. A ciò si aggiunga quanto previsto dall'art. 71, che demanda agli Stati membri la facoltà di introdurre eccezioni alla regola dell'*opt-out*, con il rischio di determinare ulteriori divergenze applicative nella disciplina dell'uso secondario dei dati sanitari nei diversi ordinamenti nazionali.

Le criticità sin qui richiamate rinviano, in ultima analisi, a un problema di carattere strutturale. La tensione tra l'obiettivo di promuovere un ampio riutilizzo dei dati sanitari e quello di garantire un elevato livello di tutela dei diritti fondamentali non appare risolta. L'impianto dell'EHDS sembra muovere dall'assunto che tale bilanciamento sia già stato operato a monte dal legislatore, configurando l'uso secondario come assetto ordinario del trattamento, mentre l'intervento dell'interessato viene relegato prevalentemente alla funzione di correttivo *ex*

⁵⁸ European Data Protection Board – European Data Protection Supervisor, *Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space*, 2022, punti 23–25, p. 9

*post*⁵⁹. In tale prospettiva, il diritto di esclusione riconosciuto dall'art. 71 EHDS, pur presentato come strumento di rafforzamento dell'autonomia individuale rispetto a dati qualificati come particolarmente sensibili, si configura come il risultato di un compromesso che non elimina il rischio di un arretramento sostanziale della tutela, anche in ragione delle ampie possibilità di deroga rimesse agli Stati membri per motivi di interesse pubblico rilevante, tra cui la ricerca scientifica. Tale assetto incide altresì sulla percezione di legittimità e sulla fiducia dei cittadini nei meccanismi di condivisione dei dati sanitari, in particolare laddove le finalità perseguite e le garanzie predisposte non risultino pienamente comprensibili.

Le perplessità si accentuano ulteriormente in ragione della latitudine delle finalità legittime di uso secondario e della conseguente sovrapposizione tra ricerca scientifica, innovazione tecnologica e interessi economici, anche privati. In questo contesto, il richiamo all'interesse pubblico, all'altruismo dei dati⁶⁰ e, più in generale, a un'etica pubblica della salute rischia di assolvere a una funzione prevalentemente retorica, laddove gli attori coinvolti sono presenti su piani diversi e la condivisione dei dati sanitari tende a essere configurata come doverosa per definizione, più che come espressione di una scelta realmente libera e consapevole. L'assenza di meccanismi effettivi di partecipazione degli interessati alle decisioni collettive di interesse generale in materia di ricerca confermerebbe questo peculiare "dovere alla condivisione". Questo dovere si presenta come altra faccia della medaglia sull'attuale configurazione dell'uso secondario dei dati. Il risultato è stato una progressiva ridefinizione dalla qualificazione giuridica dei dati sanitari, sempre più assimilati a beni finalizzati a interessi superindividuali e sociali, «massimamente espressi nella ricerca scientifica»⁶¹ e funzionali a politiche di sanità pubblica, innovazione e mercato. In tale slittamento, i dati sanitari tendono a perdere il loro carattere strettamente personale e a essere sottratti al regime dell'autodeterminazione individuale fondato sul consenso. Tale esito non discende dall'assenza di garanzie formali, ma dal modo in cui esse sono strutturate nell'EHDS. Il Regolamento privilegia infatti strumenti organizzativi e procedurali - quali l'intermediazione degli organismi responsabili dell'accesso ai dati sanitari (artt. 55, 57, 68 e 69 EHDS), il trattamento in am-

⁵⁹ G. GORGONI, *Lo spazio europeo dei dati sanitari e il buon cittadino europeo: fare di virtù necessità?*, cit.; D. CORTI, *Consenso (a fasi progressive), interesse pubblico per l'LA, opt-out per l'uso secondario: le nuove regole per la ricerca scientifica sui dati sanitari*, cit.

⁶⁰ Il DGA introduce il concetto di altruismo dei dati come messa a disposizione volontaria e non remunerata di dati personali e non personali per finalità di interesse generale, tra cui la ricerca scientifica e la sanità pubblica, disciplinando requisiti e garanzie per le organizzazioni che operano in tale ambito (artt. 2, punto 16, e 16-22).

⁶¹ L. TRAPANI, *La circolazione dei dati sanitari per uso secondario e la riduzione dei divari*, cit.

bienti sicuri senza trasferimento diretto agli utenti (artt. 73 EHDS), il divieto di reidentificazione (art. 61, EHDS), e, in taluni casi, la restituzione dei soli risultati di elaborazioni richieste dagli utenti in forma statistica anonimizzata (art. 69 EHDS)⁶² – che spostano il baricentro della tutela dal controllo individuale *ex ante* a una gestione sistemica del dato.

In tale assetto, il consenso e gli obblighi informativi assumono un ruolo subordinato, mentre la capacità dell'interessato di incidere sulle finalità e sulle condizioni del trattamento risulta attenuata e temporalmente posticipata, anche in ragione della qualificazione dell'uso secondario come trattamento lecito fondato su basi normative autonome. Il diritto di opposizione, declinato nel meccanismo dell'*opt-out* di cui all'art. 71 EHDS, opera infatti come rimedio successivo e strutturalmente limitato: da un lato, non incide sui trattamenti già autorizzati o in corso (art. 71, par. 3), EHDS); dall'altro, come visto, può essere oggetto di deroghe (art. 71, par. 4), EHDS). Anche laddove l'anonimizzazione sia assunta come presidio di tutela, essa opera prevalentemente come tecnica funzionale alla circolazione e al riutilizzo dei dati nell'ambito dell'uso secondario, senza eliminare né i rischi residui di re-identificazione, implicitamente riconosciuti dal legislatore europeo, né gli effetti indiretti che l'utilizzo dei dati può produrre sui singoli e sui gruppi di riferimento, in particolare attraverso modelli predittivi, attività di ricerca applicata e lo sviluppo di sistemi di intelligenza artificiale (art. 53, par. 1, lett. e), EHDS).

Questa tensione strutturale risulta particolarmente problematica se si considera, da una parte, l'inclusione tra i dati sanitari anche di quelli raccolti o generati in contesti non strettamente riconducibili alla cura, come le applicazioni per il benessere, e, dall'altra, l'estensione dell'uso secondario all'addestramento di sistemi di intelligenza artificiale senza soffermarsi troppo sulla «complessità, opacità, autonomia, imprevedibilità e vulnerabilità» di queste tecnologie⁶³. In questi casi, la presunzione di utilità sociale del riutilizzo dei dati tende a prevalere su una valutazione puntuale dell'impatto sui diritti fondamentali, sollevando questioni rilevanti non solo in termini di protezione dei dati personali, ma anche con riferimento all'autonomia individuale, al diritto di partecipazione alla scienza, alla giustizia sociale e alla sostenibilità democratica del modello di *governance* delineato. Ne deriva una equiparazione problematica tra la tutela della salute e finalità di sviluppo e innovazione non necessariamente coincidenti, con il ri-

⁶² Accanto alle domande di accesso, gli utenti possono presentare agli organismi responsabili una «richiesta di dati sanitari» (art. 69 EHDS) per le finalità di cui all'art. 53 del Regolamento. In tal caso non è concesso l'accesso ai dati, ma l'organismo fornisce unicamente una risposta in forma statistica anonimizzata.

⁶³ PAGALLO, *Il dovere alla salute. Sul rischio di sottoutilizzo dell'intelligenza artificiale in ambito sanitario*, cit.

schio di favorire vantaggi competitivi per gli attori commerciali che accedono ai dati. In tale contesto, il cittadino *dataficato*⁶⁴ tende a slittare da soggetto di diritti a oggetto di pratiche di ricerca e valorizzazione dei dati⁶⁵.

5. Conclusioni

Entrato in vigore il 26 marzo 2025, l'EHDS seguirà un'attuazione graduale a decorrere dal 2027, con la piena applicazione delle regole principali sull'uso secondario dei dati a partire dal 2029 e successive estensioni dal 2031 (art. 105 EHDS)⁶⁶. Proprio la fase di implementazione offre oggi l'opportunità di un ulteriore cambio di paradigma: creare un ambiente favorevole alla condivisione e alla messa a disposizione dei dati, fondato su fiducia e principi comuni, nell'interesse collettivo dell'Unione di valorizzare realmente il potenziale dei dati sanitari. In questa prospettiva, il Regolamento affianca agli strumenti giuridici e organizzativi anche misure volte a rafforzare la fiducia dei cittadini, prevedendo iniziative di alfabetizzazione digitale e campagne di informazione istituzionale finalizzate a rendere comprensibili la portata degli interessi generali perseguiti e le garanzie predisposte a tutela degli interessati (artt. 83 e 84 EHD).

Tuttavia, l'efficacia dell'EHDS dipenderà, da un lato, dalla concreta attuazione delle infrastrutture tecniche e organizzative previste dal Regolamento, in particolare dagli organismi responsabili dell'accesso ai dati sanitari (artt. 55–58 EHDS), dagli ambienti sicuri di trattamento (artt. 73 EHDS) e dall'infrastruttura transfrontaliera *HealthData@EU* dedicata all'uso secondario dei dati sanitari (art. 75 EHDS), nonché dagli atti di esecuzione della Commissione relativi all'interoperabilità, alla sicurezza e al funzionamento operativo dello spazio europeo dei dati sanitari (artt. 73, 75, 77 e 78 EHDS)⁶⁷. Dall'altro lato, essa dipenderà dalla capacità di evitare che le clausole di flessibilità nazionale si traducano in nuove segmentazioni del mercato e in differenze sostanziali nelle tutele. In breve, l'EHDS potrà ridurre la frammentazione solo se l'armonizzazione “di cornice” non verrà neutralizzata, nella pratica, da implementazioni divergenti a livello statale⁶⁸.

⁶⁴ S. RODOTÀ, *Trasformazioni del corpo*, in *Politica del diritto*, 2006 (1), p. 3–24.

⁶⁵ G. GORGONI, *Lo spazio europeo dei dati sanitari e il buon cittadino europeo: fare di virtù necessità*, cit.

⁶⁶ Si veda anche: Commissione europea, *European Health Data Space Regulation*, disponibile su: https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space-regulation-ehds_en (ultimo accesso: 30 gennaio 2026).

⁶⁷ Giova ricordare che il Regolamento istituisce un articolato quadro di governance a livello europeo, comprendente un Comitato dello spazio europeo dei dati sanitari e un forum dei portatori di interesse (artt. 92–93 EHDS), nonché disposizioni in materia di sanzioni e diritto al risarcimento per le violazioni delle sue disposizioni (artt. 99–100 EHDS).

⁶⁸ Art. 51, par. 4, e art. 71, Regolamento (UE) 2025/327; European Data Protection Board –

Al di là dei profili istituzionali e attuativi, emerge una questione ulteriore, di ordine strutturale e sostanziale. La disciplina dell'EHDS presuppone, almeno in parte, che il bilanciamento tra diritti individuali e interessi collettivi sia già stato operato a monte dal legislatore, configurando il riutilizzo dei dati come assetto ordinario e riservando all'intervento dell'interessato una funzione correttiva *ex post*, affidata al meccanismo dell'*opt-out*. In questa traiettoria, la legittimazione dell'uso secondario tende ad appoggiarsi non solo su argomenti giuridici, ma anche su un lessico valoriale, quali l'"interesse pubblico" e l'"altruismo dei dati", che segnala il passaggio dall'etica "ordinaria" della ricerca, centrata sul consenso informato e sulla relazione diretta tra ricercatore e partecipante, verso una più ampia etica pubblica della salute, nella quale la condivisione dei dati è presentata come doverosa in quanto funzionale a benefici sociali sistemici⁶⁹.

Tale impostazione appare particolarmente problematica quando la convergenza tra ricerca biomedica e tecnologie digitali rende la ricerca permeabile a interessi commerciali, in particolare di grandi operatori tecnologici e imprese attive nello sviluppo di soluzioni di sanità digitale, intelligenza artificiale e *data analytics*, che possono accedere ai dati e valorizzarli in prodotti e servizi⁷⁰. Per scongiurare tale esito, sarà fondamentale che attori pubblici e privati cooperino in un uso responsabile del dato sanitario, fondato su *accountability* effettiva, trasparenza ed efficaci sistemi di controllo,

In definitiva, la realizzazione dello Spazio europeo dei dati sanitari non dipenderà soltanto dalla disponibilità dei dati o dall'efficienza delle infrastrutture, ma dalla capacità dell'EHDS di mantenere credibile il nesso tra uso dei dati, tutela dei diritti fondamentali e fiducia dei cittadini, evitando che la valorizzazione del dato sanitario come risorsa collettiva si traduca in un arretramento sostanziale delle garanzie poste a presidio dell'autodeterminazione individuale.

European Data Protection Supervisor, *Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space*, 2022.

⁶⁹ R. SALA, *Lo spazio europeo dei dati sanitari: una questione di etica pubblica*, in *Notizie di Politeia*, 2025, (XLI, 158), pp. 7-17.

⁷⁰ A. CAGGIANO, *Interessi e norme nell'ecosistema europeo dei dati sanitari: la tecnoregolazione abilitativa e le sfide per l'efficacia*, in A. MORACE PINELLI (a cura di), *Sanità digitale – Regolamento "EHDS" (UE) 2025/327 sullo spazio europeo dei dati sanitari. I. Uso dei dati e assetti organizzativi*, Pisa: Pacini Giuridica, 2025, pp. 19-34.

OPEN GOVERNMENT DATA

Monica Palmirani

SOMMARIO: 1. Introduzione. 2. Le origini. 3. Le motivazioni. 4. I principi. 5. La normativa europea. 6. La normativa italiana. 7. Le linee guida. 7.1 I formati aperti. 7.2 I metadati. 7.3 Le licenze standard. 7.4. Linked Open Data. 8. I cataloghi di Open Government Data. 9. Il benchmarking. 10. L'ecosistema open government data. 11. I digital twin basati sugli open data. 12. Conclusioni-

1. Introduzione

L'*open data* è un processo complesso avviato da un ente di natura privata o pubblica che porta alla pubblicazione di dati in un formato tecnicamente aperto, ossia leggibile dai computer senza vincoli, arricchiti con altre informazioni (chiamate *metadati*) che ne descrivono la natura e dotati di una licenza standard che ne garantisce il pieno riutilizzo senza condizioni giuridiche se non l'obbligo di riconoscere l'attribuzione dell'autore. Ci sono molte definizioni di *open data* a cura di organizzazioni no-profit¹² e proposte dalle norme sovranazionali e nazionali, ma non deve essere confuso con il mero formato aperto dei dati che è invece una delle condizioni affinché si realizzi il processo di *open data*. Il principio che è alla base dell'*open data* risiede nella consapevolezza che i dati sono fondamentali per prendere decisioni, per elaborare prodotti digitali, per estrarre analisi, per allenare intelligenze artificiali, per fornire ai cittadini e alle imprese materiali preziosi. Gli *open data* sono essenziali, se adottati dalle pubbliche amministrazioni, anche per realizzare i principi di trasparenza amministrativa e monitoraggio delle azioni degli enti pubblici. Realizzare gli *open data* in un determinato contesto, significa fornire ai suoi portatori di interessi (e.g., imprese, cittadini, enti, giornalisti, etc.) i pilastri per la partecipazione al governo del territorio.

¹ <https://opendatahandbook.org/guide/it/>, Open data handbook, Open Knowledge Foundation (OKFN).

² <https://centre.humdata.org/ufaqs/what-is-open-data/>

2. Le Origini

Nel 2009 Sir. Tim Berners-Lee, ideatore del WWW, tenne un discorso al famoso TED talk³ dal titolo “The Next Web”, nella conferenza di Long Beach. In questo discorso si enunciò per la prima volta il concetto chiamato “Raw data now”, intendendo appellarsi al rilascio dei dati, specialmente da parte delle pubbliche amministrazioni, delle istituzioni, dei centri di ricerca e delle università, rendendoli accessibili e riusabili. Successivamente, l’inventore del Web teorizzò i pilastri del Linked open data⁴ le specifiche tecnologiche dell’Open data. Nel medesimo anno 2009, il presidente degli Stati Uniti d’America, Barack Obama, firmò il *Memorandum on Transparency and Open Government*⁵ nel quale diede inizio ad una profonda trasformazione delle politiche di apertura dei dati nei diversi dipartimenti federali, avviando così una rivoluzione che ha portato alla creazione del portale <https://data.gov/> che annovera mezzo milione di dataset. Successivamente anche il Regno Unito avvia un portale <https://www.data.gov.uk/> con il supporto dello stesso Tim Berners-Lee. Nel 2013 il G8 sancisce il manifesto dell’Open Data e definisce questo approccio essenziale per lo sviluppo di democrazie inclusive, trasparenti, partecipate. Successivamente il G20 del 2015 definisce l’Open Data Charter⁶, ribadendo l’importanza di aprire i dati della pubblica amministrazione per combattere la corruzione nei governi⁷.

In realtà già nel 2003 l’Unione europea emana la direttiva 2003/98/CE relativa al riutilizzo dell’informazione del settore pubblico, fornendo i primi elementi per diffondere la cultura del riuso. L’art. 3 infatti statuisce quanto segue: «Gli Stati membri provvedono affinché, ove sia permesso il riutilizzo di documenti in possesso degli enti pubblici, questi documenti siano riutilizzabili a fini commerciali o non commerciali conformemente alle condizioni indicate nei capi III e IV. I documenti sono resi disponibili, ove possibile, per via elettronica». Il concetto del riuso non implica tuttavia in modo automatico il concetto dell’apertura dei dati perché il riuso necessita di un richiedente e non un gesto aperto a tutta la comunità spontaneo da parte della pubblica amministrazione.

³ https://www.ted.com/talks/tim_berners_lee_the_next_web

⁴ C. BIZER, T. HEATH, T. BERNERS-LEE, *Linked Data - The Story So Far*, in *International Journal on Semantic Web and Information Systems (IJSWIS)*, 2009 (5,3), pp. 1-22.

⁵ <https://obamawhitehouse.archives.gov/open/documents/open-government-directive>

⁶ <https://knowledgehub.transparency.org/guide/international-anti-corruption-commitments-/8157>

⁷ <https://www.nazaha.gov.sa/Media/Posts/G20-Anti-Corruption%20Open%20Data%20Principles.pdf>, https://g7g20-documents.org/fileadmin/G7G20_documents/2013/G7/United%20Kingdom/Leaders/1%20Leaders%27%20Language/G8%20Open%20Data%20Charter_18062013-.pdf

Dovremo attendere la nuova normativa europea per poter trovare le definizioni di open data come superamento del concetto di riuso.

3. Le motivazioni

Le principali motivazioni del fenomeno open data si articolano in tre categorie: i) economiche; ii) sociali; iii) tecnologiche. Dopo l'esplosione del Web 1.0 che vedeva pagine statiche HTML, succeduta dalla stagione del Web 2.0 dove i portali iniziano a fornire strumenti per consentire agli utenti di scrivere in autonomia i propri contenuti (e.g., blog, wiki, social media), ecco che arriva la stagione del Web 3.0 dove i contenuti sono visti anche come dati da elaborare arricchiti da metadati (dati sui dati) che ne definiscono i contenuti sotto forma di concetti (e.g., tag dei luoghi e delle persone, geolocalizzazione, microtargeting degli interessi degli utenti). In questa nuova dimensione del Web 3.0 risulta particolarmente importante condividere o meglio “rilasciare” i dati in formato aperto per il massimo riutilizzo affinché si possa trarre beneficio da questa importante fonte di informazione.

Il Web 4.0 attuale vede l'interazione del Web con i dispositivi digitali (e.g., sensori, smartphone, devices⁸), e quindi il rilascio di questi dati è anche fonte di trasparenza in una realtà che è ormai spesso intermediata da algoritmi (e.g., agenti intelligenti come gli assistenti vocali). Questa è la motivazione economica che muove il movimento open data: rilasciare dati di qualità affinché enti con finalità pubblica, e non solo di mercato, possano condividere delle informazioni utili all'economia. Quindi questi dati hanno un valore nel mercato molto elevato, basti pensare ai dati sanitari e alle statistiche aggiornate degli ospedali.

Vi è sicuramente una motivazione sociale ed etica di richiesta da parte dei cittadini di maggior trasparenza dell'azione pubblica e quindi i dati risultano essere strumento di monitoraggio della buona amministrazione, contrastando corruzione, infiltrazioni della criminalità organizzata, mala gestione delle risorse pubbliche. Per questo molti attivisti richiedono a gran voce dati sui fondi per la ricostruzione post-terremoto, sulla qualità delle opere per mettere in sicurezza il territorio dopo importanti emergenze idriche, sulla situazione dell'edilizia scolastica, sulle spese per il piano pandemico. Il rilascio dei dati pubblici aumenta la fiducia nelle istituzioni, e crea i presupposti per una maggior partecipazione civica al governo di un territorio, consentendo ai cittadini di incidere fattivamente nelle politiche locali.

Infine, vi è anche una motivazione tecnologica. Condividere e rilasciare nell'ecosistema dell'informazione digitale dati di natura pubblica significa non solo

⁸ <https://digital-dryads.eu/>

portare all'attenzione una parte di realtà digitale chiusa nei database della pubblica amministrazione e metterla in circolo, ma anche mitigare eventuali storture prodotte dal monopolio delle bigtech che essendo spesso governate da normativa extra-giurisdizionale (e.g., USA, China) possono avere una percezione di fenomeni giuridici distorta. Per questo l'open data è anche un fenomeno che riequilibra i poteri nella sfera informativa. Si potrà obiettare che tali dati sono pochi in confronto a quelli accumulati dalle bigtech, ma occorre ricordare che la qualità e la natura dei dati delle pubbliche amministrazioni e degli enti aventi pubblica rilevanza mostrano attraverso i dati un aspetto pubblicistico e non privatistico della relazione stretta fra cittadini e Stato. La Figura 1 mostra in modo grafico le motivazioni sopra esposte.



Figura 1: Schema delle motivazioni del fenomeno Open Data
fonte portale della Commissione Europea⁹

A queste motivazioni, recentemente, se ne aggiunge un'altra di grande rilievo: utilizzare i dati delle pubbliche amministrazioni per popolare strumenti di intelligenza artificiale (IA) al fine di produrre servizi migliori per i cittadini, ridurre i costi, incrementare l'efficienza. La recente legge 132/2025 nell'art. 14¹⁰ fornisce il perimetro di utilizzo dell'intelligenza artificiale nella PA in Italia collocandola come supporto alla decisione e in una relazione strettamente strumentale, sotto il controllo del funzionario. Tuttavia, nulla dice sui dati che de-

⁹ <https://data.europa.eu/it/dataeuropa-academy/what-open-data>

¹⁰ Si veda l'art. 14, Legge 23/09/23, n. 132, Uso dell'intelligenza artificiale nella pubblica amministrazione, «1. Le pubbliche amministrazioni utilizzano l'intelligenza artificiale allo scopo di incrementare l'efficienza della propria attività, di ridurre i tempi di definizione dei procedimenti e di aumentare la qualità e la quantità dei servizi erogati ai cittadini e alle imprese, assicurando agli interessati la conoscibilità del suo funzionamento e la tracciabilità del suo utilizzo. 2. L'intelligenza artificiale è impiegata esclusivamente in funzione strumentale e di supporto all'attività provvedimentale, restando in capo al funzionario responsabile, ai sensi delle vigenti norme, il potere decisionale e la responsabilità in ordine ai provvedimenti e ai procedimenti in cui essa è utilizzata. 3. Le pubbliche amministrazioni adottano misure tecniche, organizzative e formative per garantire un utilizzo responsabile dell'intelligenza artificiale e per sviluppare le capacità trasversali degli utilizzatori. 4. Le pubbliche amministrazioni provvedono agli adempimenti previsti dal presente articolo con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente», <https://www.normattiva.it/eli/stato/-LEGGE/2025/09/23/132/CONSOLIDATED>

vono popolare tali strumenti di IA e per il principio di trasparenza è bene che i cittadini possano accedere non solo alla logica dell'algoritmo, ma anche ai dati con i quali l'IA è stata addestrata. L'Open Data svolge quindi un'ulteriore funzione, rendere più spiegabile la decisione supportata dall'IA mediante la lettura dei dati che hanno alimentato tali tecnologie¹¹.

4. I principi

I principi sui quali si fonda il paradigma open data sono espressi con la sigla FAIR¹² che è l'acronimo di *Findable - Accessible - Interoperable - Reusable*. *Findable*: rintracciabili affinché si possano verificare e far circolare; *Accessible*: una volta rintracciati i dati devono essere accessibili; *Interoperable*: i formati dei dati devono consentire di interoperare e integrarsi fra loro; *Reusable*: i dati devono essere riutilizzabili senza limitazioni dovute a protezioni del diritto d'autore. La ricerca in particolare necessita di dati per condurre esperimenti e analisi, e gli open data forniscono importanti informazioni utili per il progresso della scienza. Durante la pandemia del coronavirus, la mancanza di dati sugli spostamenti delle persone non ha consentito ai governi di predire le zone a rischio, ritardando così le misure di contenimento della pandemia. La mancanza di dati relativi alle opere d'arte e ai musei annotati con informazioni storiche di qualità, sfavorisce lo sviluppo del turismo. La scarsità di dati relativi alla situazione idrologica aggiornati in tempo reale impedisce agli esperti di prevenire disastri ambientali che arrecano gravi danni a cose e mettono in pericolo le persone. L'accesso quindi ai dati, di qualità, aggiornati in tempo reale, ben annotati con tutte le informazioni di contesto, produce un effetto positivo sulla società, sui servizi delle pubbliche amministrazioni, sulla ricerca e sulla cultura, nonché sul processo democratico di un paese.

Questi principi sono stati adottati da molti paesi che hanno integrato nelle loro policy digitali di governo il processo *open data*, costruendo una rete mondiale di enti (Open Government Partnership) che cooperano per condividere buone pratiche volte a migliorare la trasparenza e la capacità di rendicontare le azioni intraprese (la c.d. *accountability*).

Gli *open data* sostengono la legalità dei territori (e.g., per esempio pubblicando i beni confiscati alle mafie, si veda il sito Confiscati Bene¹³), combattono la

¹¹ M. PALMIRANI, S. SAPIENZA, *Spiegabilità e conoscibilità algoritmica nell'AI Act alla luce del quadro regolamentare europeo*, Roma: Luiss University Press, 2025.

¹² M. WILKINSON ET AL., *The FAIR Guiding Principles for scientific data management and stewardship*, 2016, <https://doi.org/10.1038/sdata.2016.18>.

¹³ <https://www.confiscatibene.it/>

corruzione (e.g., si veda Open Coesione¹⁴ che monitorizza l'utilizzo dei fondi europei), favoriscono la comprensione dei processi democratici (e.g., si veda OpenParlamento¹⁵).

Accanto ai principi FAIR, si introducono altri importanti pilastri quali l'open data by-default (aprire i dati in automatico se privi di un divieto), la qualità e la tempestività dei dati (aggiornare i dati in real-time), l'elaborazione mediante API per favorire lo scambio machine-to-machine (accessibilità in tempo reale ai dati e non dopo mesi).

Nel 2021 la comunità scientifica tutela i dati aperti degli indigeni, elabora ulteriori principi legati primariamente a concetti giuridici ed etici definendo così il paradigma CARE¹⁶ (Figura 2) composto da altri quattro importanti elementi: Collective Benefit, Authority to Control, Responsibility, and Ethics¹⁷.

Questa nuova frontiera di principi nasce dalla necessità, non solo delle comunità indigene, di ribadire la sovranità di alcuni dati, specie quelli socio-culturali, affinché non ci sia una cannibalizzazione da parte di grandi aziende (e.g., vedi il caso che ha visto la Disney negoziare con la Comunità Sámi¹⁸ per l'appropriazione culturale nell'uso di vestiti tradizionali nel film di animazione Frozen 1) o di altri stati dei simboli distintivi di certe comunità.

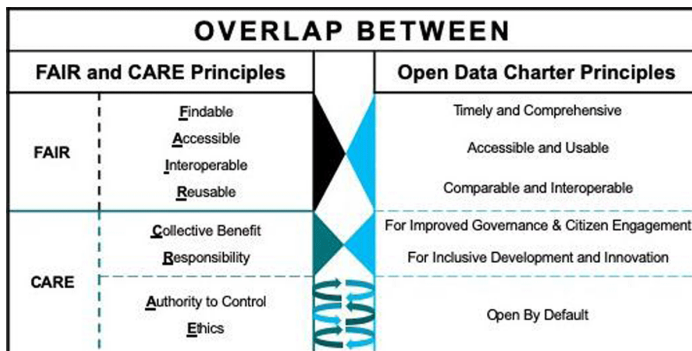


Figura 2: Comparazione fra i principi FAIR, CARE, e quelli provenienti dall'Open Data Charter¹⁹

I principi CARE avranno probabilmente lo stesso seguito dei principi FAIR in un prossimo futuro estesi a diverse situazioni dove la sovranità dei dati, i be-

¹⁴ <https://opencoesione.gov.it/it/>, progetto sostenuto non solo da attivisti, ma anche da enti e istituzioni.

¹⁵ <https://parlamento19.openpolis.it/>, OpenParlamento.

¹⁶ <https://www.gida-global.org/care>

¹⁷ S.R. CARROLL ET AL., *Operationalizing the CARE and FAIR Principles for Indigenous data futures*, 2021). <https://doi.org/10.1038/s41597-021-00892-0>

¹⁸ https://www.samediggi.fi/wp-content/uploads/2019/09/Agreement_WDAS_SAMI.pdf

¹⁹ S.R. CARROLL ET AL., *The CARE Principles for Indigenous Data Governance*, in *Data Science Journal*, 2021 (19), pp. 1–12, <https://doi.org/10.5334/dsj-2020-043>.

nefici collettivi, e l'autorità di controllo sul patrimonio dei dati possono fornire autorevolezza ai dataset, mediante anche una certificazione di autenticità, nonché il rispetto dei principi etici.

5. La normativa europea

La legislazione europea introduce i primi nuclei di regolazione degli open data nel 2003 con la direttiva 2003/98/CE (chiamata PSI I) avendo come obiettivo di normare il riuso dei dati della pubblica amministrazione. Successivamente ai fatti del G8 e del G20, la Commissione Europea rivede la direttiva apportando notevoli modifiche mediante la direttiva 2013/37/UE²⁰, includendo i concetti di “formato aperto”, “standard formale aperto”²¹, nonché regole che definiscono in maniera più chiara i termini di trasparenza delle tariffe a copertura dei costi²².

Nel 2019 il legislatore unionista consolida, aggiorna e semplifica la normativa in tema di riuso dei dati e open data, emanando la Direttiva 2019/1024/UE (PSI II), inserendo concetti in linea con i principi FAIR, la richiesta di avere licenze standard per favorire il riuso dei dati transfrontalieri, l'indicazione di provvedere a realizzare API per accedere in tempo reale a dati aggiornati e di qualità, maggiore attenzione agli aspetti economici dei dati e contemporaneamente al renderli accessibili gratuitamente o con un compenso limitato a recuperare i costi marginali di produzione. La PSI II (Public Sector Information) introduce inoltre un maggior coordinamento con le norme di protezione dei dati personali definite dal GDPR²³ soprattutto in merito a dati particolari²⁴. Gli open data infatti non possono includere dati personali o dati che possono arrecare danno a imprese e cittadini, per questo nella PSI II si citano misure di anonimizzazione che devono essere applicate prima del rilascio dei dati²⁵.

²⁰ <http://data.europa.eu/eli/dir/2013/37/oj>

²¹ L'Art. 1, 2013/37/UE introduce modifiche nell'art. 2 della direttiva 2003/97/CE nelle definizioni: «7. “formato aperto”, un formato di file indipendente dalla piattaforma e messo a disposizione del pubblico senza restrizioni che impediscano il riutilizzo dei documenti»: 8. “standard formale aperto”, uno standard che è stato definito in forma scritta, precisando in dettaglio i requisiti per assicurare l'interoperabilità del software».

²² L'Art. 1, 2013/37/UE introduce modifiche all'art. 7 della direttiva 2003/97/CE.

²³ Regolamento (UE) 2016/679, <http://data.europa.eu/eli/reg/2016/679/oj>

²⁴ Si veda Direttiva (UE) 2019/102, considerando (53), «Al momento di prendere decisioni sulla portata e sulle condizioni del riutilizzo di documenti del settore pubblico contenenti dati personali, per esempio nel settore della sanità, può essere imposto l'obbligo di procedere a valutazioni d'impatto sulla protezione dei dati a norma dell'articolo 35 del regolamento (UE) 2016/679».

²⁵ Si veda *Ibid*, art. 6, «1. Il riutilizzo di documenti è gratuito. Tuttavia, può essere autorizzato il recupero dei costi marginali sostenuti per la riproduzione, messa a disposizione e divulgazione dei documenti, nonché per l'anonimizzazione di dati personali o per le misure adottate per proteggere le informazioni commerciali a carattere riservato».

Nella PSI II troviamo la definizione di “formato aperto”, come «un formato di file indipendente dalla piattaforma e messo a disposizione del pubblico senza restrizioni che impediscano il riutilizzo dei documenti», ma non troviamo una definizione di open data (dati aperti) se non una descrizione nel considerando (16)²⁶.

Dal testo normativo, tuttavia, si evincono le condizioni di rilascio: un insieme di dati (chiamato dataset) si dice che è rilasciato in formato aperto se onora tre condizioni: i) è in formato tecnologicamente aperto, in un formato leggibile meccanicamente, conforme a standard formali aperti; ii) viene accompagnato da una licenza che favorisce il riuso senza condizioni se non l'attribuzione dell'autore; iii) ha una descrizione dettagliata mediante dei metadati tecnologici condivisi e standard.

Il “formato leggibile meccanicamente”, «è un formato di file strutturato in modo tale da consentire alle applicazioni software di individuare, riconoscere ed estrarre facilmente dati specifici, comprese dichiarazioni individuali di fatto e la loro struttura interna”. Per «standard formale aperto», si intende “uno standard che è stato definito in forma scritta, precisando in dettaglio i requisiti per assicurare l'interoperabilità del software».

Quindi non tutti i dataset in formato aperto sono classificabili come Open Data. Sono necessari anche altri elementi quali la licenza, i metadati e un formato tecnologico leggibile dagli elaboratori (*machine-readable*). Facciamo un esempio. Un dataset di dati dei musei comunali in formato proprietario che si può quindi leggere solo con uno strumento tecnologico a pagamento, non accompagnato da licenza di condivisione e senza metadati, pubblicato in un sito del museo protetto da privative sulla proprietà intellettuale, non è in open data. Lo stesso dataset in un formato standard aperto (e.g., XML) accompagnato da una

²⁶ *Ibid*, considerando(16), «Il concetto di apertura dei dati si intende generalmente riferito a dati in formati aperti che possono essere utilizzati, riutilizzati e condivisi liberamente da chiunque e per qualsiasi finalità. Le politiche relative all'apertura dei dati, che incoraggiano un'ampia disponibilità e il riutilizzo dell'informazione del settore pubblico a fini privati o commerciali, con vincoli minimi o in assenza di ogni vincolo di natura legale, tecnica o finanziaria, e che favoriscono la circolazione di informazioni non solo per gli operatori economici ma principalmente per il pubblico, possono svolgere un ruolo importante nel promuovere l'impegno sociale nonché avviare e favorire lo sviluppo di nuovi servizi basati su modi innovativi di combinare tali informazioni tra loro e di usarle. Si incoraggiano pertanto gli Stati membri a promuovere la creazione di dati basati sul principio dell'«apertura fin dalla progettazione e per impostazione predefinita», con riferimento a tutti i documenti che rientrano nell'ambito di applicazione della presente direttiva. Nel farlo essi dovrebbero assicurare al contempo un livello coerente di tutela degli obiettivi di interesse pubblico, per esempio la sicurezza pubblica, anche laddove siano interessate informazioni sensibili relative alla protezione delle infrastrutture critiche. Dovrebbero altresì assicurare la protezione dei dati personali anche là dove le informazioni in un insieme di dati individuale possono non presentare un rischio di identificazione o di individuazione di una persona fisica, ma possono, se associate ad altre informazioni disponibili, comportare un siffatto rischio».

licenza di riuso (e.g., cc-by 4.0), e annotato da metadati standard leggibili dalle macchine (e.g., RDF) è in open data (Figura 3).

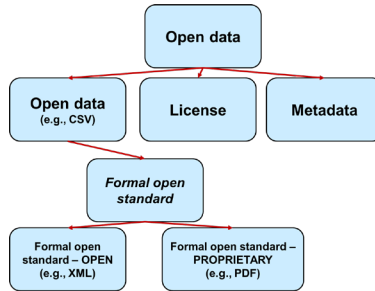


Figura 3: Grafico schematico della definizione di Open Data

È rilevante a tal fine ricordare che il Regolamento europeo di esecuzione 2023/138/UE²⁷ implementa le norme relative all'allegato I della Direttiva (UE) 2019/1024 (Direttiva Open Data) che individua le categorie tematiche considerate “serie di dati di elevato valore” (High-Value Datasets):

1. Dati geospaziali;
2. Dati relativi all'osservazione della terra e all'ambiente;
3. Dati meteorologici;
4. Dati statistici;
5. Dati relativi alle imprese e alla proprietà delle imprese;
6. Dati relativi alla mobilità.

Gli intrecci fra la regolazione dell'Open Data e altri regolamenti appartenenti alla Strategia Europea dei Dati rendono lo scenario complesso e articolato. Il Data Governance Act (Regolamento UE 2022/868²⁸) ha infatti introdotto una forma nuova di contribuzione dei dati chiamata “altruismo dei dati” definito come «la condivisione volontaria di dati sulla base del consenso accordato dagli interessati al trattamento dei dati personali che li riguardano, o sulle autorizzazioni di altri titolari dei dati volte a consentire l'uso dei loro dati non personali, senza la richiesta o la ricezione di un compenso che vada oltre la compensazione dei costi sostenuti per mettere a disposizione i propri dati, per obiettivi di interesse generale, stabiliti nel diritto nazionale, ove applicabile, quali l'assistenza sanitaria, la lotta ai cambiamenti climatici, il miglioramento della mobilità, l'agevolazione dell'elaborazione, della produzione e della divulgazione di statistiche ufficiali, il miglioramento della fornitura dei servizi pubblici, l'elaborazione delle politiche pubbliche o la ricerca scientifica nell'interesse generale».

²⁷ http://data.europa.eu/cli/reg_impl/2023/138/oj

²⁸ <http://data.europa.eu/cli/reg/2022/868/oj>

Sono state create figure nuove di intermediari definiti “organizzazioni per l’altruismo dei dati”, con natura non profit, che agevoleranno la raccolta e la distribuzione dei dati contribuiti volontariamente, creando così un nuovo indotto capace di alimentare l’ecosistema degli open data.

6. La normativa italiana

La normativa italiana, con ritardo, implementa la direttiva del 2003 (2003/-98/CE - PSI) mediante il d.lgs. 36/2006²⁹ e mediante il d.lgs. 102/2015³⁰ applica le modifiche introdotte dalla direttiva 2013/37/UE. L’Italia introduce inoltre nel CAD (Codice dell’Amministrazione Digitale d.lgs. 82/2005³¹) le definizioni di formato aperto e dati di tipo aperto³². La definizione di “formato aperto” tratteggia le condizioni tecnologiche di come produrre i dataset. La definizione di “dati di tipo aperto” (open data) regola le procedure organizzative e giuridiche per il rilascio dei dati, includendo la licenza giuridica e i metadati di annotazione, in tal modo chi legge la definizione ha immediatamente chiaro al lettore (si veda la definizione in nota).

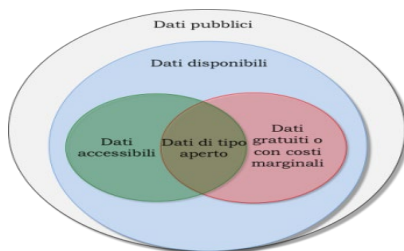


Figura 4: Grafico tratto dalle linee guida Agid³³

Tale materia è molto complessa quando si tratta di Open Government Data poiché intervengono elementi di diritto pubblico; in particolare occorre citare la legge 241/1990³⁴ sull’accesso agli atti. La legge 241/1990 definisce le riserve e

²⁹ https://www.normattiva.it/eli/stato/DECRETO_LEGISLATIVO/2006/01/24/36/CONSOLIDATED

³⁰ https://www.normattiva.it/eli/stato/DECRETO_LEGISLATIVO/2015/05/18/102/CONSOLIDATED/

³¹ https://www.normattiva.it/eli/stato/DECRETO_LEGISLATIVO/2005/03/07/82/CONSOLIDATED/

³² Art. 1, d.lgs. 82/2005, consolidato al 2026, comma 1, “l-bis) formato aperto: un formato di dati reso pubblico, documentato esaurientemente e neutro rispetto agli strumenti tecnologici necessari per la fruizione dei dati stessi; l-ter) dati di tipo aperto: i dati che presentano le seguenti caratteristiche: 1) sono disponibili secondo i termini di una licenza o di una previsione normativa che ne permetta l’utilizzo da parte di chiunque, anche per finalità commerciali, in formato disaggregato;”

³³ <https://docs.italia.it/AgID/documenti-in-consultazione/lg-opendata-docs/it/bozza/principi-general/requisiti-comuni.html>

³⁴ <https://www.normattiva.it/eli/stato/LEGGE/1990/08/07/241/CONSOLIDATED>

le eccezioni al paradigma open data. Dall'altra troviamo il d.lgs 33/2013³⁵ sulla trasparenza amministrativa che definisce l'accesso civico ai dati e documenti della pubblica amministrazione senza dover giustificare con un legittimo interesse la richiesta. Un tema molto importante da affrontare quando si trattano gli open data è l'analisi della competenza degli enti nel trattare i dati. Una pubblica amministrazione può rilasciare infatti i dati di cui è in possesso se ne ha la competenza giuridica dettata dalle funzioni statutarie e di legge. Per esempio, l'ISTAT³⁶ ha la competenza esclusiva di rilasciare i dati statistici in open data anche se i comuni li raccolgono localmente. Abbiamo sicuramente profili legati alla disciplina della protezione dei dati personali³⁷ e della proprietà intellettuale dei dati.

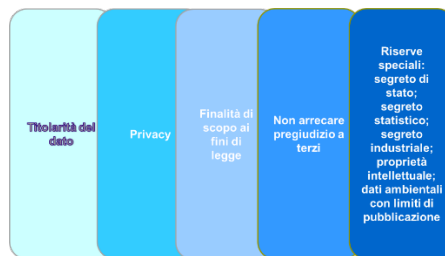


Figura 5: Ambiti giuridici da esaminare nell'Open data

7. Le linee guida

In questa materia elementi tecnologici, giuridici, e organizzativi si intersecano con un grado di complessità che richiede competenze interdisciplinari. Per questo motivo gli Stati membri hanno creato linee guida per aiutare gli enti pubblici ad applicare in modo corretto il paradigma Open Data. Anche l'Italia ha elaborato nel tempo diverse versioni di linee guida ora aggiornate e disponibili³⁸.

7.1 I formati aperti

I formati aperti dei dati, dal punto di vista tecnologico, sono definiti nell'allegato B delle linee guida e possiamo riassumerli come segue:

³⁵ https://www.normattiva.it/eli/stato/DECRETO_LEGISLATIVO/2013/03/14/33/CONSOLIDATED

³⁶ <https://www.istat.it/>, Istituto nazionale di statistica.

³⁷ EU Commission, The Symbiosis between Data Protection and Open Data, 2024, <https://data.europa.eu/sites/default/files/report/The%20Symbiosis%20between%20Data%20Protection%20and%20Open%20Data.pdf>

³⁸ https://www.agid.gov.it/sites/default/files/repository_files/lg-open-data_v.1.0_1.pdf

Format	Non-proprietary	Machine readable	Achievable stars
RDF	Yes	Yes	☆☆☆☆
XML	Yes	Yes	☆☆☆
JSON	Yes	Yes	☆☆☆
CSV	Yes	Yes	☆☆☆
ODS	Yes	Predominantly	☆☆☆
XLSX	Yes	Predominantly	☆☆☆
XLS	No	Predominantly	☆☆
TXT	Yes	Predominantly	☆☆*
HTML	Yes	Predominantly	☆☆*
PDF	Yes	No	☆☆
DOCX	Yes	No	☆☆
ODT	Yes	No	☆☆
PNG	Yes	No	☆☆
GIF	No	No	☆☆
JPG/JPEG	No	No	☆☆
TIFF	No	No	☆☆
DOC	No	No	☆☆

Figura 6: Tabella esemplificativa dei formati aperti così come illustrati nelle linee guida Agid

Come si può osservare (Figura 6), non tutti i formati tecnologici sono idonei per essere annoverati come open data. In rosso quelli che sono non idonei, in giallo quelli che solo parzialmente lo sono ed infine quelli verdi che sono pienamente conformi ai requisiti dell'open data.

7.2 I metadati

Pilastro essenziale degli Open Data sono i metadati ossia le informazioni sulla natura dei dati per fornire il contesto in cui sono stati creati. A livello europeo è stata definita un'ontologia per classificare i dati mediante un vocabolario di metadati uniforme per tutto lo spazio europeo. Questo vocabolario è chiamato DCAT-AP e ogni Stato membro ha sviluppato il proprio profilo DCAT-AP_IT³⁹ per adeguare il vocabolario alle esigenze dei servizi italiani.

Gli elementi obbligatori:

- Identificativo del dataset;
- Titolo del dataset;
- Descrizione del dataset;
- Data di ultima modifica del dataset;
- Tematica del dataset;
- Titolare del dataset;

³⁹ https://github.com/giorgialodi/Guida-pratica-DCAT-AP_IT?tab=readme-ov-file; <https://www.dati.gov.it/content/dcat-ap-it-v10-profilo-italiano-dcat-ap-0>

- Frequenza di aggiornamento del dataset;
- Distribuzione del dataset.

Punteggio qualità metadati (data.europa.eu)

4.00 — **Esccellente**

Approfondisci

Disponibilità Parcheggi (VIGENTE)

Titolare - Nome* Comune di Bologna - Innovazione Digitale e Dati	Titolare - Codice Ipa/P. Iva* c._8964
Editore Comune di Bologna - Innovazione Digitale e Dati	Editore - Codice Ipa/P.Iva c._8964

Descrizione*

Disponibilità parcheggi pubblici a Bologna, orario vigente. Le rilevazioni vengono effettuate ogni 10 minuti. Viene segnalata solo l'ultima rilevazione. Lo storico delle rilevazioni è disponibile al seguente dataset (https://opendata.comune.bologna.it/replora/dataset/disponibilita_parcheggi-storico/informazioni/)

URI*

https://opendata.comune.bologna.it/api/v2/catalog/dataset/disponibilita_parcheggi-storico/informazioni/

Termini*

[Governo e settore pubblico](#)

[Trasporti](#)

Parole chiave

OK

Data di rilascio

2020-02-14

Frequenza di aggiornamento*

ALTRO

Data di ultima modifica*

2020-02-14

Figura 7: Metadati nel portale italiano dei dati aperti relativi a un dataset del Comune di Bologna

Vi sono altri vocabolari di metadati per annotare i dati specifici, per esempio quelli geografici, considerando che i dati geospaziali sono considerati di altro valore. Il vocabolario GeoDCAT-AP fornisce infatti una sintassi RDF per i metadati INSPIRE e ISO 19115.

7.3 Le licenze standard

Un elemento essenziale che connota gli open data è la licenza aperta, ossia che consenta il riuso con il minimo grado di restrizioni e consenta sempre di rilevare l'attribuzione dell'autorità o dell'agente autore del dataset. Occorre specificare che i dataset, sotto il profilo della proprietà intellettuale, sono regolati in Europa dalla normativa delle banche dati (Direttiva 96/9/CE e Direttiva Copyright 2019/790). Tuttavia, esistono due tipologie di banche dati: quelle che rappresentano una creazione originale e quelle che non lo sono. Le prime sono tutelate dal diritto d'autore, le seconde sono regolate dal diritto *sui generis* che tutela il costituente della banca dati con diritti più deboli. Se quindi il dataset è creativo e originale (e.g., bibliografia, catalogo, selezione, elaborazione, scelta e ragionata di dati), si possono applicare gli istituti del diritto d'autore. Se invece il dataset è privo di originalità e non è intervenuta l'opera intellettuale di creatività, allora siamo di fronte a dataset che non sono protetti dal diritto d'autore ma dal diritto del costituente.

Spesso i dataset appartengono alla categoria delle banche dati creative e quindi dotate di natura tale da essere protette dal diritto d'autore. Se tuttavia ci troviamo davanti a dataset prodotti meccanicamente, mediante sensori, senza intervento di esperti, allora si potrebbe ipotizzare la tutela mediante il solo istituto del diritto sui generis.

Dal recente report pubblicato dalla Commissione Europea⁴⁰ viene in luce una proliferazione di licenze presenti nel catalogo europeo dell'ordine delle migliaia. Spesso trattasi di licenze nazionali secondo la giurisdizione dei singoli Stati membri. Tuttavia, la più utilizzata risulta la cc-by 4.0 che appartiene alla grande famiglia delle Creative Commons (CC)⁴¹. Le Creative Commons sono licenze permissive che utilizzano gli istituti del diritto d'autore per limitare le privative e quindi favorire il riutilizzo.

Ogni licenza delle Creative Commons è espressa mediante un'icona composta da diversi simboli che rappresentano i permessi, gli obblighi, i requisiti (Figura 8). By indica la richiesta di indicare l'autore, SA indica l'obbligo di riutilizzare l'opera con la medesima licenza, NC indica che è vietato il riuso a scopi commerciali, ND indica che è vietato derivare altre opere,

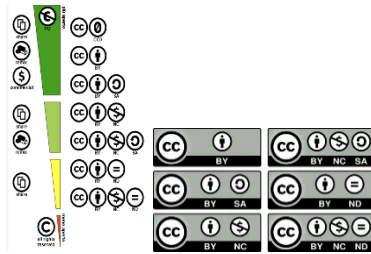


Figura 8: Tipologie di licenze CC⁴²

Non tutte le licenze CC sono una valida opzione per l'apertura dei dati così come regolata in Europa. Qui riportiamo una tabella che indica in verde quelle che sono compatibili con i principi di apertura, riuso, anche a scopi commerciali, dei dataset nel paradigma Open Data.

Si può notare (Figura 9) infatti che le licenze CC che portano il simbolo ND e NC sono considerate licenze compatibili per l'apertura dei dati perché ne limitano fortemente il riuso a seconda della finalità (non commerciale) o del processo di riuso (manipolazione, estrazione, modificazione).

⁴⁰ H. GRAUX, *Report on licence usage on the data.europa.eu portal*, January 2025, <https://data.europa.eu/sites/default/files/report/Report%20on%20licence%20usage%20on%20the%20data.europa.eu%20portal.pdf>

⁴¹ <https://creativecommons.it/chapterIT/>

⁴² Da Wikipedia, https://commons.wikimedia.org/wiki/File:Creative_commons_tipos.jpg.

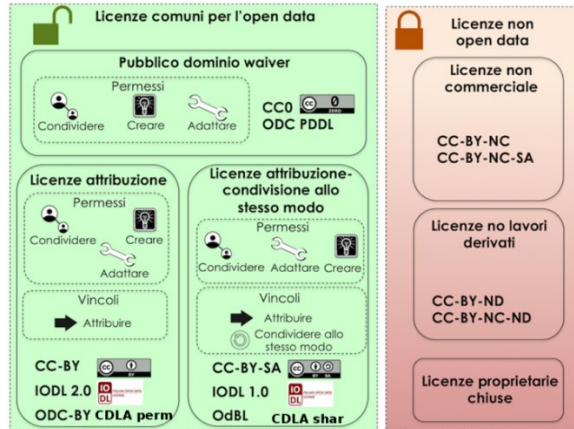


Figura 9: Tabella delle licenze ammissibili nel paradigma open data

7.4. Linked Open Data

Non tutti i dataset hanno la stessa qualità. Esiste una scala di misura di qualità definita dallo stesso inventore del Web, che utilizza diverse caratteristiche per qualificare la bontà dei dati. L'aderenza a questi parametri consente di produrre un prodotto finale che si integra con le tecnologie del Semantic Web. Tale tecnica si chiama Linked Open Data (LOD) e denota la presenza di caratteristiche tecnologiche descritte nella Figura 10. Un dataset deve innanzitutto avere una licenza aperta (una stella), poi deve essere rappresentato in un formato *machine-readable* (due stelle), successivamente il dataset deve utilizzare un formato aperto (tre stelle) e un nome univoco persistente nel tempo denominato URI-Uniform Resource Identifier- (quattro stelle). Infine, per raggiungere le cinque stelle i dati devono essere annotati con un'ontologia formale standard mediante un formato RDF. Nella Figura 8 si vede come la qualità crescente dei dati è proporzionale all'efficienza dei servizi erogati.

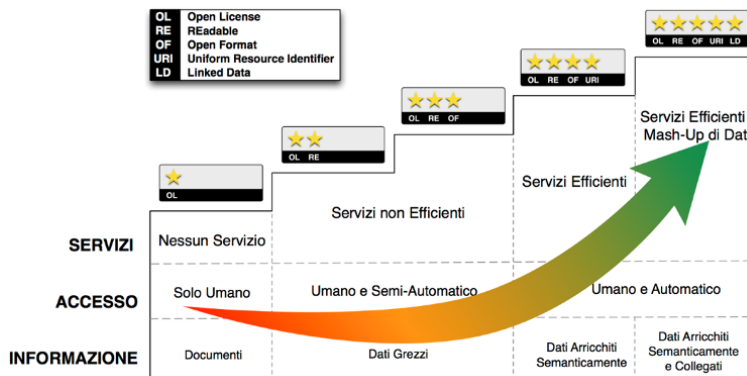


Figura 10: Scala del Linked Open Data (LOD)

Le stesse licenze Creative Commons sono in LOD ed è consigliato di annotare i dataset con la stessa metodologia anche per le licenze. Ogni dataset ha il link al testo giuridico della sentenza, nel contempo le CC hanno sviluppato un meccanismo visuale formato dalla composizione di più icone. Ciascuna icona rappresenta un permesso, un obbligo, una richiesta. L'icona non è una semplice annotazione visiva, è una prescrizione sintetica normativa. Poiché le icone non sono leggibili chiaramente nel loro significato giuridico dalle macchine, accanto al codice dell'icona si inseriscono delle istruzioni RDF (asserzioni) che specificano al computer le condizioni normative della licenza (Figura 11). In questo modo si potranno filtrare dal catalogo tutti i dataset che hanno una certa licenza. Oppure si potrà richiedere la compatibilità giuridica di due o più dataset confrontando il codice corrispondente alle licenze.

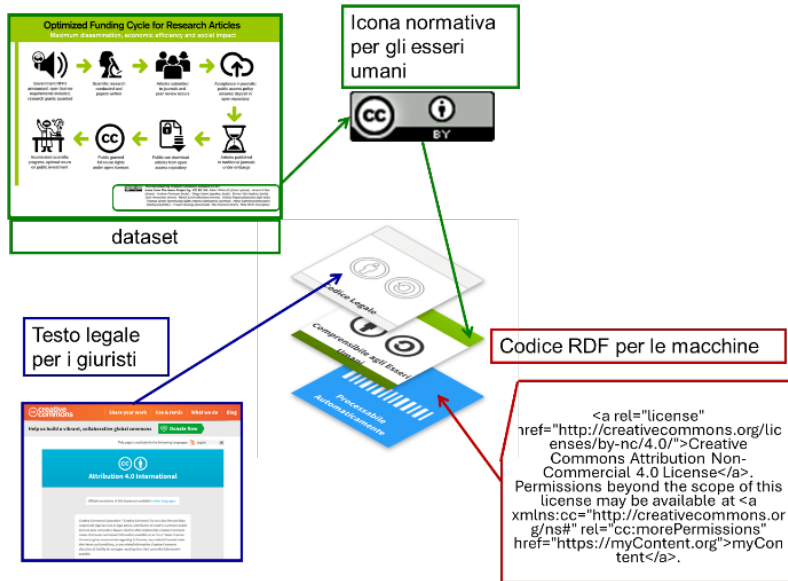


Figura 11: Meccanismo delle Creative Commons che implementa il paradigma LOD

8. I cataloghi di Open Government Data

Il movimento mondiale dell'Open Government Data si articola anche attraverso un meccanismo di pubblicazione dei dataset mediante portali chiamati cataloghi nei quali è possibile consultare i dati in diversi formati, le licenze sono chiaramente indicate e i metadati curati con dettaglio.

The image shows two web portals. The top portal is the 'Updated data.europa academy - out now' with a search bar and several informational cards: 'Guida alla ricerca di set di dati', 'Maturità dei dati aperti', 'Qualità dei metadati', 'Storie di dati', 'Accademia', 'Canale per le collaborazioni', 'Bulk download', 'Raccogli dati', and 'Studi'. The bottom portal is 'dati.gov.it' (i dati aperti della pubblica amministrazione) with a search bar, filters for 'Catalogo: Comune di Bologna', 'Sportello unico dati protetti DGA', and 'Categorie HVD'. It displays search results for 'Disponibilità Parcheggi (STORICO)' with various data format icons like CSV, JSON, OCTET, GeoJSON, GPX, KML, PARQUET, RDF_XML, JSON_LD, RDF_TURTLE, N3, SHP, and NLS.

Figura 12: Catalogo europeo e catalogo italiano dei dati aperti

Esiste un meccanismo di propagazione delle informazioni secondo un modello federato dei cataloghi per evitare duplicazioni dannose al principio di aggiornamento e certezza del dato. In sintesi, dalla periferia gli enti che sono più prossimi per competenza alla cura dei dati mettono a disposizione dei cataloghi dove trovare i dati senza duplicarli. I cataloghi dialogano fra loro, in verticale (Comune, Regione, Stato, Europa) e in orizzontale (catalogo generale, catalogo specifico dei dati geografici). Questo consente al catalogo nazionale di raccogliere le informazioni e i metadati (inclusi i link alle sorgenti originali dei dati) e di diffonderli al portale europeo⁴³. La Figura 13 mostra proprio come i geodati

⁴³ <https://data.europa.eu/it>

sono collegati al catalogo italiano che poi li trasmette al portale europeo. Solo i metadati sono trasmessi, mentre i dataset rimangono presso la sorgente primaria.

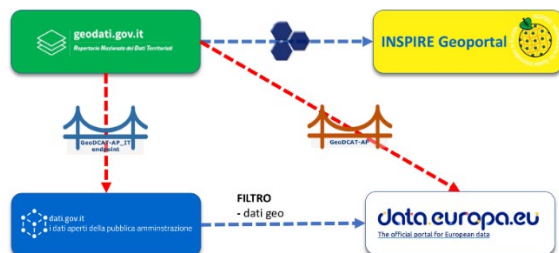


Figura 13 – Meccanismo di propagazione delle informazioni open data⁴⁴

La Figura 14 mostra la strategia europea per poter concentrare su un unico catalogo europeo tutti i dataset open data europei e favorire così lo sviluppo economico, il riuso dei dati nella ricerca, la condivisione fra pubbliche amministrazioni europee.

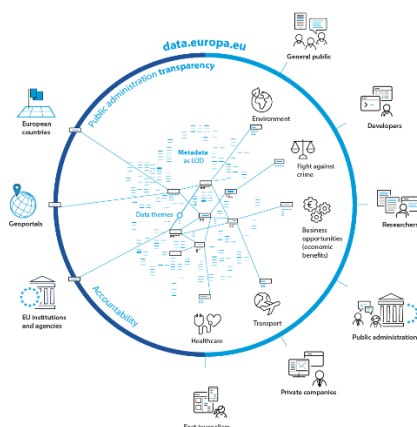


Figura 14 – Ecosistema dei dati aperti secondo la visione della strategia europea⁴⁵

9. Il benchmarking

Uno degli elementi essenziali del paradigma open data è il carattere internazionale e distribuito che connota l'incrocio dei dati provenienti da diverse fonti, creando un ecosistema di dati utili a diversi scopi: dalla ricerca, all'erogazione di servizi per i cittadini e le imprese, e per lo sviluppo economico delle imprese.

⁴⁴ <https://docs.italia.it/AgID/documenti-in-consultazione/lg-opendata-docs/it/bozza/pubblicazione-e-strumenti-di-ricerca/strumenti-per-la-ricerca.html>

⁴⁵ Dal portale Europeo <https://data.europa.eu/en/publications/datastories/linking-data-data-europaeu>

Per questo motivo, già dalla sua nascita, sono stati creati indici di misura delle politiche di supporto, del grado di accessibilità mediante portali specializzati, della qualità dei dati, e del loro impatto nella società. La Commissione europea ha istituito un indice di maturità dell'open data⁴⁶ per misurare i progressi non solo nei confronti degli Stati membri, ma includendo anche stati associati (Norvegia, Islanda, Svizzera) e stati limitrofi quali l'Albania, la Bosnia Erzegovina, il Montenegro, la Macedonia del Nord, la Serbia, l'Ucraina.

L'Italia sin dai primi momenti ha sviluppato una comunità degli open data molto rilevante, promossa sia da gruppi e associazioni di attivisti, sia da parte degli enti locali, creando così un'esigenza di attenzione da parte del legislatore nazionale, il quale ha inserito l'Open Data come elemento fondante della Trasformazione Digitale dell'agenda italiana⁴⁷.



Figura 15: Indici per la misurazione della maturità degli open data⁴⁸

Siamo posizionati nella rosa dei trascinatori dell'open data a livello europeo ed internazionale. Altri indici, infatti, misurano lo stato di salute degli open data governativi e delle pubbliche amministrazioni a livello mondiale quali il Barometro degli Open Data promosso dalla Web Foundation⁴⁹.

10. L'ecosistema open government data

Il paradigma open government data non è pensato per essere unidirezionale, dall'amministrazione verso il cittadino, ma è invece un ecosistema che realizza il concetto di co-progettazione insieme ai portatori di interessi del territorio. La Figura 16 mostra questo ecosistema, formato dalla pubblica amministrazione che rilascia i dati, dai cittadini che verificano la qualità dei dati e suggeriscono le priorità utili per il territorio, le imprese arricchiscono i dati con metadati e ontologie per rendere questi preziosi materiali utili per lo sfruttamento economico.

⁴⁶ <https://data.europa.eu/en/open-data-maturity/2025>

⁴⁷ <https://www.agid.gov.it/it/ambiti-intervento/open-data>

⁴⁸ <https://data.europa.eu/en/open-data-maturity/2025>

⁴⁹ <https://webfoundation.org/our-work/projects/open-data-barometer/>

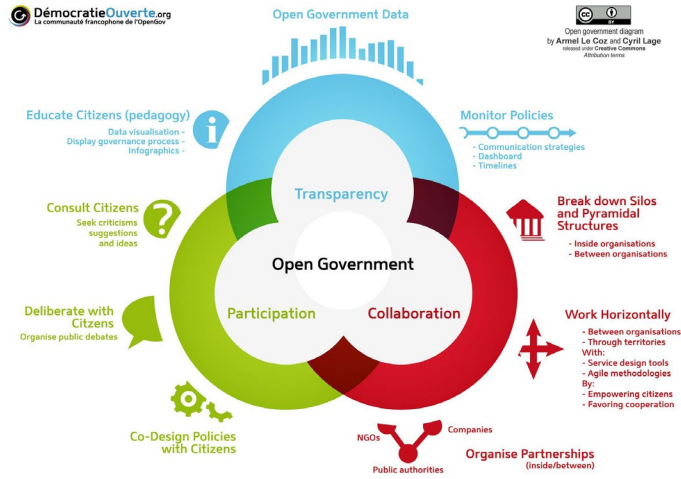


Figura 16: Schema dell'ecosistema degli Open Government Data

Per mantenere la qualità dei dati, occorre avere un processo ciclico della cura dei dati che parte dall'inventario dei dati interni ad ente, prosegue con l'analisi delle priorità legate al territorio mediante momenti di co-progettazione. Definite le priorità, si devono analizzare i dati dal punto di vista giuridico ed etico. Successivamente si devono pulire i dati e annotarli con i metadati per poterli poi pubblicare negli appositi portali capaci di diffondere gli indici ai cataloghi nazionali e successivamente al portale europeo.



Figura 17: Ciclo di vita del processo open data

11. I digital twin basati sugli open data

Gli open data stanno diventando particolarmente importanti per il monitoraggio delle città intelligenti, realizzando uno strumento denominato digital twin o gemello digitale che utilizza i dati raccolti dai molti sensori sparsi per la città al fine di riprodurre un modello digitale nel quale poter monitorare, misurare, prevedere i comportamenti globali nel territorio. Un chiaro esempio di digital twin lo abbiamo nella città di Amsterdam (Figura 18) che usa gli open data per monitorare il consumo energetico e bilanciare così l'erogazione di energia⁵⁰.



Figura 18: Digital Twin di Amsterdam per il monitoraggio del consumo energetico

Analogamente il portale Globalforestwatch (Figura 19) fornisce, mediante gli open data, un monitoraggio dello stato della deforestazione per ogni paese del mondo⁵¹.



Figura 19: Deforestazione della Finlandia monitorata mediante open data

⁵⁰ <https://www.geodan.com/knowledge-and-innovation/managing-urban-processes-intelligently-with-the-amsterdam-smart-city-dashboard/>

⁵¹ <https://www.globalforestwatch.org/dashboards/country/FIN/>

Analogamente <https://www.checkmyfloodrisk.co.uk/> (Figura 20) monitora in tempo reale lo stato di inondazione del Regno Unito.

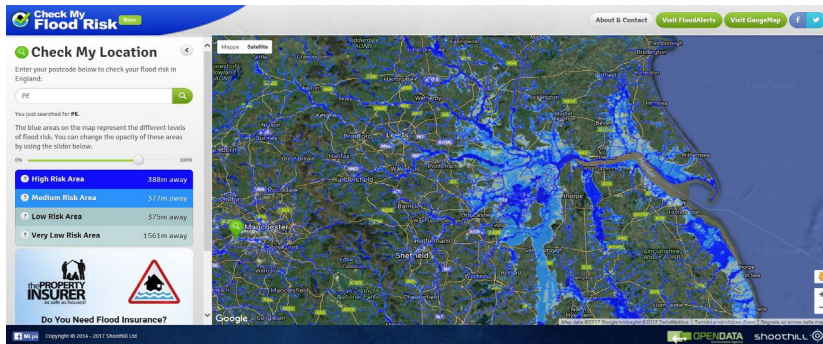


Figura 20: Mappa del rischio di inondazione basata sugli open data

12. Conclusioni

Il fenomeno dell'Open Data è un complesso insieme di processi che coinvolgono diverse discipline e saperi, anche all'interno della stessa analisi giuridica serve una metodologia trasversale che utilizza competenze di diritto pubblico, diritto europeo, diritto delle tecnologie, diritto d'autore e privacy. A questo si devono aggiungere competenze tecnologiche per governare i formati, i metadata, l'architettura di propagazione dei cataloghi e della metodologia LOD. Occorre infine ricordare che il quadro normativo della Strategia europea dei dati si arricchisce dinamicamente di nuovi regolamenti che integrano la visione originale dell'Open Data. L'utilizzo, inoltre dell'intelligenza artificiale rende questi dataset preziosi e strategici per realizzare, anche se in piccola parte, il diritto alla sovranità dei dati. I principi FAIR e CARE sostengono diritti fondamentali dei cittadini, delle imprese e delle società a ottenere i dati, poterli riusare e anche rivendicarne la certificazione etica.

INVESTIGARE I DATI INFORMATICI: LA *DIGITAL FORENSICS* TRA NORME GIURIDICHE, STANDARD TECNICI E INNOVAZIONI TECNOLOGICHE

Raffaella Brighi, Michele Ferrazzano

SOMMARIO: 1. Introduzione. 2. Evoluzione e ambiti dell'informatica forense. 3. Le proprietà del dato informatico: elementi rilevanti per l'informatica forense. 4. L'importanza del metodo scientifico nell'informatica forense. 5. La *digital evidence*. 6. Norme, standard e best practice nella *digital forensics*. 7. Le fasi del trattamento del reperto informatico. 8. Il ruolo di esperti di informatica forense e dei laboratori certificati di digital forensics. 9. Prospettive di utilizzo di soluzioni di IA nelle investigazioni di *digital forensics*. 10. Conclusioni.

1. Introduzione

In un contesto socio-tecnologico ormai pervaso da una connettività ubiqua, la cosiddetta “società dei sensori”, l'attività giurisdizionale si avvale sempre più di informazioni desunte dai dati conservati nei dispositivi digitali e trasmessi attraverso le reti.

Processi di datificazione, frutto di una raccolta continua, automatizzata e potenzialmente illimitata di informazioni, convertono ogni aspetto dell'esperienza umana – dagli spostamenti ai consumi, dalle relazioni alle emozioni – in flussi di dati digitali che circolano nelle reti globali. Tracce digitali prodotte da azioni consapevoli dell'utente oppure generate automaticamente dai sistemi (log di rete, file temporanei, frammenti di documenti cancellati) si trovano in ‘luoghi’ fino a poco tempo fa impensabili: telecamere di sorveglianza, stampanti 3D, dispositivi biomedicali – basti pensare ai pacemaker che trasmettono parametri clinici in remoto. Questa massa informativa riveste un ruolo cruciale nelle moderne attività investigative perché ogni sistema che elabori dati digitali può essere tecnicamente analizzato al fine di ricavarne informazioni rilevanti da utilizzare come elemento di prova in procedimenti giudiziari¹. Il fenomeno ha riguardato innanzitutto i reati legati all'informatica: reati informatici², ad esempio le

¹ M. FERRAZZANO, *Dai veicoli a guida umana alle autonomous car. Aspetti tecnici e giuridici, questioni etiche e prospettive per l'informatica forense*, Torino: Giappichelli, 2018.

² Alcune importanti fattispecie di reato, legate strettamente all'informatica, sono state introdotte

frodi informatiche, il falso informatico, l'accesso abusivo, il danneggiamento di dati e sistemi informatici oppure anche reati non "necessariamente" informatici ma attuati attraverso strumenti informatici³. Oggi, tuttavia, è diventato necessario, in fase di indagine, porre attenzione ai dispositivi digitali anche in fattispecie di reato non inerenti all'informatica. Il ricorso a informazioni desunte dai dati digitali si è esteso in via definitiva a qualsiasi contesto in cui diventi necessario produrre, a sostegno della propria tesi, quelle che sono "rappresentazioni informatiche" di fatti (ad esempio e-mail, messaggi, post su piattaforme web): nel processo civile, in ambito giuslavorista, in materia di diritto amministrativo, ma anche nelle investigazioni aziendali (Corporate Digital forensics), allo scopo di individuare eventuali attacchi informatici provenienti dall'esterno, scoprire dipendenti infedeli, attività di spionaggio, furto o danneggiamento dei dati, violazione delle policy aziendali.

Allo stesso tempo, si registra un progressivo aumento quantitativo e qualitativo di minacce e attacchi informatici che hanno impatti significativi su comunità, istituzioni e imprese. L'informatica ha offerto nuove opportunità anche alle organizzazioni criminali che, a fronte di eterogeneità di target e motivazioni (finanziaria, terroristica, predatoria) sfruttano la complessità delle infrastrutture informatiche e di rete. L'accertamento dell'accadimento di un fatto illecito e l'individuazione del suo autore risultano sempre più complessi, a causa della diffusione di strumenti e tecnologie che ostacolano l'attività investigativa: tra questi si annoverano i meccanismi di anonimato, la virtualizzazione, la crittografia, le tecniche anti-forensi, l'ubiquità degli spazi di archiviazione, le architetture distribuite e, più in generale, la crescente ampiezza e diversificazione delle sorgenti di dati digitali⁴.

nel nostro ordinamento dalla legge del 23 dicembre 1993, n. 547 parzialmente modificata dalla legge 18 marzo 2008, n. 48 in attuazione della Convenzione di Budapest del 2001. Si tratta dei c.d. reati (necessariamente) informatici, ovvero reati che presentano «espressamente, sul piano della loro formulazione letterale, elementi di tipizzazione descrittivi di modalità, oggetti, attività caratterizzanti dalla, o frutto, della tecnologia informatica, vale a dire impicanti, connessi o relativi a procedimenti di elaborazione automatizzata di dati, secondo programmi informatici», in L. PICOTTI, *La nozione di criminalità informatica e la sua rilevanza per le competenze penali europee*, in *Riv. Trim. dir. Pen. Ec.*, 2011 (4), pp. 827 ss.

³ Reati come la pedopornografia, gli atti persecutori, la diffamazione e il bullismo trovano nella dimensione online nuove forme; accanto a questi le estorsioni, sempre più diffuse nella modalità di sextorsion e ransomware, i reati di sostituzione di persona o lo spionaggio coniugano fattispecie tradizionali con reati nati digitali, andando a incrementare, secondo una concezione più ampia e elastica, il perimetro dei c.d. computer crime. Il quadro giuridico, molto vario e di difficile ricostruzione, ricomprende tentativi di adeguare fattispecie esistenti a nuove realtà tecnologiche, tentativi di applicare vecchie fattispecie a condotte che avvengono online, e interventi d'urgenza in reazione a gravi fatti di criminalità (uno tra tutti la modifica all'art. 612 bis c.p. in tema di cyberstalking).

⁴ R. BRIGHI, *Sfide recenti e nuovi paradigmi dell'Informatica forense*, in ID. (a cura di), *Nuove questioni di informatica forense*, Roma: Aracne, 2022, pp. 17-39.

In sintesi, il dato digitalizzato si configura quale fulcro dell'attività investigativa contemporanea: esso non solo documenta il passato, ma consente di anticipare tendenze criminose, ridefinendo il rapporto fra diritto alla sicurezza e tutela della privacy in un ecosistema informativo senza precedenti.

2. Evoluzione e ambiti dell'informatica forense

L'informatica forense è la scienza forense che definisce le modalità di individuazione, acquisizione e interpretazione dei dati digitali da dispositivi informatici e reti per ricavarne elementi di prova utili all'attività investigativa o prove spendibili nelle sedi processuali e valutabili dal giudice. È dunque una scienza forense al pari di altre scienze (come la medicina legale o la chimica forense): a differenze delle altre, però, l'informatica è oggi talmente presente nella vita di tutti noi che una prova informatica è ormai rinvenibile in quasi tutti i processi.

Originariamente comparsa negli Stati Uniti sotto il nome di *Computer forensics* (quando informatica era sinonimo solo di computer) per far fronte all'incremento della domanda di analisi dei dati digitali a fini di giustizia, oggi è soppiantata dalla più ampia definizione di *Digital forensics* che si può declinare in diverse specializzazioni tra cui le principali sono *disk forensics* per l'esame di supporti di memorizzazione, *network forensics* in contesto di esame di dati in rete, *web forensics* per dati relativi a pagine web, *mobile forensics* per i dispositivi mobili e così via per altri ambiti specialistici.

Se in un primo momento l'attenzione era rivolta solo ai casi di rilevanza penale e in particolare per i reati informatici in senso stretto (come, ad esempio, l'accesso abusivo a sistema informatico), nel corso degli anni è stato compreso come la portata della disciplina è ben più ampia riguardando tutte le situazioni nelle quali il dato informatico è un elemento probatorio.

Nella letteratura scientifica italiana le prime definizioni risalgono all'inizio degli anni 2000, quando si è iniziato a utilizzare il termine *informatica forense*⁵. A partire da queste prime definizioni, i confini della materia si sono prepotentemente dilatati, spinti dalla sempre crescente dipendenza della società moderna dalle tecnologie informatiche⁶.

⁵ La definizione che si attribuisce a Cesare Maioli è precedente al 2004. C. MAIOLI, *Dar voce alle prove: elementi di informatica forense*, in P. POZZI (a cura di), *Crimine virtuale, minaccia reale*, Milano: Franco Angeli, 2004. Per una introduzione di ruolo, principi e metodi della informatica forense si veda anche G. ZICCARDI, *L'ingresso della computer forensics nel sistema processuale italiano: alcune considerazioni informatico-giuridiche*, in L. LUPARIA (a cura di), *Sistema penale e criminalità informatica*, Milano: Giuffrè, 2009; P. PERRI, *Computer forensics (indagini informatiche)*, in *Digesto delle discipline penalistiche*, Torino: Utet, 2011; G. FAGIOLI, A. GHIRARDINI, *Digital forensics*, Milano: Apogeo Editore, 2020 e S. ATERNO *et al.* (a cura di), *Cyber Forensics e indagini digitali*, Torino: Giappichelli, 2021.

⁶ Sulle linee di ricerca più recenti si veda R. BRIGHI (a cura di), *Nuove questioni di informatica forense*, cit.

Le nuove competenze nell'intelligenza artificiale e nella *data science* si stanno, inoltre, unendo al campo della *Digital forensics* a supporto dell'analisi delle attività criminali e, più in generale, delle attività di *intelligence*⁷. La comprensione generale dei fenomeni e l'orientamento delle strategie investigative possono oggi essere efficacemente supportati dall'impiego di metodi e tecniche⁸, in grado di individuare relazioni e regolarità all'interno di grandi *dataset*, laddove le capacità analitiche umane si rivelerebbero inadeguate⁹.

La ricerca di soluzioni tecniche adeguate alle sfide poste dalla contemporaneità non può prescindere dal rispetto delle garanzie proprie del *giusto processo*. Qualunque innovazione nell'ambito delle attività tecniche deve necessariamente confrontarsi con il principio dell'utilizzabilità dibattimentale delle informazioni raccolte, le quali devono essere pienamente accessibili e valutabili da tutte le parti processuali, nel rispetto del contraddittorio e a tutela del diritto di difesa. In tal modo, si salvaguardano i diritti fondamentali delle persone coinvolte nel procedimento.

Al contempo, è necessario scongiurare il rischio che le indagini si traducano in «vere e proprie incursioni investigative nel nucleo più intimo dell'individuo»¹⁰, in cui soggetti privati – tra cui i fornitori di servizi digitali – assumano un ruolo determinante nel consentire l'accesso ai dati oggetto di accertamento. L'intermediazione di tali attori, ormai inevitabile nel contesto delle indagini digitali, impone un'attenta riflessione sul bilanciamento tra efficienza investigativa e tutela dei diritti fondamentali.

L'analisi forense presuppone che l'esaminatore abbia una profonda conoscenza dal punto di vista informatico del funzionamento del sistema di interesse, unendo competenze sistemistiche (dal funzionamento del sistema operativo alla modalità di organizzazione dei dati in un file system), di programmazione e ingegneria del software, di banche dati, oltre che competenze giuridiche necessarie per non invalidare il lavoro tecnico che può pure essere finemente svolto.

I dati contenuti nei dispositivi di memorizzazione devono essere salvati propriamente e spesso celermente, ossia raccolti e preservati quanto prima nel tempo rispetto all'accadimento dell'evento di interesse e senza che i contenuti presenti in essi vengano alterati. Per quanto possibile, è importante che durante l'esame dei reperti tutte le procedure siano controllabili e ripetibili: in altri ter-

⁷ E. CASEY, *The value of forensic preparedness and digital-identification expertise in smart society*, in *Digital investigation*, 2017 (22), pp.1-2.

⁸ Molteplici sono le tecniche utilizzate in tale ambito, tra le più note: il *data mining*, il *datawarehouse*, il *machine learning*, il *clustering*.

⁹ È questo il dominio della c.d. *Cyber Intelligence*.

¹⁰ Così si esprime R. ORLANDI in *Usi investigativi dei cosiddetti captatori informatici. Criticità e inadeguatezza di una recente riforma*, in *Riv. it. dir. proc. pen.*, 2018 (2), p. 539.

mini, qualsiasi esperto, anche indipendente o incaricato dell'attività tecnica in un secondo momento, deve essere in grado, leggendo i documenti e disponendo di una copia, di ripetere e verificare tutte le operazioni eseguite durante le indagini.

3. Le proprietà del dato informatico: elementi rilevanti per l'informatica forense

Nella pratica del procedimento giudiziario, la peculiare struttura dei dati digitali genera l'illusione che ciò che è rappresentato digitalmente sia indiscutibile, così come il significato attribuibile a tale rappresentazione. Ciò ci induce a credere acriticamente che una prova digitale sia idonea a sostenere il ragionamento logico-probatorio del giudice.

Il dato digitale è rappresentato per mezzo di sequenze di bit che assumono il valore di 0 (zero) oppure 1 (uno), non comprensibili all'uomo, che assumono significato diverso a seconda di come vengono interpretati. Pertanto, richiedono una serie di operazioni attraverso le quali si realizza una trasformazione che può portare a risultati diversi (visualizzati come testo su uno schermo o come video, o ancora come immagine stampata su carta). Senza interpretazione, i dati non possono avere alcun significato. Lo stesso dato informatico può essere visualizzato in maniera differente a seconda del sistema impiegato e degli algoritmi e *software* che ne hanno accesso: si pensi ad esempio a una pagina web che può essere mostrata graficamente oppure testualmente nel suo codice, oppure riprodotta con un lettore vocale o stampata su carta.

L'informazione in formato digitale possiede caratteristiche intrinseche che ne definiscono la natura e ne complicano la gestione in un contesto forense. In primo luogo, essa è *immateriale*¹¹, priva di una consistenza fisica autonoma e dipendente da un supporto di memorizzazione fisico (ad esempio, hard disk, SSD, memorie flash) per la sua esistenza¹². In secondo luogo, è caratterizzata da un'elevata *volatilità*, in quanto può essere alterata o irrimediabilmente cancellata con estrema facilità e rapidità¹³. Un'altra proprietà fondamentale è la *alterabilità*: i dati digitali possono subire modifiche, sia dolose che colpose, senza lasciare tracce evidenti dell'intervento. Infine, la loro *replicabilità* permette di generare un numero illimitato di copie identiche all'originale, sollevando questioni complesse riguardo all'autenticità e all'individuazione della fonte primaria.

¹¹ Si tratta in realtà di una materialità diversa: i dati constano comunque di elementi fisici, anche se *intangibili*. Cfr. S. PIETROPAOLI, *Informatica criminale*, Torino: Giappichelli, 2025, pp. 85-98.

¹² Il bit non si presenta in forma fisica e la sua archiviazione richiede un adeguato supporto in grado di mantenerne memoria e consentirne il successivo accesso.

¹³ In alcuni casi il dato digitale è facilmente disperdibile per le caratteristiche del supporto che lo contiene (ad esempio, i dati in memoria RAM di un sistema in esecuzione che viene spento).

Qualsiasi dato digitale, da un semplice documento di testo a un complesso file multimediale, è fondamentalmente rappresentato da una sequenza di bit (cifre binarie 0 e 1). Convenzioni standardizzate, come la codifica ASCII o Unicode, stabiliscono una corrispondenza univoca tra specifiche sequenze di bit e i caratteri alfanumerici. Ad esempio, una determinata stringa di testo corrisponde a una precisa successione binaria registrata su un dispositivo di archiviazione.

Un operatore con accesso al sistema può impartire comandi che modificano lo stato di questi bit, alterando così l'informazione originale. La criticità risiede nel fatto che un'analisi diretta del supporto a livello fisico, esaminando la sequenza di bit in un dato istante, non permette di per sé di determinare se tale sequenza sia stata modificata. La stringa binaria non conserva una cronologia intrinseca dei suoi stati precedenti; di conseguenza, non è possibile accertare, basandosi unicamente sulla sequenza stessa, se un singolo bit o un insieme di bit abbiano assunto valori diversi in passato.

Nel contesto processuale, le modalità di acquisizione, conservazione e analisi dei dati digitali sono frequentemente oggetto di contestazione. Tale scenario deriva dalla natura stessa dell'evidenza digitale, che risulta inaccessibile e incomprendibile ai non addetti ai lavori (si pensi, ad esempio, all'analisi di file di log di sistema per ricostruire attività illecite).

Procedure inadeguate, imperizia tecnica, scarse conoscenze o negligenza da parte degli operatori possono compromettere irrimediabilmente l'integrità del reperto. Ciò comporta il rischio concreto che il giudizio si fondi su elementi probatori identificati in modo errato, acquisiti con metodologie non forensi o conservati senza garantire la catena di custodia. Tali carenze procedurali possono inficiare la validità di perizie e consulenze tecniche, rendendole inattendibili.

Analogamente a qualsiasi altra forma di prova, anche per l'evidenza digitale l'onere di dimostrarne l'autenticità e l'affidabilità ricade sulla parte che la introduce nel procedimento giudiziario. È pertanto imperativo che chi presenta un reperto digitale sia in grado di provare, attraverso una documentazione rigorosa e l'applicazione di metodologie forensi convalidate, che i dati non siano stati alterati dal momento del loro sequestro fino alla loro presentazione in giudizio.

La presunzione di ripudio non va intesa come una generale dichiarazione di inattendibilità del dato informatico. Esistono infatti strumenti che consentono di verificare l'integrità e l'attendibilità del dato digitale come, ad esempio, la firma digitale o la PEC. Tuttavia, la maggior parte dei dati che confluisce in un procedimento giudiziario non nasce e non è concepita nell'ottica di un uso forense. Per tali ragioni, è errato ritenere aprioristicamente privo di valore qualsiasi dato informatico introdotto nel processo. Spetta alla parte che lo produce l'onere di fornire dimostrazione della sua genuinità e attendibilità, anche attraverso elementi probatori di supporto, quali dati ulteriori o testimonianze coe-

renti. Simmetricamente, la parte che intende contestare tale elemento non può limitarsi a un disconoscimento generico, ma è tenuta a formulare una contestazione specifica, argomentando le ragioni della propria obiezione in modo puntuale e contestualizzato.

4. L'importanza del metodo scientifico nell'informatica forense

Il metodo scientifico costituisce il paradigma attraverso cui la scienza persegue una conoscenza della realtà che sia oggettiva, affidabile, verificabile e condivisibile, nei limiti delle capacità cognitive umane. Lo scienziato, avvalendosi del proprio bagaglio di conoscenze ed esperienze, formula enunciati di carattere generale e leggi nomotetiche. Tuttavia, nessuna legge scientifica, per quanto consolidata, può esplicitare esaustivamente la totalità delle variabili di un caso particolare sottoposto a giudizio. Il singolo evento processuale rappresenta infatti un *unicum* irripetibile, mentre la legge scientifica, per sua natura, si riferisce a una classe generale di fenomeni. Ne consegue una tensione intrinseca tra la generalità della scienza e la specificità del caso legale¹⁴.

All'interno del processo, le fasi di ammissione, assunzione e valutazione della prova si avvalgono di strumenti gnoseologici mutuati dalla scienza e dalla tecnica. Si tratta di principi metodologici, procedure tecnologiche e apparati tecnici il cui impiego richiede necessariamente competenze specialistiche. La sfida centrale consiste nel conciliare il ricorso a leggi scientifiche, per loro natura soggette a revisione continua in virtù del progresso tecnologico, con il pieno rispetto dei principi del giusto processo, in particolare del diritto di difesa. Tale equilibrio è fondamentale, poiché una sentenza di condanna può essere emessa solo qualora la colpevolezza dell'imputato sia accertata al di là di ogni ragionevole dubbio. L'aggettivo ragionevole postula un'oggettività basata su un'argomentazione logica e non contraddittoria. In materia di prova scientifica, ciò impone al giudice di esplicitare nella motivazione la propria valutazione critica del metodo impiegato, considerando il suo grado di controllabilità e attendibilità, la presenza di revisioni critiche da parte della comunità scientifica di riferimento e l'indicazione dei margini di errore noti¹⁵.

Traslando questi principi nel dominio della digital forensics, la natura stessa dell'evidenza digitale impone la considerazione di due elementi interconnessi. Il

¹⁴ Per approfondimenti si veda: M.C. TALLACHINI, *Scienza e diritto. Verso una nuova disciplina*, in S. JASANOFF, *La scienza davanti ai giudici. La regolazione giuridica della scienza in America*, Milano; Giuffrè, 2001, p. VI; S. HAACK, *Legalizzare l'epistemologia. Prova, probabilità e causa nel diritto*, Milano: Egea, 2015.

¹⁵ Si veda R. BRIGHI, C. MAIOLI, *Un cambio di paradigma nelle scienze forensi. Dall'armonizzazione tecnico-giuridica a una nuova cornice epistemologia*, in *Informatica e diritto*, 2015 (XXIV), pp. 217-234.

primo, di carattere metodologico, consiste nell'aderenza a standard e linee guida specifici del settore. Un criterio efficace per l'interazione tra informatica e diritto prevede che tali standard non impongano l'adozione di una tecnologia specifica, per non ostacolare l'innovazione, ma al contempo che le procedure operative delineate riflettano le pratiche consolidate e ampiamente accettate dagli esperti di informatica forense. Il secondo elemento è quello legato alla competenza dell'esperto, il quale applica il proprio giudizio tecnico ai dati digitali sin dalla fase di repertazione. Questa dimensione è cruciale, poiché un procedimento giudiziario può essere gravemente compromesso da una conoscenza inadeguata dei doveri e delle responsabilità legali che disciplinano il trattamento dei dati digitali, dalle conseguenze di una loro gestione impropria, nonché dalla mancata applicazione delle tecniche validate.

Gli specialisti di *Digital forensics* fanno riferimento a diverse linee guida, sia internazionali sia di settore, che stabiliscono i principi per la corretta gestione del reperto digitale. Si osserva nel tempo un'evoluzione di tali normative tecniche, che da un approccio iniziale marcatamente proceduralizzato e dettagliato si sono orientate verso una maggiore enfasi sulla definizione di una metodologia generale, sulla formazione interdisciplinare in informatica giuridica e sui principi deontologici.

In pratica, tuttavia, lo sviluppo e l'implementazione di procedure universali incontrano due ordini di limitazioni. Il primo è di natura tecnologica, legato alla costante diversificazione dei supporti di memorizzazione e all'ecosistema operativo in cui un dispositivo agisce. Il secondo è legato al fattore umano e agli obiettivi specifici perseguiti dai diversi attori del processo: per le forze dell'ordine, l'obiettivo primario sarà l'acquisizione di elementi utili all'indagine preservando l'integrità della prova; per l'autorità giudiziaria, sarà quello di correlare i risultati tecnici a fattispecie penalmente rilevanti; per il consulente tecnico, infine, l'obiettivo consisterà nel verificare che le procedure adottate siano state eseguite in modo conforme a garantire il corretto esercizio del diritto di difesa.

Il dibattito filosofico-giuridico per la comprensione e la risoluzione delle questioni giuridico-epistemologiche è stato spesso troppo astratto e, dunque, distante dal "sistema giustizia". Ciò ha portato a trascurare il rapporto tra i professionisti del diritto e gli scienziati forensi che, invece, è fondamentale per il bilancio complessivo dell'ecosistema delle scienze forensi. I tentativi di coordinamento descritti – protocolli operativi, best practices, standardizzazione – stanno tuttavia progressivamente indirizzando la definizione di una cornice epistemologica di riferimento anche per le scienze forensi.

5. La *digital evidence*

I dati digitali sono fatti elementari che per assumere significato necessitano di un'interpretazione per divenire comprensibili all'uomo. Per sua natura, il dato digitale ha le seguenti caratteristiche: è immateriale, per cui necessita di un supporto idoneo per contenerlo quali ad esempio CD-ROM, hard disk, chiavette USB; è volatile, in quanto può essere disperso facilmente; deteriorabile, perché modificabile in modo anche anonimo e/o involontario; è riproducibile in un numero potenzialmente infinito di copie. I rischi di alterazione coinvolgono anche gli stessi investigatori se non idoneamente preparati a svolgere un'indagine di informatica forense.

Per evitare confusione tra i concetti di “prova” e di “elemento di prova”, ai fini della trattazione si userà un termine che indica in maniera più ampia il concetto di dati che ha finalità di utilizzo come prova, ossia il termine “evidenza digitale” (“*digital evidence*”). Si può considerare *digital evidence* ogni dato informatico allocato su un particolare dispositivo oppure trasmesso da sistemi informatici e telematici che possa avere una rilevanza processuale. Ogni dato utilizzato per supportare o confutare una tesi è da definirsi evidenza digitale.

Le evidenze digitali si pongono in una posizione in cui perde consistenza la naturale propensione dell'uomo a rapportarsi al mondo reale con l'uso dei cinque sensi, in particolare il tatto, per cui appare più difficile far assumere rilevanza a questo genere di prove.

Eoghan Casey propone una definizione di *digital evidence* riferendosi a «qualsiasi dato memorizzato o trasmesso usando un computer che supporta o respinge una teoria su come è avvenuto un fatto offensivo o che individua elementi critici dell'offesa come l'intenzionalità o l'alibi». Se un tempo i dati venivano salvati esclusivamente nei dispositivi di memorizzazione digitali, collegati al sistema informatico fisicamente utilizzato dall'utente finale, oggi numerose informazioni sono delocalizzate da una singola postazione e conservate nel complesso in una rete all'interno del *cloud* o in generale in rete.

Come evidenziato in §3, la natura immateriale dei dati digitali li rende intrinsecamente più vulnerabili a manipolazioni e alterazioni rispetto alle fonti probatorie tradizionali. Questa caratteristica, spesso di difficile percezione, individuazione e documentazione, impone l'adozione di specifici accorgimenti tecnici e metodologici per garantirne l'affidabilità. Solo attraverso il rispetto di tali procedure è possibile conferire al dato digitale un adeguato valore probatorio nell'ambito processuale.

Alla luce degli aspetti citati, ogni prova digitale deve godere dei seguenti requisiti:

- *integrità*: nessuna delle attività svolte dovrebbe alterare i dati, salvo i casi

in cui l'acquisizione degli stessi richiede necessariamente l'adozione di procedure che comportino delle modifiche che dovranno comunque essere limitate al massimo;

- *autenticità*: il dato digitale deve presentarsi nella condizione in cui è stato originariamente acquisito;
- *completezza*: il dato informatico va acquisito insieme al suo contesto per poter esaurientemente comprenderne il valore probatorio, sia per le tesi di chi lo produce, sia per chi lo subisce;
- *affidabilità*: il dato informatico non deve risultare alterato e deve offrire tutte le garanzie per sgombrare ogni dubbio in merito alla loro autenticità e veridicità;
- *pertinenza*: il dato informatico deve parlare del caso per il quale è richiesto il suo contributo;
- *sufficienza*: il dato informatico deve essere raccolto in maniera sufficiente a poterne apprezzare il contributivo informativo;
- *documentazione*: gli operatori devono documentare dettagliatamente in merito alle operazioni svolte, agli strumenti adottati e alle motivazioni nei casi in cui più scelte fossero possibili, per consentire a un terzo di verificare ed esaminare quanto svolto.

6. Norme, standard e best practice nella digital forensics

A dare un impulso fondamentale all'inquadramento normativo dei molti problemi legati alla digital evidence è stato il Consiglio d'Europa, che ha promosso l'adozione della Convenzioni sulla criminalità informatica del 23 novembre 2001 (c.d. Convenzione di Budapest), che rappresenta il primo accordo internazionale su questi temi. La Convenzione, oltre a delineare numerosi crimini informatici, detta disposizioni sull'acquisizione, raccolta e conservazione della prova digitale. In particolare, la Convenzione impone alle parti aderenti di adottare misure tecniche dirette ad «assicurare la conservazione dei dati originali e ad impedirne l'alterazione». I dati acquisiti devono essere vagliati in dibattimento da tutte le parte del processo - normalmente a distanza di tempo – e, se non si adottano le misure tecniche opportune, l'attività di acquisizione diventa vana e difficilmente ripetibile; la prospettiva dell'attività tecnica è dunque quella della *utilizzabilità* in dibattimento, a disposizione delle parti processuali.

La convenzione di Budapest è stata ratificata dall'Italia con con la L. n. 48/2008 del 18 marzo 2008, che ha apportato importanti modifiche al Codice di procedura penale al fine di adeguarlo alle esigenze proprie della prova informatica.

Il legislatore, con lungimiranza, ha tuttavia evitato di cristallizzare in norme cogenti le mutevoli procedure tecniche dell'informatica forense. Una siffatta canonizzazione normativa si sarebbe rivelata un ostacolo all'evoluzione della disciplina, incapace di adattarsi alla rapidità del progresso tecnologico e alle peculiarità irripetibili di ciascun caso concreto. Il legislatore si è pertanto concentrato sul risultato – la genuinità e l'integrità della prova – demandando la definizione del *modus operandi* a un corpus di *normazione tecnica volontaria* e di *best practice* sviluppato a livello internazionale. Questo approccio garantisce che la metodologia forense mantenga il proprio carattere scientifico, fondato su principi di validità, ripetibilità e verificabilità, essenziali per il corretto esercizio del diritto e l'amministrazione della giustizia.

Prima dell'avvento di una standardizzazione formale, la comunità forense ha operato sulla base di principi cardine, universalmente riconosciuti, volti a garantire l'ammissibilità dell'evidenza digitale. Tali principi, ancora oggi validi, includono: *a)* inalterabilità del reperto originale: l'acquisizione della prova deve avvenire senza modificare in alcun modo il dato sorgente, operando, per prassi consolidata, su una copia forense (o *bit-stream image*), cioè una duplicazione speculare e completa del dispositivo di memorizzazione; *b)* autenticazione e integrità: è imperativo dimostrare che la copia acquisita sia identica all'originale, impiegando algoritmi di hashing (come ad esempio MD5, SHA1, SHA256), la cui funzione è generare un'impronta digitale univoca del dato; la corrispondenza degli hash tra originale e copia ne attesta l'identità; *c)* ripetibilità dell'accertamento: le procedure adottate devono essere documentate con un tale livello di dettaglio da permettere a un altro esperto, nelle medesime condizioni, di ripetere l'analisi e pervenire ai medesimi risultati; *d)* verificabilità, imparzialità e oggettività: l'analista forense è uno scienziato che deve operare con assoluta imparzialità, limitandosi a esporre i fatti tecnici così come emergono dall'analisi, senza trarre conclusioni soggettive non dimostrabili.

Questi principi sono stati progressivamente codificati in documenti e standard più strutturati, emanati da enti governativi e organizzazioni internazionali. Tra i precursori si annoverano la RFC 3227 (*Guidelines for Evidence Collection and Archiving*) e i manuali del Dipartimento di Giustizia statunitense e FBI. Tuttavia, è con la serie ISO/IEC 27000 che la disciplina ha trovato il suo quadro di riferimento più autorevole e scientificamente rigoroso. La famiglia di standard ISO/IEC 27000, dedicata alla sicurezza delle informazioni, contiene un sottoinsieme di norme specificamente concepite per l'informatica forense, che disegnano un processo completo e coerente. Le norme principali includono:

- ISO/IEC 27037 (*Guidelines for identification, collection, acquisition and preservation of digital evidence*): considerato il documento fondamentale per la prima fase del processo forense, definisce le procedure per gestire la

prova dalla scena del crimine (fisica o virtuale) fino al laboratorio. Introduce ruoli professionali chiave come il *Digital Evidence First Responder* (DEFR), il primo operatore qualificato a intervenire, e il *Digital Evidence Specialist* (DES), con competenze più approfondite. Un aspetto centrale della norma è la rigorosa gestione della catena di custodia, un documento imprescindibile che traccia ogni passaggio e manipolazione del reperto, garantendone la tracciabilità e l'integrità.

- ISO/IEC 27041 (*Guidance on assuring suitability and adequacy of incident investigation methods*): questa norma si concentra sulla validazione dei metodi investigativi. Stabilisce i criteri per assicurare che gli strumenti software e hardware, nonché le procedure impiegate, siano idonei allo scopo e scientificamente validi. Impone un approccio basato sul rischio e sulla verifica, fondamentale quando si impiegano nuove tecnologie, inclusi gli strumenti basati su intelligenza artificiale, per i quali è necessario comprendere e validare il modello algoritmico.
- ISO/IEC 27042 (*Guidelines for the analysis and interpretation of digital evidence*): si occupa della fase analitica, fornendo un framework per l'esame e l'interpretazione dei dati estratti. Affronta i problemi di continuità, validità e riproducibilità, guidando l'analista nella selezione dei processi più idonei a esaminare l'evidenza in modo obiettivo e a documentare le conclusioni in maniera trasparente e comprensibile.
- ISO/IEC 27050-1 (*Electronic discovery*): sebbene orientata al contesto dell'e-discovery, spesso legato ad ambiti civilistici e aziendali, questa norma fornisce principi applicabili anche in ambito penale, soprattutto per quanto concerne la gestione di grandi volumi di dati non strutturati (es. email, documenti) e la loro revisione in vista di un procedimento legale.

Accanto alla normativa ISO, un riferimento imprescindibile, soprattutto nel contesto statunitense ma con influenza globale, è il framework del NIST (National Institute of Standards and Technology), con diverse pubblicazioni specializzate per argomento: ad esempio la pubblicazione SP 800-86 sulla gestione degli incidenti oppure SP 800-101 sulla mobile forensics.

Gli standard attuali, per quanto robusti, sono costantemente sfidati dall'evoluzione tecnologica. La diffusione del *cloud computing*, dell'Internet of Things (IoT), dei sistemi industriali e dei sistemi virtuali introduce paradigmi che mal si conciliano con il modello tradizionale di sequestro del reperto fisico. L'acquisizione di dati volatili da remoto, la gestione di prove distribuite su più giurisdizioni e la necessità di interfacciarsi con i *Cloud Service Provider* richiedono un aggiornamento continuo delle *best practice*. La sfida futura per gli enti di standar-

dizzazione sarà quella di sviluppare linee guida flessibili e tecnologicamente neutre, capaci di normare i principi dell'indagine forense in ambienti decentrizzati e astratti, garantendo che il valore probatorio dell'evidenza digitale rimanga saldo anche in assenza di un supporto fisico tangibile, in un quadro di rincorsa continua al nuovo ritrovato della tecnologia.

7. Le fasi del trattamento del reperto informatico

Sulla base degli standard più rilevanti è possibile identificare le fasi principali del processo di indagine digitale.¹⁶

Le indagini digitali sono definite come “l'uso di metodi scientificamente derivati e comprovati per l'identificazione, la raccolta, il trasporto, l'archiviazione, l'analisi, l'interpretazione, la presentazione, la distribuzione, la restituzione e/o la distruzione di prove digitali derivanti da fonti digitali, preservando al contempo [...] le prove digitali e mantenendo la catena di custodia” (ISO/IEC 27043). Esse comprendono diverse fasi e due fasi principali (Figura 1).

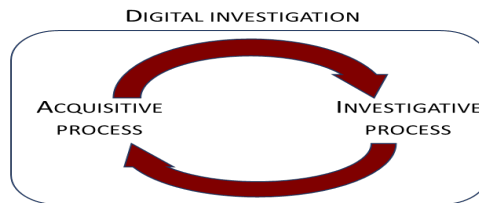


Figura 1: Processo di Digital investigation

Le sue due fasi principali consistono nei processi di acquisizione dei dati (fase 1) e utilizzo degli stessi per un'indagine (fase 2). Il risultato del *processo di acquisizione* costituisce l'input per il *processo investigativo*. A volte, il risultato del processo investigativo può suggerire altre attività che richiedono un nuovo processo di acquisizione. E così via, fino alla fine dell'indagine.

La “fase uno” è il processo di gestione [iniziale] delle prove digitali, che comprende l'identificazione, la raccolta, l'acquisizione e la conservazione delle potenziali prove digitali. Come suggerisce il nome, il processo di acquisizione è il processo attraverso il quale i dati vengono acquisiti o catturati. Il suo obiettivo

¹⁶ La schematizzazione adottata in questa sezione è stata presentata in R. BRIGHI, M. FERRAZZANO, *Digital forensics: best practices and perspective*, in M. CAIANIELLO, A. CAMON (a cura di), *Digital forensics evidence. Towards common european standards in antifraud administrative and criminal investigations*, Milano: Wolters Kluwer, 2021, pp. 13-48, come esito del progetto di ricerca DEVICES – Digital forensic EVIDence: towards Common European Standards in antifraud administrative and criminal investigations. Progetto Hercule III 2018 Legal Training and Studies (OLAF).

è individuare, identificare, raccogliere e/o acquisire e conservare tutti i dati che possono essere rilevanti per un'indagine e che possono essere utilizzati come prove in procedimenti amministrativi, disciplinari o giudiziari.

La «fase due», il processo investigativo, riguarda l'analisi delle prove, l'interpretazione dei risultati dell'analisi, la comunicazione dei risultati dell'interpretazione e la presentazione di tali risultati in tribunale, con l'uso di strumenti e tecniche analitiche specifiche che consentono di stabilire collegamenti tra le informazioni.

Ciascuna fase è composta da passaggi (Figura 2) che devono essere seguiti in sequenza in ogni investigazione digitale. Tuttavia, vi sono alcuni fattori che richiedono una valutazione caso per caso delle operazioni da eseguire. Tra i fattori che incidono vi sono, ad esempio, la condizione operativa del sistema (acceso o spento), l'impossibilità di rimuoverlo in quanto impiegato per l'erogazione di un servizio critico o collocato all'interno di una rete che ne impedisce l'accesso fisico diretto, nonché eventuali limitazioni di natura giuridica che ne ostacolano l'acquisizione.

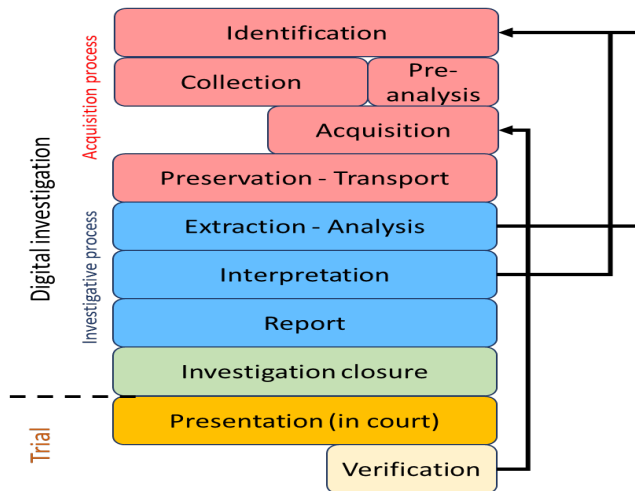


Figura 2: Fasi dell'investigazione digitale

La prima fase, detta *identificazione*, rappresenta il processo di ricerca, ricognizione e documentazione di potenziali prove in formato digitale, ovvero dei dispositivi di memorizzazione di bit che possono essere rilevanti ai fini dell'indagine, individuando dove possibile anche i dati che si possono trovare all'esterno o in *cloud*. Non si tratta comunque solo di una banale ricerca di dispositivi ma occorre definire le giuste priorità tenendo conto del rischio di volatilità

dei dati, allo scopo di minimizzare il danneggiamento di potenziali prove digitali e di ottenere il dato più integro e genuino possibile. Lo scopo è riuscire a identificare tutti i supporti fisici e remoti, la provenienza/destinazione di un dato, nonché il luogo fisico e/o virtuale in cui è memorizzato.

Occorre, quindi, verificare la disponibilità di accesso a luoghi fisici e virtuali per la sincronizzazione o l'accesso da remoto ai dati di interesse. Oltre l'individuazione delle periferiche tradizionali che contengono dati digitali rilevanti, quali *server*, *computer* e *notebook* (*hard disk*, SSD), dispositivi rimovibili (*hard disk* esterni, unità USB, supporti ottici) e periferiche multimediali (video camere e memorie interne/aggiuntive), è importante analizzare ogni altro sistema di memorizzazione di dati digitali utile alle indagini in corso, quali assistenti vocali, sistemi di domotica, sistemi di antifurto e automobili.

Una volta identificati i dispositivi digitali che potrebbero contenere dati digitali rilevanti per l'indagine, l'informatico forense (il DEFR secondo le indicazioni dello standard ISO 27037) deve decidere se procedere immediatamente all'acquisizione oppure se procedere alle operazioni di raccolta del supporto che verranno seguite solo successivamente dalle operazioni di acquisizione.

La seconda fase si occupa della *raccolta dei dispositivi* che possono contenere potenziali prove digitali, che quindi vengono rimossi dalla loro posizione originale per essere trasportate in un laboratorio o, più in generale, in un altro ambiente controllato per l'acquisizione e la successiva analisi, e/o dell'acquisizione forense dei dati nei casi in cui non sia possibile, tecnicamente o giuridicamente, asportare fisicamente il reperto.

A seconda dello stato di rinvenimento (acceso o spento), la procedura adottata può subire delle variazioni di ordine di esecuzione o di scelta tra raccolta e acquisizione. La raccolta viene solitamente preferita dalle forze dell'ordine perché rispetto all'acquisizione può essere svolta più rapidamente, senza particolari competenze tecniche e rimandando ogni accesso a un momento successivo. Tuttavia, in diverse circostanze la raccolta fisica non è possibile: quando i sistemi informatici che non possono essere spenti; quando i sistemi informatici che erogano servizi anche a terzi; quando le dimensioni del sistema o la loro collocazione geografica non ne consente il trasporto agevole.

Da un punto di vista penale, la raccolta è la fase che trova riscontro nel sequestro probatorio, il mezzo di ricerca della prova con il quale l'autorità giudiziaria acquisisce il corpo del reato o le cose pertinenti ad esso che siano necessarie per l'accertamento dei fatti.

In alternativa alla raccolta, o comunque a seguito della stessa, l'*acquisizione* rappresenta il processo di produzione di una copia di evidenze digitali detta copia forense (o *bit-stream image*, o immagine bit a bit), ovvero una copia completa del supporto compresi i dati cancellati ed eseguita in modo tale da evitare di al-

terarne i dati. La procedura di acquisizione è molto diversa a seconda del tipo di reperto (hard disk, smartphone, rete...), ma in generale il prodotto finale può essere un clone, ossia un dispositivo che contiene l'esatta e identica sequenza del dispositivo sorgente, oppure un file immagine (o una serie di file frammentati) che rappresentano la sequenza del dispositivo sorgente. L'identità tra sorgente e destinazione può essere facilmente provata mediante algoritmi di *hash*, funzioni matematiche che consentono di sintetizzare la rappresentazione di milioni di bit in stringhe esadecimali di poche decine di bit: infatti, l'applicazione di una stessa funzione di hash a due sequenze di bit produce sempre lo stesso risultato (*digest*) se e solo se le due sequenze in input sono identiche. Negli ultimi anni sono sorte interessanti discussioni e anche decisioni in merito all'utilità e al senso di produrre copie forensi *bit a bit* a fronte di esigenza limitata di dati: si sta così andando verso una direzione che vuole la copia forense completa come un mezzo intermedio sul quale effettuare una fase di analisi in contraddittorio per generare poi una successiva acquisizione del solo materiale selezionato¹⁷.

Nel caso in cui la macchina sia ancora accesa al momento dell'accesso, occorre effettuare una prima analisi immediata sul posto perché lo spegnimento provocherebbe la perdita di dati volatili presenti in memoria RAM e l'inaccessibilità dei dati protetti da cifratura.

Le fasi finora descritte sono abbastanza meccaniche e ripetitive, richiedendo esclusivamente l'adozione di alcuni strumenti che, opportunamente utilizzati secondo precisi schemi, consente di disporre di dati che però non sono ancora stati oggetto di esame. La fase di *analisi* invece presuppone approfondite nozioni di architettura degli elaboratori e di sistemi operativi, ma anche di reti, di protocolli di comunicazione, di amministrazione di sistemi e anche un certo talento da parte dell'esaminatore che deve scovare il materiale rilevante ai fini dell'indagine. L'attività di analisi consiste nel recuperare quei dati utili ai fini di un'indagine forense che possono talvolta risultare nascosti, volontariamente o meno, alla vista di un comune utilizzatore.

L'attenzione dell'analista deve dunque rivolgersi ai file e al loro contenuto, ma anche a file temporanei, porzioni di file, *slack space*, artefatti di sistema operativo, metadati temporali. I dati vengono quindi esaminati partendo dalla generazione di timeline, confronto per *hash*, filtri per data, estensione o parola chiave.

All'esito dell'analisi, i dati raccolti sono "oggettivi" e chiunque troverebbe i medesimi risultati. Tuttavia, occorre dare una spiegazione del significato di quei dati: ecco, dunque, che si rende necessaria una fase di *valutazione* nella quale i bit

¹⁷ In argomento si veda M. FERRAZZANO, L. SUMMA, *La selezione di dati informatici in ambito giudiziario: prassi e modalità operative*, in R. BRIGHI (a cura di), *Nuove questioni di informatica forense*, cit., pp. 61-82.

che sintatticamente si compongono di sequenze di zero e uno possono avere significati diversi e ricostruzioni talvolta molto diverse tra loro.

Infine, l'intervento dell'informatico forense culmina con la redazione di una relazione tecnica nella quale presentare tutte le operazioni svolte, i reperti trattati e i risultati raggiunti. Ove necessario, la fase di *presentazione* può anche avvenire oralmente in dibattimento o al di fuori dalle aule processuali, ad esempio nella predisposizione della difesa con l'avvocato o per usi in ambito stragiudiziale.

8. Il ruolo di esperti di informatica forense e dei laboratori certificati di digital forensics

La crescente complessità tecnologica e le implicazioni giuridiche sottese all'impiego di algoritmi avanzati rendono obsoleto il modello dell'investigatore isolato, esigendo un approccio sistemico fondato su una dualità di competenze, rigorosi percorsi formativi e strutture operative certificate.

L'intrinseca natura interdisciplinare della digital forensics, esacerbata dall'avvento dell'IA, postula come requisito ineludibile la formazione di professionisti dotati di una solida e integrata preparazione sia nel dominio informatico sia in quello giuridico. Attualmente, il panorama formativo universitario in Italia appare ancora disorganico, demandando in larga parte al singolo la costruzione di un percorso di specializzazione post-lauream. L'itinerario elettivo muove da una solida base accademica in discipline STEM (Scienza, Tecnologia, Ingegneria e Matematica), preferibilmente con indirizzi specifici in sicurezza informatica, ma vedono solo in rari casi approfondimenti specifici sulla digital forensics e ancora meno sulle competenze di diritto. Tuttavia, tale fondamento tecnico deve essere obbligatoriamente integrato da una conoscenza approfondita delle discipline giuridiche pertinenti. Il bagaglio culturale dell'esperto non può prescindere da una conoscenza e comprensione puntuale del diritto e della procedura, penale e civile, con particolare riguardo alla disciplina della prova digitale, al ruolo processuale del Consulente Tecnico e del Perito, e alle fonti normative sovranazionali e interne che regolano la materia, quali la Convenzione di Budapest sul Cybercrime del 2001, recepita con la Legge n. 48/2008. La frequente sottovalutazione della componente giuridica costituisce un vizio metodologico che può inficiare irrimediabilmente l'ammissibilità e la valutazione della prova digitale nel contraddittorio processuale. Risulta pertanto imperativo che le istituzioni accademiche strutturino percorsi di studio *ad hoc*, quali corsi di laurea magistrale o master universitari, capaci di fondere organicamente l'insegnamento dell'informatica come scienza con quello del diritto processuale e delle nuove tecnologie.

La complessità degli scenari investigativi contemporanei, caratterizzati da volumi massivi di dati e dall'impiego di tecniche di offuscamento sofisticate, pone inoltre ulteriori elementi da considerare che richiedono un recepimento anche sotto il profilo normativo. L'approccio al caso da parte di un singolo professionista non è più sostenibile. La gestione di un'indagine digitale complessa, che può spaziare dall'analisi di infrastrutture di rete a quella di dispositivi mobili e sistemi cloud, esige un'organizzazione strutturata e un team multidisciplinare. Tale modello organizzativo permette di aggregare competenze verticali differenti (ad esempio di network forensics, mobile forensics e malware analysis) per garantire un controllo incrociato sulle procedure adottate, mitigando il rischio di errore umano. L'integrazione dei sistemi di intelligenza artificiale nelle metodologie di indagine digitale, infine, non solo amplifica la capacità analitica, ma impone una riconsiderazione profonda del profilo professionale dell'esperto forense e dell'assetto organizzativo in cui opera.

In questo contesto, assume un'importanza dirimente operare all'interno di un laboratorio di informatica forense certificato. La certificazione, ad esempio secondo standard internazionali come l'ISO/IEC 17025 e ISO/IEC 27037, non rappresenta un mero formalismo, ma attesta l'aderenza del laboratorio a rigorosi protocolli di gestione della prova, la taratura periodica della strumentazione hardware e software, e la competenza del personale. L'adozione di un simile quadro operativo conferisce un crisma di oggettività e affidabilità scientifica all'intero processo di acquisizione e analisi, rafforzando in modo significativo la tenuta della prova in sede dibattimentale. La catena di custodia del reperto digitale viene così garantita non solo dalla perizia del singolo, ma dalla solidità di un intero sistema procedurale verificabile e trasparente.

L'esperto, sia esso Consulente Tecnico d'Ufficio (CTU), di Parte (CTP) o Perito, agisce quale *longa manus* tecnica dell'Autorità Giudiziaria o delle parti. La sua attività deve essere improntata al più assoluto rigore scientifico, assicurando la piena riproducibilità degli accertamenti. Qualora le best practice di settore venissero disattese, il rischio concreto è la compromissione del reperto, con la conseguente inutilizzabilità processuale della prova da esso derivante. L'obiettivo dell'analista è corroborare i risultati attraverso la correlazione di tutte le evidenze disponibili – dai metadati dei file ai log di sistema, fino alla timeline degli eventi – al fine di offrire al giudicante una ricostruzione fattuale munita di elevato grado di certezza scientifica, epurata da interpretazioni soggettive o da artefatti fuorvianti. La capacità di fronteggiare anche scenari inesplorati, spiegando fenomeni complessi con un linguaggio intellegibile anche ai non addetti ai lavori, rimane la cifra distintiva di un professionista la cui competenza è oggi, più che mai, presidio essenziale per la tutela dei diritti e l'accertamento della verità.

D'altro canto, in un contesto sempre più caratterizzato dalla pervasività dell'informatica (quale processo ormai non ha almeno una evidenza informatica?) e dalla complessità tecnica delle indagini digitali, la formazione interdisciplinare assume un ruolo strategico: essa è una leva fondamentale affinché sia gli esperti tecnici che operano in ambito forense, sia gli operatori del diritto, possiedano una reale comprensione dei reciproci vincoli, obiettivi e limiti. Parallelamente, dunque, è fondamentale che anche il professionista del diritto acquisisca consapevolezza del fatto che l'informatica forense, per quanto fondata su protocolli scientifici rigorosi, non garantisce certezze assolute, ma implica un'interpretazione critica dei dati digitali e delle relative inferenze probatorie. Così come, per gli operatori del diritto, è fondamentale comprendere cosa effettivamente sia possibile sotto un profilo tecnico, quali sono le difficoltà o i vincoli, nonché come valutare la prestazione resa dall'esperto tecnico per valutarne la qualità. Una simile consapevolezza favorisce un dialogo più efficace tra le due professionalità e contribuisce a garantire un utilizzo corretto e responsabile delle evidenze digitali nel processo.

9. Prospettive di utilizzo di soluzioni di IA nelle investigazioni di digital forensics

L'avvento e la progressiva sofisticazione dei sistemi di IA rappresentano un punto di svolta paradigmatico anche per la digital forensics. L'impiego di tali tecnologie non si limita a un mero incremento dell'efficienza operativa, ma introduce nuove metodologie d'indagine in grado di rimodulare l'approccio dell'esperto. La capacità dell'IA di processare, correlare e interpretare volumi di dati altrimenti ingestibili consente di superare i limiti intrinseci dell'analisi manuale, potenziando l'attività investigativa in diverse fasi cruciali del procedimento¹⁸. L'impiego dell'IA nell'informatica forense si manifesta primariamente nell'automazione e nell'accelerazione dei processi di analisi dei dati, specie quelli di *routine*. In un contesto investigativo moderno, l'analista si confronta con una mole esponenziale di informazioni eterogenee di diversa provenienza. Una volta raccolti, la fase di analisi può essere, almeno per una prima valutazione, delegata a sistemi di IA opportunamente addestrati (ad esempio per riconoscere e categorizzare immagini, video o documenti contenenti materiale illecito come nei casi di pedopornografia o violazione di proprietà intellettuale) con una rapidità e una precisione irraggiungibili da un operatore umano. Questo processo, noto in

¹⁸ Per una introduzione si veda M. FERRAZZANO, *L'intelligenza artificiale a servizio delle attività di informatica forense*, in *Ordines*, 2023 (2) pp.132-146 e R. BRIGHI, *Informatica forense, algoritmi e garanzie processuali*, in *Ars Interpretandi*, 2021 (X), pp.153-164.

letteratura come *automated evidence triage*¹⁹, consente una drastica riduzione dei tempi di analisi preliminare, permettendo all'investigatore di concentrare le proprie risorse cognitive sulle evidenze più significative. L'efficacia di tali sistemi risiede nella loro capacità di apprendere da dataset pre-esistenti per poi applicare tale conoscenza a nuovi casi. Come evidenziato da Garfinkel²⁰, l'automazione in ambito forense non è un concetto nuovo, ma l'IA introduce un livello di analisi semantica e contestuale precedentemente irraggiungibile.

Un altro ambito di fondamentale apporto dell'IA è il rilevamento di anomalie (*anomaly detection*). I sistemi tradizionali di analisi forense si basano spesso su firme e regole predefinite per identificare malware o attività sospette. Tale approccio si rivela inefficace di fronte a minacce sconosciute o a tecniche di offuscamento avanzate. Gli algoritmi di *machine learning*, al contrario, possono analizzare il comportamento di un sistema o di un utente nel tempo, costruendo un modello di normalità (*baseline*). Qualsiasi deviazione significativa da tale modello viene segnalata come un'anomalia potenzialmente rilevante ai fini investigativi. Questo approccio si dimostra particolarmente proficuo in alcuni contesti come, ad esempio, l'analisi del traffico di rete o l'individuazione di accessi abusivi a sistemi informatici. L'IA può correlare micro-eventi apparentemente slegati tra loro, che un analista umano noterebbe con estrema fatica e attenzione, per far emergere pattern complessi indicativi di un'attività illecita, tanto da rappresentare un salto qualitativo nell'analisi forense, trasformandola da una disciplina reattiva a una proattiva e, in certi contesti, predittiva²¹.

L'introduzione dell'IA nel processo investigativo impone una doverosa e rigorosa riflessione sulla validità giuridica e sull'ammissibilità della prova così ottenuta, senza però mascherarsi dietro i tipici argomenti di diffidenza. Uno degli argomenti tipicamente contro l'adozione di tali soluzioni vede qualificare gli algoritmi di IA come scatole nere, la cui logica decisionale non è immediatamente interpretabile. Tuttavia, l'analisi forense è notoriamente un'attività ripetibile e verificabile: partendo da una copia forense, ogni analista può utilizzare metodi e strumenti a propria discrezione. Se agli albori della disciplina la discussione tipica era tra software open source e software a codice chiuso, oggi la diatriba si sposta sul piano della competizione tra analista IA e analista umano. Nella sostanza, quindi, una IA trasparente non è fondamentale nel momento in cui un analista umano può arrivare a verificare i risultati ottenuti attraverso una strada

¹⁹ MR. REDDY *et al.*, *CyberSleuth AI: Intelligent Network Forensics Analyzer*, in *International Journal for Research in Applied Science and Engineering Technology*, 2025 (13), pp.1643-1647.

²⁰ S.L. GARFINKEL, *Digital forensics research: The next 10 years*, in *Digital Investigation*, 2010 (7), pp. S64-S73.

²¹ W. AL-KHATER *et al.*, *Intelligent digital forensics: a review and future directions*, in *Multimedia Tools and Applications*, 2017 (76/21), pp. 22353–22384.

manuale. Questo paradigma però ancora di più impone che gli analisti non si limitino a premere dei pulsanti, ma sempre più siano consapevoli del funzionamento dei sistemi informatici e del significato dei dati rilevati, viceversa il rapporto con l'IA rischia di considerare inaffidabili risultati che invece potrebbero essere robusti. Dunque, dal punto di vista del diritto processuale, l'elaborazione effettuata da un sistema di IA può essere configurata come uno dei metodi di elaborazione di dati che si inserisce nel più ampio *genus* della prova scientifica. Sarà onere del perito o del consulente tecnico illustrare al giudice non solo l'esito prodotto dall'algoritmo, ma anche il suo funzionamento, il tasso di errore noto e la metodologia di validazione del software, in aderenza ai principi espressi dalla giurisprudenza in materia.

10. Conclusioni

Il necessario intreccio tra tecnica e diritto – frutto dell'elaborazione di una cornice epistemologica per le scienze forensi, fondata sull'adozione di standard metodologici e strumenti tecnici idonei a garantire certezza procedurale e trasparenza – ha contribuito a una crescente sensibilità nei confronti della prova informatica.

Il confronto con tecnologie eterogenee – quali l'*Internet of Things* (IoT), il cloud computing, i dispositivi mobili, la blockchain, le criptovalute, gli edifici intelligenti e persino le smart cities – impone a giuristi e scienziati forensi un costante aggiornamento e una revisione critica dell'approccio tradizionale all'informatica forense. Al centro dell'attenzione rimane la prova informatica, in tutte le sue fasi: formazione, acquisizione, conservazione e valutazione e, con essa, il processo investigativo in cui si raccolgono gli elementi probatori mediante tecniche informatiche; tuttavia, ogni caso presenta nuove sfide e il futuro *Digital Forensics Expert* (DFE) dovrà essere equipaggiato con le conoscenze e le abilità per affrontare le molteplici questioni forensi nel caso presentato.

PARTE II – STRUMENTI ABILITANTI

IDENTITÀ E FIRME DIGITALI

*Chantal Bompreszzi, Monica Palmirani**

Sommario: 1. Quadro normativo. 2. Il documento informatico, le firme elettroniche e l'equivalenza funzionale. 3. Le tipologie giuridiche di firma elettronica. 4. Il valore giuridico e probatorio dei documenti elettronici e delle firme elettroniche. 5. Servizi fiduciari e certificatori. 6. L'identità digitale 7. Portafoglio europeo d'identità digitale (*EUDI Wallet*) 7.1. (*Segue*): EUDI Wallet e identità digitale auto-sovrana (SSI) 8. La frammentazione dell'*identity management* nell'UE 9. L'interoperabilità nei servizi della Pubblica amministrazione

1. Quadro normativo

L'Italia è stata tra i primi Paesi a dotarsi di un quadro normativo sui documenti informatici e le firme elettroniche. Ci si riferisce, in particolare, alla Legge 15 marzo 1997, n. 59 ("Delega al Governo per il conferimento di funzioni e compiti alle Regioni ed agli Enti locali, per la riforma della Pubblica Amministrazione e per la semplificazione amministrativa"), che all'art. 15, co. 2, disponendo che «gli atti, i dati e documenti formati dalla pubblica amministrazione e dai privati con strumenti informatici e telematici, i contratti stipulati nelle medesime forme, nonché la loro archiviazione e trasmissione con documenti informatici, sono validi e rilevanti a tutti gli effetti di legge», introduceva una regolamentazione organica sulla validità e rilevanza giuridica delle rappresentazioni informatiche di documenti. La specifica normativa sulle firme elettroniche è, invece, di derivazione comunitaria e si deve per la prima volta alla Direttiva 1999/93/CE, poi attuata in Italia con il d.lgs. 10/2002.

Queste disposizioni sono successivamente state abrogate, riordinate e consolidate all'interno del d.lgs. 7 marzo 2005, n. 82, o "Codice dell'Amministrazione digitale" (da qui in avanti, CAD). Il CAD è stato modificato a più riprese nel corso degli anni, anche per adeguarsi alle più recenti disposizioni europee del Regolamento UE n. 910/2014 del Parlamento europeo e del Consiglio del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno (d'ora in avanti, Reg. eIDAS). Quest'ultimo Regolamento è nato per garantire il buon funzionamento del mercato interno, rafforzando la fiducia nelle transazioni elettroniche, fornendo una base comune per interazioni elettroniche sicure fra cittadini, imprese e autorità pubbliche, in modo da migliorare l'efficacia dei servizi elettronici pubblici e privati, nonché dell'*eBusiness* e del commercio elettronico, nell'Unione europea. L'obiettivo del Regolamento è quello di garantire l'interoperabilità giuridica e tecnica tra gli Stati membri dell'UE riguardo agli strumenti elettronici di identificazione, autenticazione e firma, migliorando così l'efficacia dei servizi online all'interno dell'Unione europea.

* Pur senza tradire l'unitarietà del lavoro, alla Dott.ssa Bompreszzi vanno attribuiti i paragrafi da 1 a 7, e alla Prof.ssa Palmirani i paragrafi da 7.1 a 9.

La natura di Regolamento (e non di Direttiva) dell'eIDAS ha consentito al medesimo di essere direttamente applicabile in tutti gli Stati membri, scongiurando così la frammentazione normativa e favorendo l'armonizzazione del diritto nel mercato unico. Le modifiche al CAD, come testé accennato, sono appunto servite per raccordare la disciplina italiana con quella europea.

La disciplina introdotta dal CAD (la quale, a discapito di quanto il nome possa suggerire, si applica anche ai privati (ove non diversamente previsto) è integrata da Linee guida contenenti le regole tecniche (art. 71) aventi la duplice funzione di dettagliare le norme generali e di favorire l'aggiornamento dettato dall'evoluzione tecnologica.

Da ultimo, il Regolamento eIDAS è stato modificato e aggiornato nel 2024 mediante il Regolamento UE 2024/1183 (detto anche "eIDAS 2"). Le principali novità di tale revisione hanno riguardato l'introduzione del Portafoglio di identità digitale europea (o "*EUDI Wallet*") e altri nuovi servizi fiduciari come i registri elettronici e l'archiviazione elettronica a lungo termine.

2. Il documento informatico, le firme elettroniche e l'equivalenza funzionale

Il documento informatico è definito all'art. 1, lett. p, del CAD come «il documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti». Ai sensi dell'art. 3, par. 1, n. 35, del Reg. eIDAS, il documento elettronico è «qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva».

Secondo il principio di non discriminazione, esplicitato all'art. 46 del Reg. eIDAS, a un documento elettronico non sono negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziari – così come accade per i documenti cartacei – per il solo motivo della sua forma elettronica.

Il documento informatico si sostanzia in una sequenza di *bit* ed è il risultato di un'elaborazione informatica. La funzione è la medesima del documento cartaceo, e consiste nel rappresentare atti, fatti o dati giuridicamente rilevanti. A questa conclusione si è pervenuti a seguito di un vivace dibattito dottrinale, dettato dall'avvento delle nuove tecnologie e dal passaggio dal documento cartaceo a quello informatico. A tal proposito, illuminante è l'insegnamento di Carnelutti, il quale riteneva documento «qualsiasi cosa idonea a far conoscere un fatto», sostenendo l'irrilevanza della materia di cui lo stesso fosse composto. Egli affermava, difatti, che «qualunque materia, at-

ta a formare una cosa rappresentativa, può entrare nel documento: tela, cera, metallo, pietra e via dicendo»¹.

Al pari del documento, anche tra firma autografa e firma elettronica non deve sussistere discriminazione. L'art. 25 del Reg. eIDAS prescrive all'uopo che «A una firma elettronica non possono essere negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziari per il solo motivo della sua forma elettronica». Invero, seppure firma cartacea ed elettronica abbiano natura diversa (l'una basandosi sulla grafia ed essendo il risultato di un gesto umano, l'altra essendo il risultato di una procedura tecnologica), da un punto di vista giuridico occorre guardare all'idoneità della firma elettronica ad assolvere alle medesime funzioni della sottoscrizione (principio di equivalenza funzionale).

Le funzioni della sottoscrizione autografa sono tre²: indicativa, che consiste nell'identificare l'autore del documento; dichiarativa, che prevede che la sottoscrizione imputi al titolare del nome la paternità del documento; probatoria, per cui la sottoscrizione prova la provenienza del documento. A seconda della tipologia di firma elettronica utilizzata e della capacità di assolvere a queste funzioni, il legislatore o il giudice (a seconda dei casi) stabiliscono l'equivalenza alla firma autografa.

3. Le tipologie giuridiche di firma elettronica

La firma elettronica viene definita all'art. 3, par. 1, n. 10, del Reg. eIDAS come «dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare». L'art. 1, lett. aa, del CAD identifica il firmatario come «la persona *fisica* cui è attribuita la firma elettronica e che ha accesso ai dispositivi per la sua creazione, nonché alle applicazioni per la sua apposizione».

Le firme elettroniche sono giuridicamente distinte in quattro tipologie, caratterizzate da un progressivo grado di maggiore sicurezza circa la capacità di assolvere alle funzioni della firma autografa: 1) semplice; 2) avanzata; 3) qualificata; 4) digitale.

La firma elettronica semplice corrisponde alla definizione di firma elettronica fornita pocanzi. Un esempio di firma elettronica semplice potrebbe essere rappresentato dalla *e-mail*, o posta elettronica semplice.

La firma elettronica avanzata è una firma elettronica semplice che soddisfa i requisiti di cui all'art. 26 Reg. eIDAS (v. art. 3, par. 1, n. 11, Reg.). I requisiti so-

¹ F. CARNELUTTI, *Documento – teoria moderna*, in *Noviss. Dig. it.*, 1957 (VI), p. 85 ss.; *Id.*, *Documento e negozio giuridico*, in *Riv. dir. proc. civ.*, 1926 (I), p. 181 ss.

² F. CARNELUTTI, *Studi sulla sottoscrizione*, in *Riv. Dir. Comm.*, 1929 (IX-X), pp. 509 ss.

no: a) essere connessa unicamente al firmatario; b) essere idonea a identificare il firmatario; c) essere creata mediante dati per la creazione di una firma elettronica che il firmatario può, con un elevato livello di sicurezza, utilizzare sotto il proprio esclusivo controllo; d) essere collegata ai dati sottoscritti in modo da consentire l'identificazione di ogni successiva modifica di tali dati. Un esempio di firma elettronica avanzata potrebbe consistere nella firma grafometrica, la quale corrisponde a una sottoscrizione autografa apposta su un tablet informatico con una particolare penna.

La firma elettronica qualificata, ex art. 3, par. 1, n. 11, Reg. è una firma elettronica avanzata creata da un dispositivo per la creazione di una firma elettronica qualificata e basata su un certificato qualificato per firme elettroniche. I requisiti ulteriori che una firma elettronica deve avere per essere considerata qualificata sono dunque due: l'apposizione mediante un dispositivo apposito, che deve rispettare i requisiti prescritti dall'allegato II del Reg. eIDAS; la presenza di un certificato qualificato rilasciato da un prestatore di servizi fiduciari qualificato conforme ai requisiti di cui all'allegato I del Reg. eIDAS. A titolo esemplificativo, una firma qualificata può essere quella apposta con *smart card* o dispositivo USB. Esistono anche tipologie di firma elettronica qualificata "remota", che prescindono dal rilascio di un dispositivo fisico.

Per la firma elettronica qualificata, ex art. 24 bis, par. 1, Reg. si applica il principio del reciproco riconoscimento, ovvero che le firme elettroniche qualificate basate su un certificato qualificato rilasciato in uno Stato membro sono riconosciute come firme elettroniche qualificate in tutti gli altri Stati membri. La finalità sottesa a tale principio è evidentemente quella di favorire la diffusione di questi strumenti nel mercato dell'UE.

Infine, la firma digitale è un particolare tipo di firma qualificata, caratterizzata da una specifica tecnologia. Per questo tipo di firma, dunque, non si applica il principio della neutralità tecnologica. Mentre secondo quest'ultimo principio, cioè, è indifferente la tecnologia utilizzata (rilevando esclusivamente il soddisfacimento di una serie di condizioni normative), la firma digitale è basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare di firma elettronica tramite la chiave privata e a un soggetto terzo tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici. La firma digitale è una tipologia di firma tipicamente italiana, non definita dal Reg. eIDAS, bensì dal CAD (art. 1, lett. s). Per le sue caratteristiche, tuttavia, viene ricompresa all'interno delle firme elettroniche qualificate.

4. Il valore giuridico e probatorio dei documenti elettronici e delle firme elettroniche

I documenti informatici assumono un diverso valore giuridico e probatorio a seconda che siano privi di firma elettronica o sottoscritti con le varie tipologie giuridiche di firma elettronica (semplice, avanzata, qualificata, digitale).

Il documento informatico sprovvisto di firma, come già visto³, è valido ed efficace giuridicamente. L'art. 20, co.1-*bis*, del CAD statuisce che l'idoneità del documento informatico a soddisfare il requisito della forma scritta e il suo valore probatorio sono liberamente valutabili in giudizio, in relazione alle sue caratteristiche oggettive di sicurezza, integrità e immodificabilità. Sono dunque affidati alla discrezionalità del giudice, caso per caso, il valore e l'efficacia del documento, in base alle caratteristiche dello stesso. Questa regola si applica anche in caso di documento informatico firmato con firma elettronica semplice.

La medesima norma riconosce, invece, al documento informatico firmato con firma elettronica avanzata, qualificata e digitale il soddisfacimento del requisito della forma scritta e l'efficacia prevista dall'art. 2702 c.c.

Parimenti, lo stesso vale anche quando il documento è formato, previa identificazione informatica del suo autore, attraverso un processo avente i requisiti fissati dall'AGID (l'Agenzia per l'Italia Digitale) ai sensi dell'art. 71 (del CAD) con modalità tali da garantire la sicurezza, l'integrità e l'immodificabilità del documento e, in maniera manifesta e inequivoca, la sua riconducibilità all'autore. Trattasi della c.d. "firma tramite SPID" (su cui si veda *infra*).

In queste ipotesi, dunque, la discrezionalità del giudice viene meno (ex art. 2702 c.c. la scrittura privata fa piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l'ha sottoscritta) e l'equivalenza funzionale tra firma autografa ed elettronica è espressamente sancita dalla legge, seppur con dei distinguo a seconda del tipo di documento da firmare. Nello specifico, ex art. 21, co. 2-*bis*, CAD, le scritture private di cui all'articolo 1350, primo comma, numeri da 1 a 12, del codice civile, se fatte con documento informatico, sono sottoscritte, a pena di nullità, con firma elettronica qualificata o firma digitale. Gli atti di cui all'art. 1350, numero 13, del Codice redatti su un documento informatico sono sottoscritti, a pena di nullità, con firma elettronica avanzata, qualificata o digitale, ovvero sono formati con le ulteriori modalità di cui all'articolo 20, comma 1-*bis*, primo periodo (firma con SPID).

Per sintetizzare, la firma elettronica semplice è idonea alla firma di contratti e atti non formali (come ad esempio preventivi, lettere di incarico, moduli di acquisizione del consenso al trattamento dei dati personali); la firma elettronica

³ Vedi *supra*, par. 2.

avanzata e la firma tramite SPID prevedono un ambito di applicazione più ampio, che si estende anche agli atti e contratti *non* aventi ad oggetto beni immobili che richiedono la forma scritta *ad substantiam*, di cui all'art. 1350, n. 13, c.c. (vi ricadono, ad esempio, i contratti bancari) o i contratti che richiedono la forma scritta *ad probationem* (come i contratti assicurativi); infine, un ambito di applicazione massimo è riconosciuto alla firma elettronica qualificata e digitale, apponibile a qualunque contratto, anche avente ad oggetto beni immobili che richiedono la forma scritta *ad substantiam* ex art. 1350, n. da 1 a 12, c.c.

Una particolarità è rappresentata, poi, dall'art. 20, co. 1-ter, CAD, a mente del quale «L'utilizzo del dispositivo di firma elettronica *qualificata* o *digitale* si presume riconducibile al titolare di firma elettronica, salvo che questi dia prova contraria», con un'inversione dell'onere della prova normalmente prescritto per l'analogo documento cartaceo (ex art. 214 c.p.c.). Tramite questo meccanismo, la funzione probatoria del documento firmato con firma elettronica qualificata o digitale è rafforzata, poiché spetterà al titolare della firma, che la voglia disconoscere, a dover dimostrare in giudizio di non aver firmato. Il disconoscimento, qui, ha ad oggetto non la sottoscrizione, ma il dispositivo, in quanto, di base, la firma qualificata o digitale è per natura sempre vera e integra, essendo posta in atto con un dispositivo. Si passa da un criterio di "paternità" della firma autografa ad uno di "responsabilità" della firma elettronica qualificata o digitale⁴ (accompagnato, ex art. 32 CAD, da un corrispondente obbligo di custodia del dispositivo di firma da parte del titolare, il quale è altresì tenuto ad utilizzare personalmente il suddetto dispositivo).

5. Servizi fiduciari e certificatori

La firma qualificata garantisce la connessione univoca tra la firma e il firmatario grazie alla presenza di un certificato qualificato che lo attesta. Un certificato qualificato di firma elettronica è un attestato elettronico che collega i dati di convalida di una firma elettronica a una persona fisica e conferma almeno il nome o lo pseudonimo di tale persona, rilasciato da un prestatore di servizi fiduciari qualificato e conforme ai requisiti di cui all'allegato I del Regolamento eIDAS (art. 3, par. 1, n. 14 e 15).

I servizi fiduciari sono servizi elettronici, forniti normalmente dietro remunerazione, che divengono qualificati nel momento in cui offrono servizi fiduciari qualificati (art. 3, par. 1, n. 16 e 17) e la cui valutazione di conformità è effettuata da un apposito organismo accreditato a norma del Regolamento (art. 3, par. 1, n. 18). In Italia, tali organismi sono accreditati da ACCREDIA. I presta-

⁴ Questa diversità di criteri è stata affermata dal Consiglio di Stato, Sezione Consultiva per gli Atti Normativi, nell'adunanza del 7 febbraio 2005.

tori di servizi fiduciari qualificati sono soggetti a vigilanza da parte di un organismo istituzionale nazionale (in Italia, l'Agenzia per l'Italia Digitale, o AGID), a cui per avviare il servizio qualificato occorre notificare una relazione di valutazione della conformità al regolamento e agli atti di esecuzione rilasciata dall'organismo di valutazione della conformità. La verifica dell'organismo di valutazione della conformità va ripetuto ogni 24 mesi per mantenere lo status, e poi l'esito della valutazione va comunicato ad AGID.

L'elenco dei prestatori è pubblico⁵. Per rilasciare il dispositivo e il certificato qualificato di firma, il prestatore di servizio fiduciario qualificato deve identificare a monte il soggetto richiedente in modo rigoroso (ad esempio tramite SPID o di persona).

Occorre sempre verificare la validità del certificato qualificato, escludendo che esso sia scaduto, revocato o sospeso. La revoca è l'operazione con cui il certificatore annulla la validità del certificato (ad esempio, per morte del titolare), mentre la sospensione ne sospende la validità per un determinato periodo di tempo (ad esempio, per furto). L'apposizione a un documento informatico di una firma digitale o di un altro tipo di firma elettronica qualificata basata su un certificato elettronico revocato, scaduto o sospeso equivale a mancata sottoscrizione (art. 24, co. 4-*bis*, CAD).

6. L'identità digitale

Con l'avvento di Internet si è posto con forza il tema dell'identità digitale e dell'identificazione online. Emblematica la famosa vignetta di Peter Steiner pubblicata sul periodico *The New Yorker* del 5 luglio 1993, raffigurante un cane seduto su una sedia davanti ad un computer che dice al cane a fianco a sé: «*On the Internet, nobody knows you're a dog*» («Su Internet, nessuno sa che sei un cane»). Conoscere l'identità di un soggetto (i.e., poterlo identificare) è giuridicamente rilevante, a volte prescritto dalla legge. Il problema si pone quando si tratta di dover identificare in maniera certa qualcuno a distanza, *online*.

Il Regolamento eIDAS interviene anche su questo aspetto. Anzitutto, esso distingue tra “identificazione elettronica” e “autenticazione elettronica”. Con la prima, si intende «il processo per cui si fa uso di dati di identificazione personale in forma elettronica che rappresentano un'unica persona fisica o giuridica, o un'unica persona fisica che rappresenta un'altra persona fisica o una persona giuridica» (art. 3, par. 1, n. 1); con la seconda, «un processo elettronico che consente di confermare l'identificazione elettronica di una persona fisica o giuridica, oppure di confermare l'origine e l'integrità di dati in forma elettronica» (art.

⁵ <https://eidas.ec.europa.eu/efda/trust-services/browse/eidas/tls>.

3, par. 1, n. 5). Il Regolamento, poi, consente agli Stati membri di notificare alla Commissione europea degli strumenti di identificazione online, a certe condizioni (art. 7), che, se accettati dalla Commissione e pubblicati, devono essere riconosciuti come tali in tutti gli altri Stati membri (secondo il principio del mutuo riconoscimento di cui all'art. 6). Tali sistemi di identificazione elettronica sono distinti in livelli di garanzia, a seconda del grado di fiducia che forniscono circa l'identità dichiarata. I livelli si distinguono, ex art. 8, in basso, significativo ed elevato. In caso di livello basso, gli enti pubblici hanno la facoltà di riconoscimento ai fini dell'autenticazione transfrontaliera. Se invece, il livello di garanzia è pari o superiore al livello richiesto dall'organismo del settore pubblico, e se è almeno significativo o elevato, sussiste l'obbligo di riconoscimento. Queste norme valgono e sono obbligatorie in caso di identificazione presso un soggetto pubblico; permangono una facoltà per i soggetti privati.

L'Italia ha notificato lo SPID e la CIE. SPID sta per Sistema Pubblico d'Identità Digitale, e consente a ogni cittadino di ottenere la propria identità digitale tramite cui accedere con un'unica credenziale (*username* e *password*), ai servizi digitali delle Pubbliche amministrazioni degli Stati membri. La CIE è la Carta d'Identità Elettronica, emessa dal Ministero dell'Interno come documento di identificazione e utilizzabile anche per accedere ai servizi online.

Oltre i confini europei, il mutuo riconoscimento delle identità digitali è favorito dai principi statuiti, seppur solo a livello di *soft law*, dal *Working Group IV* sul Commercio elettronico dell'UNCITRAL, che ha elaborato un apposito *Model Law*⁶.

7. Portafoglio europeo d'identità digitale (*EUDI Wallet*)

Tra i nuovi servizi fiduciari introdotti dal Regolamento eIDAS 2 vi è il portafoglio europeo d'identità digitale (o *European Digital Identity Wallet*, altrimenti detto *EUDI Wallet*).

Il portafoglio europeo di identità digitale è definito come «un mezzo di identificazione elettronica che consente all'utente di conservare, gestire e convalidare in modo sicuro dati di identità personale e attestati elettronici di attributi al fine di fornirli alle parti facenti affidamento sulla certificazione e agli altri utenti dei portafogli europei di identità digitale, e di firmare mediante firme elettroniche qualificate o apporre sigilli mediante sigilli elettronici qualificati» (art. 3, n. 42).

Il portafoglio europeo di identità digitale rappresenta una delle novità più significative derivanti dalla revisione del Regolamento eIDAS, in linea con

⁶ *Model Law on the Use and Cross-border Recognition on Identity Management and Trust Services*, <https://uncitral.un.org/en/mlit>.

L'obiettivo di fornire ai cittadini dell'Unione, seppur in via facoltativa, un'identità digitale che sia sotto il loro controllo esclusivo e avviare così alla gestione di numerose credenziali, *password* e *account* in mano ai prestatori dei servizi *online*. La peculiarità del portafoglio europeo, infatti, è la divulgazione selettiva dei dati personali da parte dell'utente e sotto il proprio esclusivo controllo (v. cons. 15), al fine di garantire che tutte le persone fisiche e giuridiche nell'Unione abbiano un accesso transfrontaliero sicuro, affidabile e senza soluzione di continuità a servizi pubblici e privati (art. 5-*bis*).

Lo stesso art. 5-*bis* detta come limite temporale la fine del 2026 affinché ciascuno Stato membro fornisca almeno un portafoglio europeo di identità digitale. Questi possono essere forniti: direttamente dallo Stato membro; su incarico di uno Stato membro; indipendentemente da uno Stato membro pur essendo riconosciuti da quest'ultimo (art. 5-*bis*, par. 2). Il codice sorgente dei componenti *software* dell'applicazione deve essere caratterizzato da una licenza open source (art. 5-*bis*, par.3). Il livello di garanzia del mezzo di identificazione elettronica deve essere elevato (art. 5-*bis*, par. 11).

Qualora il portafoglio venga usato per firmare, occorre offrire a tutte le persone fisiche la possibilità di apporre firme elettroniche qualificate per impostazione predefinita e gratuitamente, limitatamente a scopi non professionali (art. 5-*bis*, par. 5, lett. g)).

La conformità dei portafogli europei di identità digitale ai requisiti prescritti è certificata da organismi di valutazione della conformità designati dagli Stati membri e comunicati alla Commissione. La certificazione è valida fino a cinque anni, a condizione che sia effettuata una valutazione di vulnerabilità ogni due anni (art. 5-*quater*). È prevista da parte della Commissione la pubblicazione di un elenco dei portafogli europei di identità digitale certificati (art. 5-*quinquies*).

Qualora gli Stati membri richiedano l'identificazione e l'autenticazione elettroniche per accedere a servizi online prestati da un organismo del settore pubblico, essi debbono accettare anche i portafogli europei di identità digitale forniti conformemente al Regolamento (art. 5-*septies*).

In Italia, il Sistema di portafoglio digitale italiano, o *IT-Wallet*, disciplinato dall'art. 64-*quater* del CAD, e integrato nell'app IO, è la versione italiana che anticipa l'*EUUDI Wallet*, e che dovrà conformarsi agli *standard* del Regolamento eIDAS per divenire compatibile e interoperabile con il sistema europeo.

7.1. (Segue): EUUDI Wallet e identità digitale auto-sovrana (SSI)

L'EUDI Wallet introduce nuove opportunità per promuovere l'eguaglianza tra diverse categorie di cittadini. In alcune implementazioni nazionali, ad esempio, la Disability Card europea è stata integrata nel portafoglio digitale nazionale (come nel caso spagnolo e nell'applicazione IO in Italia), e gli studenti possono caricare le proprie tessere universitarie digitali. Tuttavia, il regolamento eIDAS 1.0 presenta taluni elementi suscettibili di attuazione in modo non pienamente conforme al principio di minimizzazione dei dati (*privacy by default*). La riforma introdotta con eIDAS 2.0 e l'EUDI Wallet è volta precisamente a colmare tali lacune.

Nella procedura ordinaria di identificazione digitale, il regolamento eIDAS 1.0 individua almeno tre attori principali: (i) il fornitore di identità (*identity provider*), (ii) il fornitore di servizi (*service provider*) e (iii) il prestatore di attributi qualificati. In tale quadro procedurale, lo standard tecnico Security Assertion Markup Language (SAML) disciplina lo scambio dei soli dati strettamente necessari all'identificazione dell'utente. In conformità al principio di minimizzazione dei dati, sancito dall'articolo 5, paragrafo 1, lettera c), del GDPR, il fornitore di identità e il prestatore di attributi sono a conoscenza dell'identità del soggetto che richiede il servizio; tuttavia, tale informazione dovrebbe essere opportunamente schermata al fine di evitare divulgazioni indebite tramite metadati.

Ciononostante, in diverse implementazioni nazionali tale obbligo di mascheramento non viene rispettato, poiché il regolamento eIDAS 1.0 consente tecnicamente questo approccio (come nel caso dello SPID in Italia). Ne consegue che soggetti terzi possono desumere quali servizi pubblici siano stati utilizzati dall'utente, ad esempio servizi sanitari o richieste relative al casellario giudiziale. Tali prassi sollevano rilevanti criticità in ordine al rispetto del principio di minimizzazione sancito dal diritto europeo in materia di protezione dei dati personali. In taluni ordinamenti, l'assenza di un adeguato mascheramento può persino agevolare l'impiego di tali informazioni a fini di profilazione, consentendo l'offerta di servizi commerciali mirati o ampliati, in potenziale contrasto con le garanzie poste a tutela dei diritti fondamentali.

Il Portafoglio Europeo di Identità Digitale (EUDI Wallet) è stato introdotto dal regolamento eIDAS 2.0 proprio al fine di rafforzare il controllo dell'utente finale sulla comunicazione dei metadati relativi all'identità ai fornitori di servizi. Tale strumento consente, infatti, l'instaurazione di un regime di identità auto-sovrana (*self-sovereign identity*), nel quale l'interessato mantiene un controllo effettivo sul trattamento dei propri dati personali. In tal modo, l'EUDI Wallet rende concretamente operante il principio di minimizzazione dei dati, promuovendo al contempo un approccio incentrato sul cittadino e favorendo un modello decentralizzato di gestione dell'identità digitale.

L'Architecture and Reference Framework (ARF) dell'EUDI Wallet specifica ulteriormente le modalità tecniche e organizzative per la gestione, all'interno di un unico strumento, di molteplici documenti e attributi digitali — quali, ad esempio, patente di guida, documentazione sanitaria o passaporto digitale — garantendo che, durante le transazioni di credenziali, non vengano divulgati metadati non necessari. In questa prospettiva, l'EUDI Wallet costituisce una nuova infrastruttura giuridico-tecnica volta ad attribuire sia alle persone fisiche sia alle persone giuridiche un maggiore controllo sui propri dati personali. Esso consente la gestione sicura e la divulgazione selettiva dei dati identificativi personali (PID), unitamente alle attestazioni elettroniche di attributi (EAAs), rafforzando la conformità ai principi di protezione dei dati e accrescendo la fiducia nei servizi digitali pubblici e privati.

Gli attori coinvolti nel sistema sono: il titolare (*holder*) dell'identità digitale europea, ossia l'interessato; il fornitore del *wallet*; il prestatore di attestazioni di attributi, qualificati e non qualificati (autorità EAAs); e il verificatore (o *relying party*), destinatario delle attestazioni.

Lo scenario operativo può essere così descritto:

Un utente (il "titolare") intende condividere talune informazioni digitali per accedere a un servizio di eGovernment (ad esempio, il livello di istruzione richiesto per partecipare a una selezione pubblica).

Un servizio pubblico o privato (il "verificatore") richiede la prova di specifici attributi (ad esempio, esclusivamente il titolo di studio) e può accettare soltanto dati provenienti da fonti ritenute affidabili (ad esempio, un'università).

Il *wallet* del titolare seleziona automaticamente le attestazioni elettroniche pertinenti (ad esempio, il diploma rilasciato dall'università).

Con il consenso dell'interessato, il *wallet* genera una "presentazione verificabile", ossia un pacchetto sicuro contenente i dati richiesti, e lo trasmette al verificatore.

In sostanza, l'EUDI Wallet attribuisce all'utente il potere di decidere quali dati condividere, con chi e in quale momento, senza il ricorso a ulteriori intermediari.

Il *wallet* si fonda sui principi dell'identità auto-sovrana (SSI). Tale mutamento di paradigma riflette e rafforza i diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea, in particolare il diritto al rispetto della vita privata (art. 7) e il diritto alla protezione dei dati personali (art. 8). Più in generale, l'EUDI Wallet incarna il principio di autodeterminazione informativa, elaborato in sede di giurisprudenza costituzionale — in modo emblematico dalla Corte costituzionale federale tedesca — secondo cui l'individuo deve poter determinare quando, in quale misura e a quali condizioni i propri dati personali possano essere comunicati e trattati.

Diversamente dai modelli centralizzati basati su banche dati uniche, l'EUDI Wallet consente agli utenti di conservare attributi cifrati rilasciati da autorità pubbliche competenti. Tali attributi — che possono riguardare, ad esempio, la maggiore età, lo status di beneficiario di una prestazione o informazioni sanitarie — possono essere presentati in modo granulare e sicuro. Così, un soggetto chiamato a dimostrare la propria maggiore età potrà comunicare esclusivamente tale attributo, senza rivelare informazioni accessorie quali nome o indirizzo. Questo meccanismo di divulgazione selettiva rafforza il rispetto del principio di minimizzazione dei dati, accrescendo al contempo l'autonomia dell'utente e la fiducia nelle transazioni digitali.

L'articolo 5 del regolamento (UE) 2024/1183 garantisce l'uso di pseudonimi nelle transazioni elettroniche relative ai metadati e all'EUDI Wallet. Tuttavia, l'EUDI-ARF non è ancora in grado di fornire specifiche tecniche definitive, anche a causa dell'assenza di un quadro normativo pienamente armonizzato nei singoli Stati membri. In tale contesto, il *legal design* può supportare i decisori pubblici nel comprendere l'importanza dell'introduzione dello pseudonimo attraverso un approccio situazionale o prospettico, evidenziandone vantaggi e criticità nei diversi ordinamenti nazionali. Parimenti, il *legal design* può agevolare i cittadini nella comprensione delle innovazioni introdotte dall'EUDI Wallet rispetto ai precedenti strumenti di identificazione digitale, mediante fumetti, animazioni, mappe concettuali e simulazioni visuali delle operazioni. In questa direzione si collocano le iniziative intraprese dalla Commissione europea attraverso portali informativi dedicati.

L'EUDI Wallet integra altresì garanzie tecnologiche volte a rafforzare la cybersicurezza. In particolare, esso si coordina con la direttiva NIS2 al fine di assicurare il principio dell'accesso digitale sicuro ai servizi pubblici. Coerentemente con il regolamento (UE) 2024/1183, l'Agenzia dell'Unione europea per la cybersicurezza (ENISA) è stata incaricata di sostenere la certificazione degli EUDI Wallet, inclusa la predisposizione di un potenziale schema europeo di certificazione della cybersicurezza nell'ambito del Cybersecurity Act (regolamento (UE) 2019/881). Attraverso tali misure, l'EUDI Wallet risulta maggiormente resiliente rispetto ad attacchi informatici e frodi, contribuendo a rafforzare la fiducia dei cittadini nell'utilizzo dei servizi pubblici digitali.

Allo stato attuale dello sviluppo tecnologico, l'EUDI Wallet integra dunque tanto i principi del GDPR quanto i pilastri fondamentali del diritto europeo in materia di cybersicurezza. Tale convergenza consente di conciliare l'esigenza di garantire un accesso sicuro ai servizi pubblici digitali con la tutela dei diritti alla riservatezza e alla protezione dei dati personali. In questa prospettiva, l'EUDI Wallet rappresenta un esempio significativo di progettazione regolatoria capace

di armonizzare sicurezza e diritti fondamentali, contribuendo alla legittimazione e alla sostenibilità del quadro europeo dell'identità digitale.

8. La frammentazione dell'*identity management* nell'UE

Gli attuali strumenti europei di identità digitale sviluppati in conformità al regolamento eIDAS 2.0, inclusi il Portafoglio Europeo di Identità Digitale (EUDI Wallet), non risultano pienamente idonei a rendere operativi meccanismi di delega strutturati e giuridicamente robusti. Un regime di delega conforme ai principi dello Stato di diritto richiederebbe, quantomeno, l'istituzione di un registro dei rappresentanti autorizzati, la definizione puntuale dell'ambito oggettivo e della durata della delega, nonché l'individuazione dei servizi pubblici cui essa si applica. Inoltre, le amministrazioni pubbliche dovrebbero adeguare i propri sistemi informatici per consentire l'accesso delegato, circostanza che implica interventi complessi sia sul piano normativo sia su quello tecnico-organizzativo.

L'attivazione dell'EUDI Wallet è rimessa alla libera scelta del cittadino. Tale opzione progettuale mira a prevenire fenomeni di esclusione digitale e a scongiurare forme di discriminazione derivanti dall'imposizione di una specifica soluzione tecnologica. L'articolo 5a, paragrafo 15, del quadro regolatorio di riferimento sancisce espressamente tale principio, garantendo al contempo la permanenza di meccanismi alternativi di identificazione e autenticazione. Se, da un lato, questa previsione attua un approccio multicanale, idoneo ad accogliere una pluralità di strumenti di identità digitale, dall'altro lato essa contribuisce a mantenere un certo grado di frammentazione nel mercato europeo della gestione dell'identità.

Attualmente, infatti, l'*identity management* nell'Unione europea si presenta ancora fortemente frammentato, configurando un settore ad elevato valore tecnologico ed economico. In tale contesto, le proposte volte all'adozione di un'identità digitale europea unificata (EUDI) intendono superare tale dispersione. La natura facoltativa dell'EUDI Wallet garantisce flessibilità nell'integrazione di diverse soluzioni tecniche e applicative, ampliando l'accessibilità e favorendo l'inclusione. Tuttavia, questa stessa impostazione inclusiva pone criticità in relazione all'effettiva interoperabilità dei servizi pubblici transfrontalieri all'interno dell'Unione. Si rende pertanto necessario un periodo transitorio volto alla standardizzazione e armonizzazione dell'EUDI, al fine di assicurare coerenza tecnica e ampia fruibilità nei diversi Stati membri.

Particolarmente significativi risultano, in questa prospettiva, gli esiti del progetto DC4EU, che ha prodotto materiali divulgativi e tecnici quali video, schede grafiche, brochure destinate alle amministrazioni pubbliche e approfondimenti

specialistici rivolti agli esperti e alle imprese. Gli obiettivi perseguiti erano molteplici: (i) rafforzare la fiducia dei cittadini; (ii) sostenere l'interoperabilità tra servizi pubblici; (iii) supportare gli attori dell'ecosistema EUDI Wallet nell'implementazione di soluzioni di *user experience* (UX) efficaci e coerenti.

Di rilievo è altresì l'iniziativa promossa da Lissicompany, volta alla creazione di un sistema di icone finalizzato a rendere l'esperienza utente più intuitiva, accessibile e interoperabile tra diversi servizi pubblici e ordinamenti nazionali. Analogo sistema iconografico è stato adottato anche da operatori quali Maggioli per l'offerta dell'EUDI Wallet in Italia, contribuendo alla diffusione di standard comunicativi omogenei e facilmente riconoscibili.

9. L'interoperabilità nei servizi della Pubblica amministrazione

Uno degli obiettivi principali del regolamento eIDAS 1.0 era quello di rafforzare l'interoperabilità dei servizi pubblici transfrontalieri all'interno dell'Unione europea. In particolare, la facilitazione dell'accesso ai servizi sanitari digitali è funzionale a sostenere la mobilità delle persone nello spazio europeo — studenti, lavoratori, turisti — e si inserisce nel più ampio quadro della strategia digitale dell'Unione. La sanità digitale rappresenta, in tale prospettiva, una componente centrale, in quanto strumentale alla piena realizzazione di diritti fondamentali quali la libertà di circolazione, l'accesso all'istruzione e la tutela della dignità umana.

Tuttavia, eIDAS 1.0 ha conseguito tale obiettivo soltanto in misura parziale, principalmente a causa dell'eccessiva frammentazione degli strumenti di identificazione elettronica e dei relativi assetti normativi a livello nazionale. Gli Stati membri hanno adottato modelli organizzativi eterogenei, riconducibili, in via generale, a tre tipologie: (i) sistemi nei quali l'amministrazione pubblica distribuisce direttamente ai cittadini gli strumenti di identificazione digitale; (ii) sistemi in cui l'autorità pubblica definisce standard qualitativi e cornice regolatoria, mentre l'erogazione dei servizi di identità è affidata a operatori di mercato; (iii) modelli nei quali il fornitore dell'identità digitale è interamente un soggetto privato.

Ne consegue che l'interoperabilità delle identità digitali risulta strettamente dipendente dalle regole nazionali, dall'organizzazione dei sistemi di identificazione fisica, dalle esigenze di sicurezza interna e dalle modalità con cui ciascuno Stato membro disciplina la distribuzione dell'identità digitale.

Esemplificativi sono i casi dell'Italia, dove l'accesso al Sistema Pubblico di Identità Digitale (SPID) richiede il possesso del codice fiscale; della Germania, che si fonda su un distinto numero di identificazione fiscale (TIN); e della Francia, che utilizza il *Numéro d'inscription au Répertoire des Personnes Physiques*

(NIRPP). Tali sistemi, strutturalmente differenti, costituiscono un rilevante ostacolo all'interoperabilità transfrontaliera e compromettono il funzionamento fluido delle applicazioni di *eGovernment* su scala europea.

L'introduzione dell'EUDI Wallet nell'ambito di eIDAS 2.0 (art. 5a) accresce significativamente il potenziale di una effettiva interoperabilità dei servizi pubblici transfrontalieri, consentendo agli individui di esercitare un più ampio potere di autodeterminazione nelle proprie interazioni sociali, culturali, sanitarie ed economiche.

Ulteriore tassello di tale strategia è rappresentato dall'Interoperable Europe Act, entrato in vigore nel gennaio 2025, che prevede l'obbligo di predisporre una valutazione di interoperabilità (art. 5) e di individuare soluzioni interoperabili europee ai sensi dell'art. 7, al fine di agevolare l'attuazione di requisiti vincolanti in materia. In questo quadro complessivo, l'interoperabilità sanitaria assume un ruolo centrale anche nella Dichiarazione europea sul Decennio digitale, in quanto elemento essenziale per garantire la libera circolazione delle persone, l'accesso ai servizi fondamentali e la più ampia realizzazione dei diritti nell'Unione.

SMART CONTRACT E BLOCKCHAIN

Chantal Bompreszzi

SOMMARIO: 1. Inquadramento tecnologico. 2. *Smart Contract* e *Smart Legal Contract*. 3. *Smart Contract* e *Data Act*. 4. *Blockchain* e Regolamento Eidas. 5. *Blockchain* e protezione dei dati personali. 6. *Smart contract*, *Nft* e *metaverso*. 7. *Blockchain* e *self-sovereign identity*.

1. Inquadramento tecnologico

Gli *smart contracts* sono programmi informatici deterministici che si auto-eseguono sulla *blockchain* in base alle istruzioni ricevute, iscritte nell'algoritmo che li governa. Possono definirsi deterministici in quanto, a fronte di uno specifico *input*, restituiscono un *output* predeterminato, essendo la loro esecuzione prevedibile *ex ante*. Con auto-esecuzione si intende, invece, l'attuazione, ad opera del programma, di azioni prestabilite al ricorrere di condizioni codificate, secondo la logica "se X, allora Y"¹. Gli *smart contracts*, pertanto, contrariamente a quanto l'accezione potrebbe evocare, non sono necessariamente contratti. Questa obiezione, invero, non è dovuta alla natura (informatica) del linguaggio utilizzato. Lo *smart contract*, infatti, ben potrebbe rappresentare il mezzo mediante cui si articola la volontà delle parti, espressa sotto forma di linee di codice², sia a mente del principio di libertà delle forme, che del principio internazionale di non discriminazione³ (per cui a qualsiasi documento non può essere negata validità per il solo fatto di essere in forma elettronica). Piuttosto, si evidenzia che presupposto imprescindibile per l'esistenza di un contratto sia l'accordo tra le

¹ P. CUCCURU, *Blockchain ed automazione contrattuale, riflessioni sugli smart contract*, in *Nuova giur. civ.*, 2017 (I), pp. 107-119; ID., *Beyond Bitcoin: an early overview on smart contracts*, in *International Journal of Law and Information Technology*, 2017 (XXV), pp. 179-195.

² M. DUROVIC, A. JANSSEN, *The Formation of Blockchain-based Smart Contracts in the Light of Contract Law*, in *European Review of Private Law*, 2019 (VI), p. 760.

³ Il principio di non discriminazione è stato introdotto nel 1996 dalla Commissione ONU sul commercio internazionale (UNCITRAL) con il *Model Law on Electronic Commerce* (MLEC), all'art. 5, poi incluso nel 2005 nella *United Nations Convention on the Use of Electronic Communications in International Contracts*, all'art. 8. Sui due testi, vedi L. CASTELLANI, *I testi dell'UNCITRAL in materia di diritto del commercio elettronico*, in G. FINOCCHIARO, F. DELFINI (a cura di), *Diritto dell'informatica*, Milano: Utet, 2014, pp. 44-46.

parti; pertanto, in assenza di esso, lo *smart contract* non può considerarsi alla stregua di un contratto, nonostante contenga in sé la rappresentazione di clausole contrattuali. Diversamente, chiunque potrebbe caricare unilateralmente uno *smart contract*; la mera registrazione in *blockchain* non sarebbe elemento sufficiente a ipotizzare la presenza di una volontà comune⁴.

Seppur gli *smart contract* non siano di per sé contratti, né debbano avere necessariamente una rilevanza legale, certamente possono essere utilizzati in ambito contrattuale per la conclusione e/o esecuzione di contratti⁵. Se utilizzati in ambito contrattuale, vengono usualmente denominati “*smart legal contracts*”, per rimarcare la differenza con lo “*smart contract code*”⁶. In aggiunta, essi possono operare indipendentemente dalla *blockchain*, essendo addirittura antecedenti alla sua invenzione⁷.

Nel panorama *blockchain*, gli *smart contracts* rientrano tra le applicazioni più evolute. La collocazione di uno *smart contract* in *blockchain* consente di trarre vantaggio dalle caratteristiche di quest’ultima, in particolare la capacità di resistenza alle manomissioni (o immutabilità) e la decentralizzazione⁸.

La *blockchain* è un sistema distribuito, i cui dati sono replicati in copie dislocate in molteplici dispositivi elettronici, o “nodi”, essendo conseguentemente la loro perdita meno probabile. Inoltre, i dati inseriti in *blockchain* sono abbinati a degli “*hash*”, delle stringhe alfanumeriche univoche che variano al mutare del dato sottostante, raggruppati in blocchi. Ogni blocco ha il proprio *hash* identificativo che riporta al suo interno anche l’*hash* del blocco cronologicamente antecedente, fino a formare una catena (da cui il termine “*blockchain*”, o “catena di blocchi”). Grazie a questa particolare conformazione, ogni tentativo di cambiamento può essere immediatamente individuato, giacché determinerebbe la modifica dell’*hash* e di quelli successivi, che sarebbero a loro volta difforni dagli *hash* corrispondenti posti negli altri nodi della *blockchain*. La decentralizzazione,

⁴ C. SILLABER, B. WALT, *Life Cycle of Smart Contracts in Blockchain Ecosystems*, in *Datenschutz und Datensicherheit*, 2017 (VIII), pp.498-499. I due autori osservano che: «*although a smart contract has been stored on the blockchain, this fact alone should not be considered as a party’s agreement to enter the contract as anybody can submit any smart contract to the blockchain indicating an obligation for any random wallet owner.*»

⁵ La piattaforma più famosa è Ethereum (<https://ethereum.org/it/>).

⁶ J. STARK, *Making Sense of Blockchain Smart Contracts*, *CoinDesk*, 7 giugno 2016, <https://www.coindesk.com/making-sense-smart-contracts>.

⁷ Vedi *infra*, par. 2.

⁸ Lo EUROPEAN UNION BLOCKCHAIN OBSERVATORY AND FORUM, *Legal and Regulatory Framework of Blockchains and Smart Contracts*. 27 settembre 2019, <https://www.eu-blockchainforum.eu/reports>, dà la seguente definizione di *smart contract*: «*In the blockchain context, it generally means computer code that is stored on a blockchain and one or more parties can access that. These programs are often self-executing and make use of blockchain properties like tamper-resistance, decentralised processing, and the like*» (p. 22).

invece, concerne il peculiare meccanismo di duplicazione del dato in molteplici copie; mentre esso avviene normalmente a partire da un nodo centrale, in *blockchain* l'aggiornamento del database viene effettuato in contemporanea su tutti i nodi grazie alle regole stabilite da un protocollo informatico comune, o meccanismo di consenso⁹. Tale modalità consente di evitare i costi e gli eventuali errori di trasmissione del dato da un nodo all'altro, a vantaggio della trasparenza delle informazioni da condividere e di una maggiore efficienza, sia in termini di tempo che economici¹⁰.

Esistono svariate tipologie di blockchain. Si suole distinguere normalmente tra *blockchain permissionless* e *permissioned*. La differenza sta nei permessi conferiti ai soggetti che prendono parte alla *blockchain* mettendo a disposizione un proprio nodo. Nello specifico, vi sono anzitutto il permesso di scrivere (cioè di generare nuove transazioni) e di aggiornare la *blockchain* aggiungendo nuovi blocchi. Nelle *blockchain permissionless*, chiunque può divenire un utente e inserire dati in *blockchain*, oltre che aggiornare il database mediante la validazione delle transazioni effettuate. Nelle *blockchain permissioned*, tali permessi sono concessi solamente a taluni soggetti preidentificati. Un ulteriore permesso concerne la lettura di quanto incluso in *blockchain*. Le *blockchain permissionless* sono solitamente ad accesso pubblico, mentre le *blockchain permissioned* sono generalmente private, poiché le transazioni sono visibili solo agli utenti autorizzati. La ragione sta nel

⁹ Il protocollo di consenso più noto prende il nome di “*Proof of Work*” (PoW), e consiste in una competizione tra nodi (*miners*); il primo tra questi che risulti capace di risolvere un complesso problema matematico, trovando un *hash* che sia composto da un numero predeterminato di zeri nella parte iniziale, è legittimato ad inserire un nuovo blocco e a ricevere una ricompensa per il lavoro svolto. Tuttavia, ci sono centinaia di diversi meccanismi di validazione che si basano su diverse strategie del consenso. Un'altra modalità molto citata è la “*Proof of stake*” (PoS) che si basa sulla validazione delle informazioni da parte di coloro che hanno più risorse (e.g., bitcoin, potenza di calcolo, etc.). Tali meccanismi sono stati suddivisi in tre famiglie: consenso basato su algoritmi che dimostrano l'esistenza di un certo criterio sulla base di un lavoro-work (es. PoW; PoS; *Proof of Reputation* (PoR); etc.); algoritmi basati sulla votazione di nodi qualificati (es. *Delegated Proof of Stake* (DPoS); *Random Lottery*, etc.); algoritmi basati sull'autenticazione dei nodi nei quali si registrerà la transazione (es. *Proof-of-Authentication* (PoAh)). Sul tema, vedi A. SINGH *et al.*, *A survey and taxonomy of consensus protocols for blockchains*, in *Journal of Systems Architecture*, 2022 (CXXVII), <https://www.sciencedirect.com/science/article/abs/pii/S1383762122000777>.

¹⁰ Più diffusamente sulla tecnologia *blockchain*, vedi, in ambito italiano: C. BOMPRESZI, M. PALMIRANI, *Blockchain e smart contract*, in A.M. GAMBINO (a cura di), *Persona e diritti digitali nella smart city*, in G.F. FERRARI (a cura di), *Innovazione e sostenibilità per il futuro delle smart cities*, Milano: Mimesis, 2023, pp. 275-298; S. COMELLINI, M. VASAPOLLO, *Blockchain, criptovalute, I.C.O. e smart contract*, Rimini: Maggioli, 2019; L.M. PERUGINI, *Distributed ledger technologies e sistemi di blockchain: digital currency, smart contract e altre applicazioni*, Milano: Key editore, 2018; M. NICOTRA, F. SARZANA DI SANT'IPPOLITO, *Diritto della blockchain, intelligenza artificiale e IoT*, Milano: Ipsoa, 2018. In ambito internazionale: I. BASHIR, *Mastering blockchain*, Birmingham: Packt, 2018; M. SWAN, *Blockchain, Blueprint for a New Economy*, Sebastopol: O' Reilly, 2015; A. WRIGHT, P. DE FILIPPI, *Decentralized Blockchain Technology and The Rise of Lex Cryptographia*, in SSRN, 2015, <http://papers.ssrn.com/abstract=2580664>.

fatto che le *blockchain permissionless* sono *general purpose* e la loro architettura è creata dall'aggiunta progressiva dei nodi di chiunque voglia accedervi; al contrario, le *blockchain permissioned* sono costruite appositamente per uno scopo predefinito, sia esso di una singola entità o, ad esempio, di un consorzio, che decidono di investire nella creazione dell'intero sistema *hardware* e *software*¹¹.

Essendo un database, la *blockchain* può memorizzare sia il programma informatico che la sua esecuzione nel tempo, secondo il processo decentralizzato e *tamper-resistant* sopra descritto. Ne deriva l'impossibilità unilaterale di apprestare dei cambiamenti nel codice o di arrestarne l'operatività una volta avvenuto il *deployment* in *blockchain*¹². Per questa ragione, qualora lo *smart contract blockchain-based* venga utilizzato in ambito contrattuale, si è ritenuto che si possa evitare l'inadempimento della parte obbligata alla quale, una volta che lo *smart contract* venga attivato sulla *blockchain*, sarebbe impedito di governare l'esecuzione della propria prestazione, che avverrebbe automaticamente.

2. Smart Contract e Smart Legal Contract

L'espressione "*smart contract*" è stata coniata negli Anni '90 dall'informatico Nick Szabo¹³, con cui egli intendeva «a computerized transaction protocol that executes the terms of a contract»¹⁴. Szabo teorizzava di demandare interamente l'attività contrattuale a dei software, ritenuti più affidabili dell'uomo¹⁵. Al tempo, le teorie di Szabo non erano supportate da una specifica tecnologia¹⁶. Nel decennio successivo si sono sviluppati dei sistemi informatici in grado di processare termini contrattuali espressi sotto forma di dati informatici. Harry Surden ha denominato tale capacità dei computer di "leggere" clausole contrattuali come "*data-*

¹¹ Per approfondimenti sulle tipologie di blockchain, si veda EUROPEAN COMMISSION, JOINT RESEARCH CENTRE, *Blockchain Now and Tomorrow – Assessing Multidimensional Impacts of Distributed Ledger Technologies*, 2019, p. 15; G. HILEMAN, M. RAUCHS, *2017 Global Blockchain Benchmarking Study*, in SSRN, 2017, p. 20, <https://ssrn.com/abstract=3040224>.

¹² P. DE FILIPPI, A. WRIGHT, *Blockchain and the law – the rule of code*, Cambridge: Harvard University Press, 2018, pp. 74-75; R. H. WEBER, *Smart Contracts: Do we need New Legal Rules?*, in A. DE FRANCESCO, R. SCHULZE (a cura di), *Digital Revolution – New Challenges for Law*, München: Beck Nomos, 2019, pp. 299-312; A. STAZI, *Automazione contrattuale e "contratti intelligenti" – Gli smart contracts nel diritto comparato*, Torino: Giappichelli, 2019.

¹³ Per ulteriori informazioni su Nick Szabo, vedi il seguente link: https://en.wikipedia.org/wiki/Nick_Szabo.

¹⁴ N. SZABO, *Formalizing and Securing Relationships on Public Networks*, *First Monday*, 1997, <https://firstmonday.org/ojs/index.php/fm/article/view/548>.

¹⁵ K. WERBACH, N. CORNELL, *Contracts Ex Machina*, in *Duke Law Journal*, 2017 (LXVII), pp. 313-382.

¹⁶ M. GIANCASPRO, *Is a 'smart contract' really a smart idea? Insights from a legal perspective*, in *Computer Law & Security Review*, 2017 (XXXIII), pp. 825-835.

oriented contracting”¹⁷, e come “*computable contracts*” la possibilità dei medesimi di sostituire la parte contrattuale¹⁸. Come affermato dallo stesso Surden, però, con i *computable contract* se le parti non sono soddisfatte dal risultato dell’elaborazione del computer, possono scartarlo. Permangono dunque il monitoraggio e la supervisione umana¹⁹.

Gli *smart contracts* basati su *blockchain*, diversamente, appaiono come la realizzazione concreta di quanto precedentemente immaginato da Nick Szabo. La decentralizzazione e la resistenza alle manomissioni (o immutabilità) della *blockchain* impedirebbero alla parte debitrice di poter influenzare l’esecuzione del contratto una volta che lo *smart contract* sia stato attivato sulla *blockchain*, rendendolo autonomo²⁰. Pertanto, si ritiene che la *blockchain* rimuova il bisogno da parte del creditore di fare affidamento sul debitore circa l’adempimento del contratto²¹. Si passerebbe dalla fiducia nella controparte contrattuale umana alla fiducia nel codice²², potendo così aumentare le *chances* di soddisfare pienamente l’interesse del creditore²³,

In senso contrario, sono state teorizzate svariate situazioni in cui, nonostante la *blockchain*, l’auto-esecuzione di prestazioni per mezzo di *smart contract* non garantirebbe il soddisfacimento della parte creditrice. Volendo tentare una schematizzazione, si potrebbero identificare tre gruppi: a) il codice informatico non è conforme alla volontà delle parti; b) il verificarsi di malfunzionamenti tecnici;

¹⁷ H. SURDEN, *Computable Contracts*, in *U. C. Davis Law Review*, 2012 (XLVI), pp. 629-700.

¹⁸ *Ibid.*, p. 658.

¹⁹ K. WERBACH, N. CORNELL, *Contracts Ex Machina*, cit., pp. 322-323.

²⁰ P. DE FILIPPI, A. WRIGHT, *Blockchain and the Law – the Rule of Code*, cit., pp. 74-75; R.H. WEBER, *Smart Contracts: Do we need New Legal Rules?*, cit., p. 308; A. STAZI, *Automazione contrattuale e “contratti intelligenti” – Gli smart contracts nel diritto comparato*, cit., p. 100; M. MAUGERI, *Smart contracts e disciplina dei contratti*, Bologna: Il Mulino, 2021, p. 24.

²¹ A. SAVELYEV, *Contract law 2.0: ‘smart’ contracts as the beginning of the end of classic contract law*, in *Higher School of Economics Research Paper no. WP BRP 71/LAW/2016*, 2016, p. 11, <https://ssrn.com/abstract=2885241>; P. CUCCURU, *Blockchain ed automazione contrattuale, riflessioni sugli smart contract*, cit., p. 107.

²² T. J. De GRAAF, *From old to new: from internet to smart contracts and from people to smart contracts*, in *Computer Law & Security Review*, 2019 (XXXV), pp. 1-11. L’autore fa l’esempio dello sblocco di un’auto intelligente noleggiabile dietro pagamento mediante apposita *app*. Questi sostiene che, mentre senza *blockchain* il sistema informatico in grado di aprire o chiudere l’auto sarebbe sotto il controllo del noleggiatore, con la *blockchain* quest’ultimo non potrebbe alterarne il funzionamento.

²³ Secondo M. CRISAFULLI, *L’era degli Smart Contracts: potenzialità e limiti di uno strumento rivoluzionario*, in *Diritto Mercato Tecnologia*, 3 giugno 2021, p. 19 «In primo luogo, mediante l’impiego di un processo di esecuzione totalmente automatizzato, è chiaro che, almeno ipoteticamente, si potrà avere una consequenziale diminuzione di liti e dispute collegate alla materia contrattuale. In secondo luogo, come aspetto direttamente correlato al primo, andrebbero a perdere di importanza tutti quegli strumenti di garanzia volti ad assicurare l’adempimento del debitore».

c) il carattere chiuso della blockchain quando l'adempimento del contratto implica forme di interazione con il mondo esterno²⁴.

La prima ipotesi è facilmente intuibile: quando il codice dello *smart contract* non combacia con quanto voluto dalle parti, indipendentemente dal fatto che l'esecuzione avvenga correttamente sul piano tecnico, sul piano giuridico si configura un inadempimento contrattuale.

Per quanto concerne la seconda, problemi tecnici potrebbero colpire una o più componenti di un'applicazione *blockchain-based*,²⁵ influenzando negativamente sulla corretta esecuzione del contratto. Anzitutto, come ogni programma informatico, lo *smart contract* stesso potrebbe avere dei *bug*²⁶. Altre problematiche potrebbero affliggere il protocollo *blockchain* sottostante²⁷, con conseguenze negative sullo *smart contract* ivi registrato²⁸. Anche gli *oracle* – interfacce che trasmet-

²⁴ Tale schematizzazione è proposta da C. BOMPRESZI, *From Trust in the Contracting Party to Trust in the Code in Contract Performance: A Critical Analysis of the Relationship between Blockchain-Based Smart Contracts and Consumer Protection*, in *EuCML*, 2021 (IV), pp. 148-159.

²⁵ Ogni soluzione *blockchain* potrebbe intendersi come la somma di più livelli, o “*multi-layered*”. In estrema sintesi, alla base vi è il *protocol layer*, cioè l'infrastruttura hardware e software del database; su questo si eseguono i software delle varie applicazioni, che costituiscono il livello sovrastante, o *application layer*, dove si trovano anche gli *smart contract*. vedi G. HILEMAN, M. RAUCHS, 2017 *Global Blockchain Benchmarking Study*, in *SSRN*, p. 26, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3040224. Vi sono svariati *providers* di soluzioni *blockchain*; Vedi J SINGH, J.D MICHELS, *Blockchain as a Service*, in *Queen Mary University of London, School of Law, Legal Studies Research Paper No. 269/2017*, p. 4, <https://ssrn.com/abstract=3091223>, parlano di “*Blockchain-as-a-Service*” (*BaaS*), *service providers* che offrono e gestiscono varie componenti di un'infrastruttura DLT. Vedi A. DAVOLA, *Blockchain e smart contract as a service: prospettive di mercato e criticità normative delle prestazioni BAAS e SCaaS alla luce di un'incerta qualificazione giuridica*, in *Il Diritto Industriale*, 2020 (II), p. 147, distingue tra *Blockchain as a Service (BaaS)* e *Smart Contract as a Service (SCaaS)*.

²⁶ A. SAVELYEV, *Contract law 2.0: 'smart' contracts as the beginning of the end of classic contract law*, cit., p. 14; per esempio, nel 2016 Peter Vessenes (co-fondatore della Bitcoin Foundation) ha stimato che gli *smart contract* di Ethereum contenevano 100 errori ogni 1000 linee di codice informatico. Vedi P. VESSENES, *Ethereum Contracts are Going to be Candy for Hackers*, *Vessenes*, 18 maggio 2016, <http://vessenes.com/ethereum-contracts-are-going-to-be-candy-for-hackers/>.

²⁷ E. MIK, *Blockchains. A Technology for Decentralized Marketplaces*, in L.A. DI MATTEO *et al.* (a cura di), *The Cambridge Handbook of smart contracts, blockchain technology and digital platforms*, Cambridge: Cambridge University Press, 2020, pp. 160-182. Esse concernono primariamente la selezione e l'ordine delle transazioni. Al riguardo, vedi L. LUU *et al.*, *Making Smart Contracts Smarter*, *ACM SIGSAC Conference on Computer and Communications Security*, Vienna 2016, pp. 254-269, <https://doi.org/10.1145/2976749.2978309>. Per esempio, il contributo cita la cd “*transaction-ordering dependency*”, che si verifica quando più transazioni invocano lo stesso *smart contract*. Ciò può dare risultati inaspettati ad un utente che invoca uno *smart contract* quando ci sono altre transazioni concomitanti, a seconda dell'ordine in cui le transazioni sono validate e aggiunte in *blockchain*. Si immagini, in un contratto di vendita, che il venditore aggiorni il prezzo del bene in vendita al rialzo; l'acquirente potrebbe dover pagare un prezzo più alto di quello che abbia accettato di pagare inviando la propria accettazione, qualora la transazione di aggiornamento del prezzo del venditore si collochi temporalmente prima di quella di accettazione del contratto dell'acquirente.

²⁸ Riprendendo l'esempio della *transaction-ordering dependency* descritto alla nota che precede, si potrebbe pensare ad un *Puzzle contract* in Ethereum, che ricompensa gli utenti che risolvono un

tono le informazioni da e verso la *blockchain* – potrebbero non funzionare a regola d'arte²⁹. Un loro non corretto operare potrebbe minare alla realizzazione del volere contrattuale³⁰. Da ultimo, posto che gli *oracle* traggono gli input da inviare allo *smart contract* da fonti esterne di dati è indispensabile che anche queste ultime siano affidabili. Invero, anche le fonti di dati potrebbero essere soggette a malfunzionamenti o inattive³¹.

Infine, il terzo gruppo ricomprende i casi in cui l'esecuzione del contratto è inattuabile senza il collegamento tra ciò che si svolge *on-chain* e *off-chain*. Infatti, la *blockchain* è stata definita “*deaf and blind*”, non potendo direttamente ricevere informazioni se non quelle ricavabili al suo interno³² (si pensi, ad esempio, ad un trasferimento di *token* rappresentanti beni nativi di *blockchain* in cambio di un certo ammontare in criptovalute). Da qui l'importanza degli *oracle* e delle fonti esterne di dati, di cui sopra³³. Dunque, se tali informazioni non vengono trasmesse in modo appropriato o non vengono affatto veicolate, lo *smart contract* non si esegue o non si esegue correttamente, con quanto ne può seguire sul piano dell'adempimento contrattuale. D'altra parte, ciò può accadere non solo a causa di malfunzionamenti tecnici (in tal caso, si ricadrebbe nel secondo gruppo), ma anche per azioni o errori umani. Si immagini la consegna di un'opera d'arte (registrata in *blockchain* mediante apposito NFT) da parte di un trasporta-

puzzle computazionale. L'obbligato potrebbe sfruttare la *transaction-ordering*. Vale a dire, questi potrebbe aspettare fino a quando un utente non invii una soluzione corretta del puzzle e inviare immediatamente una transazione che riduca la ricompensa del contratto a zero. Se quest'ultima transazione viene aggiunta in *blockchain* prima di quella dell'utente, questi non ottiene alcuna ricompensa. Un altro esempio è il famigerato “*TheDao hack*” del 2016, dove un hacker è stato in grado di rubare oltre tre milioni di *ethers* (la criptovaluta di Ethereum) utilizzando la cd “*reentrancy vulnerability*”. Vedi L. LUU *et al.*, *Making Smart Contracts Smarter*, cit., pp. 257-259.

²⁹ E. MIK, *Smart contracts: terminology, technical limitations and real world complexity*, in *Journal of Law, Innovation and Technology*, 2017 (IX), pp. 269-300.

³⁰ Gli *oracle* potrebbero inviare informazioni errate allo *smart contract* (in entrata) o all'esterno della *blockchain* (in uscita).

³¹ M. GIANCASPRO, *Is a 'smart contract' really a smart idea? Insights from a legal perspective*, cit., p. 833. Si pensi ad un contratto di assicurazione intelligente programmato per pagare l'assicurato in caso di ritardo di un volo aereo di due ore. Si potrebbe immaginare che il *software* dell'aeroporto che riporta gli orari di arrivo non funzioni per alcune ore, e non registri il ritardo. L'esempio è di M. CLÉMENT, *Smart Contracts and the Courts*, in L.A. Di MATTEO *et al.* (a cura di), *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms*, cit., p. 280.

³² O. RIKKEN *et al.*, *Smart contracts as a specific application of blockchain technology*, 2017, p. 17, <https://dutchdigitaldelta.nl/uploads/pdf/Smart-Contracts-ENG-report.pdf>.

³³ A.U. JANSSEN, F.P. PATTI, *Demistificare gli smart contracts*, in *Osservatorio del Diritto Civile e Commerciale*, 2020 (I), pp. 31-50, spec. p. 41: «gli oracles forniscono allo smart contract le informazioni esterne necessarie per l'esecuzione (ad esempio, il prezzo delle azioni o il prezzo dell'oro). È dunque evidente che l'utilizzazione di oracle si pone in contrasto con l'assunto secondo cui gli smart contracts si eseguono automaticamente. Ogni oracle riduce il livello di automazione del contratto, poiché implica uno o più passaggi ulteriori nel processo di esecuzione delle prestazioni».

tore specializzato, che indichi erroneamente di aver condotto il bene a destinazione, mentre quest'ultimo non sia affatto pervenuto all'indirizzo del destinatario, oppure sia difforme da quanto concordato nel contratto.

Sempre a causa della natura chiusa di *blockchain*, l'esecuzione dello *smart contract* potrebbe dover essere accompagnata da altre azioni al di fuori del registro per l'adempimento del contratto. Riprendendo l'esempio fatto pocanzi dell'opera d'arte, si pensi alla prestazione di consegna fisica del bene.

3. Smart Contract e Data Act

Il Regolamento europeo sui dati, meglio conosciuto come *Data Act*,³⁴ fa parte degli atti legislativi dell'Unione europea che rientrano nella "Strategia europea in materia di dati",³⁵ il cui obiettivo è quello di creare un mercato unico in cui i dati possano circolare liberamente nello spazio europeo, a beneficio di cittadini, imprese e pubbliche amministrazioni, con regole chiare ed eque. In particolare, con il *Data Act* si mira a rendere disponibile per l'uso un maggior numero di dati e a stabilire norme su chi può utilizzarli e accedervi e per quali scopi in tutti i settori economici dell'UE.

Su questo, gli *smart contract* acquisiscono un ruolo centrale, potendo fornire ai titolari e ai destinatari dei dati garanzie del rispetto degli accordi di condivisione dei dati³⁶. Infatti, al considerando 47 il *Data Act* suggerisce l'uso di contratti intelligenti per gestire accordi a lungo termine tra i titolari e i destinatari dei dati, al fine di ridurre i costi in operazioni regolari e ripetitive nell'ambito di una relazione commerciale. Inoltre, i contratti intelligenti sono citati tra le adeguate misure tecniche di protezione che il titolare dei dati può applicare per impedire l'accesso non autorizzato ai dati (v. art. 11).

Oltre che suggerire il ricorso a contratti intelligenti per gestire le condizioni di accesso e condivisione dei dati, il *Data Act* si occupa, altresì, di fornire una definizione di "contratto intelligente"³⁷ e di stabilire i requisiti essenziali che tali

³⁴ Regolamento (UE) 2023/2854 del Parlamento europeo e del Consiglio, del 13 dicembre 2023, riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo e che modifica il regolamento (UE) 2017/2394 e la direttiva (UE) 2020/1828 (regolamento sui dati), GU L, 2023/2854, 22.12.2023, pp. 1-71.

³⁵ https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_it.

³⁶ EU BLOCKCHAIN OBSERVATORY AND FORUM, *Smart Contracts*, 4 November 2022, p. 20, https://blockchain-observatory.ec.europa.eu/publications/smart-contracts_en).

³⁷ Ai sensi dell'art. 2, par. 1, n. 39, un "contratto intelligente" è «un programma informatico utilizzato per l'esecuzione automatica di un accordo o di parte di esso utilizzando una sequenza di registrazioni elettroniche di dati e garantendone l'integrità e l'accuratezza del loro ordine cronologico».

contratti intelligenti devono avere per essere utilizzati per l'esecuzione degli accordi di condivisione dei dati succitati³⁸.

Coerentemente a quanto già ribadito, i contratti intelligenti non sono necessariamente legati alla *blockchain*, essendo la nozione di contratto intelligente *ivi* fornita tecnologicamente neutra³⁹. Ma, come esplicitato al considerando 104 del regolamento in esame, “*i contratti intelligenti possono ad esempio essere collegati a un registro elettronico*”. La locuzione di registro elettronico si ricava dal nuovo Regolamento eIDAS, con un chiaro riferimento alla *blockchain*, su cui si veda *infra*.

4. Blockchain e Regolamento eIDAS

Il recente Regolamento UE n. 1183 del 2024⁴⁰, di modifica del Regolamento UE n. 910 del 2014 altrimenti conosciuto come Regolamento eIDAS (da cui il riferimento al regolamento di modifica come eIDAS 2) ha previsto, tra i nuovi servizi fiduciari, il registro elettronico, definito quale «una sequenza di registrazioni di dati elettronici che garantisce l'integrità di tali registrazioni e l'accuratezza dell'ordine cronologico di tali registrazioni» (art. 3, punto 52). L'art. 45 *duodecies*, nel suo primo paragrafo, contrasta la negazione di effetti giuridici ai registri elettronici e l'ammissibilità come prova unicamente per via della forma elettronica⁴¹. Dalla lettura congiunta del primo e del secondo paragrafo dell'art. 45 *duodecies* emerge poi una suddivisione tra registri elettronici semplici e registri elettronici qualificati, quest'ultimo inteso come «un registro elettronico fornito da un prestatore di servizi fiduciari qualificato e che soddisfa i requisiti di cui all'articolo 45 *terdecies*» (art. 3, par. 1, n. 53). Le due tipologie si differenziano dal punto di vista dell'effetto giuridico. Più precisamente, l'articolo non disciplina gli effetti giuridici del registro elettronico semplice, ma questi ultimi possono dedursi da quanto disposto per i registri elettronici qualificati, per i quali si presume l'ordine cronologico sequenziale univoco e l'integrità dei dati in

³⁸ Ai sensi dell'art. 36, i requisiti essenziali sono: robustezza e controllo dell'accesso; cessazione e interruzione sicure; archiviazione e continuità dei dati; controllo dell'accesso; coerenza. La conformità ai requisiti essenziali è presunta nei casi previsti ai paragrafi successivi dell'art. 36. Ai sensi della Proposta Digital Omnibus (COM(2025) 837 final del 19/11/2025) l'art. 36 verrebbe soppresso per evitare difficoltà sul piano dei costi e delle opportunità nei confronti degli innovatori. La soppressione “*promuovrebbe pertanto lo sviluppo e l'introduzione sul mercato di nuovi modelli di business, favorirebbe l'innovazione e ridurrebbe gli ostacoli per le tecnologie emergenti*” (v. cons. 16).

³⁹ Vedi cons. 104.

⁴⁰ Regolamento (Ue) 2024/1183 del Parlamento europeo e del Consiglio dell'11 aprile 2024 che modifica il regolamento (UE) n. 910/2014 per quanto riguarda l'istituzione del quadro europeo relativo a un'identità digitale, GU L, 2024/1183, 30.04.2024, pp. 1-56.

⁴¹ In ossequio al principio di non discriminazione, elaborato originariamente in seno all'UNCITRAL e adottato nel Model Law on electronic Commerce del 1996, nel Model Law on Electronic Signatures del 2001 e nella Convention on the Use of Electronic Communications in International Contracts del 2005, nonché trasposto nel Regolamento eIDAS.

essi contenuti. La presunzione viene fatta valere mediante la dimostrazione del raggiungimento dei requisiti propri di un registro elettronico qualificato (elencati al successivo art. 45 *terdecies*)⁴². Viceversa, in caso di registro elettronico semplice varrà la valutazione discrezionale del giudice. Un registro elettronico qualificato è riconosciuto come tale, secondo il principio del mutuo riconoscimento, in tutti gli altri Stati membri (art. 24-*bis*, n. 11).

Il Regolamento eIDAS 2 riconosce a livello europeo effetti giuridici alla *blockchain*. L'utilizzo dell'espressione "registro elettronico" è chiaramente ispirata al principio della neutralità tecnologica. In futuro, infatti, potrebbero nascere tecnologie diverse dalla *blockchain*, seppur con le medesime caratteristiche, con il rischio di non trovare una copertura normativa. Oltretutto, esistono già sistemi distribuiti alternativi alla *blockchain*, ma sprovvisti dell'usuale raggruppamento delle transazioni di dati in blocchi, i quali vengono erroneamente denominati *blockchain* poiché in grado di fornire le stesse funzionalità. Il rispetto del principio della neutralità tecnologica, invece, rende la disciplina adatta agli sviluppi e alle varianti future, in questo campo presumibilmente molto plausibili e rapidi data la giovinezza della tecnologia.

Dall'analisi di questi articoli si desume che il legislatore europeo intende accostare alla *blockchain* effetti giuridici più ampi della mera validazione temporale elettronica⁴³, da cui va distinta⁴⁴.

L'art. 8-*ter* della Legge n. 12 dell'11 febbraio 2019, di conversione del decreto legge 14 dicembre 2018, n. 135, rubricato "Tecnologie basate su registri distribuiti e smart contract", fornisce una definizione di tecnologie basate su registri distribuiti e di *smart contracts*, a cui riconosce determinati effetti giuridici. La norma, che è già stata oggetto di molte critiche⁴⁵, appare per buona parte in contrasto con le previsioni del Reg. eIDAS 2 sui registri elettronici.

⁴² La Commissione europea entro il 21 maggio 2025 stabilisce mediante atti di esecuzione un elenco di norme di riferimento e, se necessario, specifiche e procedure applicabili ai requisiti prescritti per i registri elettronici qualificati, secondo la classica procedura prescritta all'articolo 48, par. 2, del Regolamento. La rispondenza dei registri elettronici alle norme, alle specifiche e alle procedure di cui agli atti d'esecuzione della Commissione ammette di poter presumere il rispetto dei requisiti elencati all'art. 45 *terdecies*, par. 1 (vedi art. 45 *terdecies*, par. 2 e 3).

⁴³ C. BOMPRESZI, *Nuovo eIDAS e registri elettronici: regole e impatti per i servizi fiduciari*, *AgendaDigitale.eu*, 9 settembre 2021, <https://www.agendadigitale.eu/documenti/nuovo-eidas-e-registri-elettronici-le-nuove-regole-e-gli-impatti-per-i-servizi-fiduciari/>.

⁴⁴ Vedi cons. 68 Reg. eIDAS 2.

⁴⁵ Vedi S. RIGAZIO, *Smart contracts e tecnologie basate su registri distribuiti nella L. 12/2019*, in *Dir. Inf. Inf.*, 2021(II), pp. 369-395; G. REMOTTI, *Blockchain smart contract. Un primo inquadramento*, in *Oss. dir. civ. e comm.*, 2020 (I), pp. 189-228; G. FINOCCHIARO, *Intelligenza artificiale e protezione dei dati personali*, in *Giurisprudenza Italiana*, 2019 (VII), pp. 1670-1677; M. MANENTE, *L. 12/2019 – Smart contract e tecnologie basate su registri distribuiti – prime note*, Studio 1_2019, Marzo 2019, p. 6, https://www.notariato.it/ufficio_studi/studio-12019-di-legge-122019-smart-contract-e-tecnolo-

A mente del comma 1 dell'art. 8-ter, sono “tecnologie basate su registri distribuiti” *quelle* «tecnologie e protocolli informatici che usano un registro condiviso, distribuito, replicabile, accessibile simultaneamente, architetturealmente decentralizzato su basi crittografiche, tali da consentire la registrazione, la convalida, l'aggiornamento e l'archiviazione di dati sia in chiaro che ulteriormente protetti da crittografia verificabili da ciascun partecipante, non alterabili e non modificabili». La definizione rimanda evidentemente alle cosiddette “*distributed ledger technologies*” (o DLT), e dunque si riferisce ad una tecnologia specifica, di cui esplicita alcune caratteristiche tecniche, contrariamente alla scelta del legislatore europeo di sposare il principio di neutralità tecnologica sia nella denominazione che nella descrizione del *database*.

Il comma 3, poi, sancisce che «la memorizzazione di un documento informatico attraverso l'uso di tecnologie basate su registri distribuiti produce gli effetti giuridici della validazione temporale elettronica di cui all'articolo 41». La validazione temporale elettronica, secondo la definizione dell'art. 3, par. 1, n. 33 del Regolamento eIDAS consente di accostare data e ora a dati in forma elettronica ad opera di altri dati in forma elettronica, al fine di provare l'esistenza dei medesimi in un determinato momento. Sinonimo di validazione temporale è l'utilizzo dell'espressione “marca temporale” (o “*timestamp*”), che normalmente viene effettuata mediante funzioni di “*hash*” in grado di generare un'impronta digitale univoca dei dati da validare.

Nel menzionare la validazione temporale elettronica, il comma 3 rimanda all'art. 41 del Regolamento eIDAS, che disciplina gli effetti giuridici della validazione temporale elettronica. In particolare, se la validazione temporale elettronica è qualificata (e cioè soddisfa determinati requisiti elencati all'art. 42 Reg.), essa gode della presunzione di accuratezza della data e dell'ora indicate e dell'integrità dei dati a cui data ed ora sono associate; in caso contrario, tale valutazione è rimessa al libero apprezzamento del giudice. Il quarto comma della legge italiana subordina la produzione degli effetti giuridici della validazione temporale all'individuazione di determinati *standard* tecnici elaborati dall'Agenzia per l'Italia digitale.

Ad ogni buon conto, il carattere obbligatorio e direttamente applicabile dello strumento del regolamento impone allo Stato italiano di adeguare il proprio or-

gie-basate-suregistratidistribuiti ; C. BOMPRESZI, *Commento in materia di Blockchain e Smart contract alla luce del nuovo Decreto Semplificazioni*, in *Diritto Mercato Tecnologia*, 2019, <https://www.dimt.it/news/breve-commento-alla-legge-11-febbraio-2019-n-12-di-conversione-del-decreto-legge-14-dicembre-2018-n-135-recante-disposizioni-urgenti-in-materia-di-sostegno-e-semplificazione-per-le-imprese-e-per-la-pu/>.

dinamento. In ogni caso, la mancata adozione di *standard* tecnici e linee guida da parte di AGID rende la disciplina italiana sostanzialmente inapplicata.

Un altro punto di contatto tra *blockchain* e regolamento eIDAS è la possibilità di qualificare come documento informatico ogni dato e/o informazione inseriti in *blockchain*, *smart contract* compresi. A ribadirlo è uno studio dell'EU Blockchain Observatory and Forum del 2019⁴⁶, per quanto ciò si possa ricavare immediatamente in via interpretativa. Ai sensi dell'eIDAS, infatti, il documento elettronico è «qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva» (art. 3, par. 1, n. 35)⁴⁷.

5. Blockchain e protezione dei dati personali

Nell'ambito della protezione dei dati personali, sono stati colti degli aspetti della tecnologia *blockchain* che potrebbero contribuire a raggiungere gli obiettivi posti dal GDPR e che potrebbero dunque rappresentare un'opportunità per la protezione dei dati personali degli utenti. Nella Dichiarazione istitutiva della *Blockchain Partnership* Europea⁴⁸ si è affermato che i servizi *blockchain-based* aiuteranno a preservare l'integrità dei dati e garantiranno una migliore gestione dei dati medesimi da parte dei cittadini e delle organizzazioni che interagiscono con le pubbliche amministrazioni. Il Parlamento europeo, in una Risoluzione del 3 ottobre 2018 ha dichiarato che la *blockchain* «può costituire uno strumento che rafforza l'autonomia dei cittadini dando loro l'opportunità di controllare i propri dati e decidere quali condividere nel registro, nonché la capacità di scegliere chi possa vedere tali dati»⁴⁹.

⁴⁶ EU BLOCKCHAIN OBSERVATORY AND FORUM, *Legal and Regulatory Framework of Blockchains and Smart Contracts*, cit., p. 21.

⁴⁷ Parimenti, ai sensi del Codice dell'Amministrazione Digitale (D.Lgs. 82/2005, o CAD) il documento informatico è in il documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti» (art. 1, 1° co., lett. p). Anche a livello internazionale, peraltro, le leggi *ad hoc* di California (California Assembly Bill 2658 <https://legiscan.com/CA/text/AB2658/id/1732549>), Tennessee (Tennessee Senate Bill No. 1662 <https://legiscan.com/TN/text/SB1662/2017>) e Arizona (Arizona House Bill No. 2417 <https://www.azleg.gov/legtext/53leg/1R/laws/0097.htm>), esplicitamente accostano ad ogni *record* in *blockchain* la denominazione di “*electronic record*”.

⁴⁸ Iniziativa che ha coinvolto 30 Stati europei per collaborare sul tema (<https://digital-strategy.ec.europa.eu/en/policies/blockchain-partnership>).

⁴⁹ Risoluzione del Parlamento europeo del 3 ottobre 2018 sulle tecnologie di registro distribuito e blockchain: creare fiducia attraverso la disintermediazione (2017/2772\(\text{RSP}\)), considerando A.

Capacità di tenuta sicura, trasparente e tracciabile dei dati, accesso e condivisione selettivi sarebbero in linea con alcuni importanti principi del GDPR, quali il principio di *privacy by design*⁵⁰, di trasparenza⁵¹ o di minimizzazione⁵².

D'altra parte, non mancano elementi di frizione tra la tecnologia *blockchain* e la normativa europea a tutela dei dati personali.

Una delle domande più ricorrenti tra gli esperti è se sia individuabile un titolare del trattamento⁵³ e, in caso affermativo, chi possa essere considerato tale, in presenza di applicazioni decentralizzate che colliderebbero con la visione centralizzata e gerarchica che accompagna il GDPR. Le maggiori difficoltà interessano le *blockchain* di tipo *permissionless*, in assenza di un'entità deputata a governare il sistema e ad assumere decisioni strategiche, e in cui i nodi sono uguali tra loro, senza limitazioni d'accesso, senza preidentificazione, senza predeterminazione a monte degli usi (e quindi delle finalità) per cui la *blockchain* è stata concepita.

⁵⁰ Art. 25 GDPR, per cui il titolare del trattamento deve mettere in atto «misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente Regolamento e a tutelare i diritti degli interessati».

⁵¹ Art. 5, par. 1, lett. a GDPR, ai sensi del quale i dati personali sono trattati «in modo lecito, corretto e trasparente nei confronti dell'interessato».

⁵² Art. 5, par. 1, lett. c GDPR, che richiede che i dati siano «adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati». Su questi aspetti, si veda A.M. GAMBINO, C. BOMPRESZI, *Blockchain e protezione dei dati personali*, in *Dir. Inf. Inf.*, 2019 (III), pp. 619-646. Più in generale, sul rapporto tra *blockchain* e protezione dei dati personali, vedi G. D'ACQUISTO, *Blockchain e GDPR: verso un approccio basato sul rischio*, in *Federalismi.it*, 2021 (II), pp. 53-65; U. TATAR *et al.*, *Law versus technology: Blockchain, GDPR, and tough tradeoffs*, in *Computer Law & Security Review*, 2020 (XXXVIII), pp. 1-11; F. FAINI, *Blockchain e diritto: la "catena del valore" tra documenti informatici, smart contracts e data protection*, in *Resp. civ. e prev.*, 2020 (I), pp. 297-316; M. FINCK, *Blockchain and the General Data Protection Regulation – Can distributed ledgers be squared with European data protection law?*, [https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU\(2019\)634445_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf); ID., *Blockchain regulation and Governance in Europe*, Cambridge: Cambridge University Press, 2018; ID., *Blockchains and Data Protection in the European Union*, Max Planck Institute for Innovation and Competition Research Paper n. 18-01; A.M. GAMBINO, C. BOMPRESZI, *Circolazione e protezione dei dati nella blockchain*, in A.M. GAMBINO, A. STAZI (a cura di), *La circolazione dei dati – Titolarità, strumenti negoziali, diritti e tutele*, Pisa: Pacini, 2020, pp. 213-240; T. LYONS *et al.*, *Blockchain and the GDPR – a Thematic Report Prepared by the European Union Blockchain Observatory and Forum*, 16 ottobre 2018, <https://www.eublockchainforum.eu/reports>; M. BERBERICH, M. STEINER, *Blockchain technology and the GDPR – How to Reconcile Privacy and Distributed Leers?*, in *European Data Protection Law Review*, 2016 (II), pp. 422-426; L. D. IBÁÑEZ *et al.*, *On Blockchains and the General Data Protection Regulation*, https://eprints.soton.ac.uk/422879/1/Block_chains_GDPR_4.pdf; P. DE FILIPPI, *The interplay between decentralization and privacy: the case of blockchain technologies*, in *JSRN*, 2016, <https://ssrn.com/abstract=2852689>.

⁵³ Ai sensi dell'art. 4, par. 1, n. 7 del GDPR, il titolare del trattamento è la persona fisica o giuridica che determina le finalità (il perché) e i mezzi (il come) del trattamento. Questi assume la responsabilità dell'osservanza delle norme a protezione dei dati personali nei confronti dei soggetti (interessati) i cui dati personali sono oggetto di trattamento da parte del titolare.

Le ricostruzioni in proposito sono varie. Tra le più accreditate quella che attribuirebbe il ruolo di titolare ai singoli nodi (o meglio, ai singoli *user*⁵⁴) del sistema, che si siano avvalsi dell'infrastruttura *blockchain* per un particolare scopo.

Anche qualora l'identificazione del titolare del trattamento sia astrattamente possibile, e si avvalori la tesi più condivisa sopra esposta, rimarrebbe arduo per il titolare poter monitorare e governare la gestione dei dati inseriti; l'ostacolo starebbe, cioè, nell'incontrollata duplicazione dei dati personali in nodi detenuti in luoghi e da soggetti non identificabili, in netto contrasto con i dettami delle più importanti norme del GDPR, primo tra tutti il principio di *accountability*⁵⁵.

Oggetto di dibattito è anche la presunta incompatibilità tra l'immutabilità di *blockchain* e alcuni principi e diritti che richiederebbero interventi successivi sul *database*, come il principio di limitazione della conservazione⁵⁶, il diritto di cancellazione⁵⁷ o di rettifica⁵⁸. Circa le soluzioni avanzate sul piano legale, la più plausibile sembra quella che intende la non disponibilità del dato non come distruzione fisica di esso, ma come inaccessibilità tecnica, attraverso varie modalità (come lo storage di dati *off-chain*, la distruzione della chiave privata, l'aggiunta di transazioni che annullino o correggano le precedenti, etc.). Rimane poi l'opzione tecnica di concepire *blockchain* editabili, come i *chameleon hashes*, che consentirebbero la modifica dell'*hash* pur non alterando quelli immediatamente successivi che compongono la catena di blocchi.

Un altro interrogativo attiene alla possibilità di parlare di trasferimento dei dati personali⁵⁹ a fronte dell'operazione di replica delle copie di *blockchain* in nodi all'infuori dei confini europei. Si è avanzato sul punto un parallelismo con la sentenza *Bodil Lindqvist* della Corte di Giustizia Europea⁶⁰, che ha negato che

⁵⁴ I nodi sarebbero semplicemente le componenti tecnologiche dell'infrastruttura, mentre gli *users* sarebbero i soggetti che, mediante collegamento ai nodi, inseriscono le transazioni.

⁵⁵ Il principio di *accountability* sta ad indicare la responsabilità che incombe sul titolare del trattamento e abbraccia una concezione del rischio che non è limitata alla fase della violazione, ma che si estende anche a quella precedente, in cui il dato non è stato violato ma potrebbe esserlo sulla base di determinati rischi che spetta al medesimo valutare, approntando tutta una serie di accorgimenti in via cautelativa. Problemi non si porrebbero con *blockchain permissioned*, che di fatto replicano un modello di *governance* centralizzato. Problemi non si porrebbero con *blockchain permissioned*, che di fatto replicano un modello di *governance* centralizzato.

⁵⁶ Art. 5, par.1, lett. e GDPR: i dati vanno «conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati».

⁵⁷ Art. 17 GDPR.

⁵⁸ Art. 16 GDPR.

⁵⁹ Il GDPR non fornisce una definizione di “trasferimento”, la quale è stata perciò elaborata per differenza rispetto al concetto di “comunicazione”: con il secondo, si intendono gli spostamenti di dati tra titolari, all'interno dell'Unione; con il primo, i movimenti di dati tra soggetti, titolari o responsabili, purché uno di essi localizzato fuori dai confini europei.

⁶⁰ Corte UE, 6 novembre 2003, C- 101/01 *Lindqvist*.

l'inserimento di dati personali in un sito web potesse essere qualificato come "trasferimento" per il fatto che al medesimo possono avere accesso destinatari situati al di fuori dell'Unione europea, perché «i dati personali che giungono al computer di una persona che si trova in un paese terzo, provenienti da una persona che li ha caricati su un sito Internet, non sono stati trasferiti direttamente tra queste due persone, ma attraverso l'infrastruttura informatica del fornitore di servizi di ospitalità presso il quale la pagina è caricata». Il ragionamento potrebbe essere esteso alla *blockchain*. Infatti, in *blockchain* gli *user* possono accedere ai dati contenuti nei blocchi, dai vari nodi in cui la *blockchain* è replicata, i quali potrebbero essere situati anche in Paesi terzi. Anche qui, i dati non sono trasferiti direttamente, ma all'esito di un processo di validazione e successiva replica nei nodi della *blockchain*. Anche qualora si discorra di trasferimento in senso affermativo, comunque, si discute la fattibilità di una conformità con le disposizioni del GDPR corrispondenti⁶¹. È stato infatti osservato che nelle *blockchain permissionless* i destinatari del trasferimento e la loro collocazione sono sconosciuti. In aggiunta, anche la possibilità di identificare un titolare del trattamento sarebbe dubbia. In assenza di questi elementi, l'assicurazione di un adeguato livello di protezione dei dati personali sarebbe preclusa.

Volendo fare un bilancio, un'inconciliabilità assoluta sarebbe da escludere, trattandosi peraltro di conclusione che arresterebbe il progresso tecnologico e il mercato di riferimento. Semmai, è stato suggerito un approccio caso per caso, tenuto anche conto del fatto che esistono più tipologie di *blockchain* e che le stesse sono diversamente modulabili a seconda della singola applicazione⁶². Le maggiori problematiche si riscontrano comunque innanzi a *blockchain permissionless*, su cui si dovrebbe dunque evitare di far ricadere la scelta⁶³.

⁶¹ Art. 44 ss. GDPR. Secondo la disciplina sul trasferimento, il trasferimento di dati personali è ammesso se la Commissione europea ha deciso che il luogo in cui il trasferimento è effettuato garantisce un livello di protezione adeguato (art. 45 GDPR). In assenza di una decisione in tal senso della Commissione europea, il trasferimento è consentito solo se il titolare o il responsabile del trattamento hanno fornito garanzie adeguate e a condizione che gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi (Art. 46 GDPR).

⁶² Secondo T. LYONS *et al.*, *Blockchain and the GDPR – a thematic report prepared by the European Union Blockchain Observatory and Forum*, cit., p. 16: «GDPR compliance is not about the technology, but it is about how the technology is used (...). There is no such thing as a GDPR-compliant blockchain technology. There are only GDPR-compliant use cases and applications».

⁶³ Lo studio condotto per lo European Parliamentary Research Service da M. FINCK, *Blockchain and the General Data Protection Regulation – Can distributed ledgers be squared with European data protection law?*, cit., suggerisce tre *policies*: l'elaborazione di specifiche linee guida da parte del Comitato europeo per la protezione dei dati, in maniera coordinata con le autorità di controllo nazionali; il ricorso a certificazioni e codici di condotta; la promozione di una ricerca interdisciplinare.

Nell'aprile del 2025, il Comitato Europeo per la Protezione dei Dati (EDPB) ha adottato delle Linee guida sul trattamento dei dati personali attraverso le tecnologie blockchain⁶⁴. Le linee guida sottolineano l'importanza di implementare misure tecniche e organizzative fin dalle prime fasi della progettazione del trattamento. L'EDPB chiarisce anche che i ruoli e le responsabilità dei diversi attori coinvolti nel trattamento dei dati personali tramite blockchain devono essere valutati durante la fase di progettazione. Inoltre, le organizzazioni dovrebbero effettuare una Valutazione d'Impatto sulla Protezione dei Dati (DPIA) prima di trattare dati personali tramite tecnologie blockchain, soprattutto se il trattamento potrebbe comportare un alto rischio per i diritti e le libertà delle persone. Secondo il Comitato, le organizzazioni dovrebbero anche garantire la massima protezione dei dati personali degli individui durante il trattamento, affinché questi dati non siano accessibili di default a un numero indefinito di persone. Le linee guida forniscono esempi di diverse tecniche di minimizzazione dei dati, così come di gestione e conservazione dei dati personali. In generale, si dovrebbe evitare di memorizzare dati personali in una blockchain se ciò contrasta con i principi della protezione dei dati. Infine, il Comitato evidenzia l'importanza dei diritti degli individui, in particolare riguardo alla trasparenza, alla rettifica e alla cancellazione dei dati personali.

6. Smart contract, Nft e metaverso

Oltre le criptovalute, che costituiscono il primo caso d'uso legato alla tecnologia *blockchain* come mezzo di pagamento alternativo al contante (es. *bitcoins*)⁶⁵, attualmente possono rinvenirsi risorse digitali sotto forma di “gettoni digitali”, o “*tokens*”, i quali possono rappresentare potenzialmente ogni diritto o bene, o della realtà (materiale e immateriale) o “*blockchain* nativi”, in quanto originatisi nella stessa *blockchain*⁶⁶ (come la cd “*crypto art*”)⁶⁷. Tali *tokens* traggono vantaggio dalle caratteristiche della *blockchain*, sopra descritte, divenendo anch'essi, come

⁶⁴ EUROPEAN DATA PROTECTION BOARD, *Guidelines 02/2025 on processing of personal data through blockchain technologies*, https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2025/guidelines-022025-processing-personal-data_en.

⁶⁵ Su cui si rimanda a A.M. GAMBINO, C. BOMPRESZI, *Blockchain e criptovalute*, in G. FINOCCHIARO, V. FALCE (a cura di), *Fintech: diritti, concorrenza, regole – Le operazioni di finanziamento tecnologico*, Bologna: Zanichelli, 2019, pp. 267-290.

⁶⁶ C. BOMPRESZI, *Implications of Blockchain-Based Smart Contracts on Contract Law*, Baden Baden: Nomos, 2021, p. 44.

⁶⁷ Opere d'arte digitale pubblicate direttamente su *blockchain*.

qualunque informazione registrata all'interno del *database*, unici, inalterabili, non riproducibili, non falsificabili e irrevocabilmente trasferibili⁶⁸.

A seconda della funzione, i *token* vengono intesi o come mezzo di pagamento (*crypto-currency*), o come mezzo di speculazione finanziaria (*security token*) o come mezzo di accesso a un bene o un diritto (*utility token*). A parità di strumento tecnologico, cioè, si ha una diversa qualificazione giuridica, con esiti divergenti circa le norme di riferimento. Recentemente, a livello europeo, con il Regolamento del Parlamento europeo e del Consiglio relativo ai mercati delle cryptoattività (*Markets in Crypto-Assets* o MiCA)⁶⁹ è stato fornito un quadro normativo d'insieme sulle cryptoattività, definite come «una rappresentazione di un valore o di un diritto che può essere trasferito o memorizzato elettronicamente, utilizzando la tecnologia di registro distribuito o una tecnologia analogica», con esclusione di quelle che rientrano già nella definizione di strumenti finanziari (da assoggettare alla disciplina corrispondente)⁷⁰ e degli NFT⁷¹.

Quest'ultimo acronimo sta per “*Non-Fungible Tokens*”, ovvero *token* che, in ragione dei metadati contenuti, sono tecnologicamente non interscambiabili con altri *token* della stessa tipologia, da cui si differenziano divenendo unici (da qui l'aggettivo “infungibili”)⁷².

Gli *smart contract* permettono la “programmabilità” dei *token*⁷³, potendo automatizzare le operazioni previste dal codice e attinenti al trasferimento, al ricorrere di condizioni stabilite *ex ante*, del *token* medesimo, o all'esercizio di altre azioni connesse al *token*.

L'associazione *smart contract/token* assume rilevanza giuridica laddove il *token*, anche non fungibile, rappresenti beni o diritti di cui disporre mediante *smart contract*. Da questo punto di vista, si può ipotizzare o che lo *smart contract* predetermini le condizioni per il trasferimento del *token* medesimo, o che consenta la

⁶⁸ EUROPEAN UNION BLOCKCHAIN OBSERVATORY AND FORUM, *Regulatory Framework of Blockchains and Smart Contracts*, cit., p. 26.

⁶⁹ Regolamento (UE) 2023/1114 del Parlamento europeo e del Consiglio, del 31 maggio 2023, relativo ai mercati delle cryptoattività e che modifica i regolamenti (UE) n. 1093/2010 e (UE) n. 1095/2010 e le direttive 2013/36/UE e (UE) 2019/1937, GU L 150 del 9.6.2023, pagg. 40–205. Il 13 settembre 2024 è stato pubblicato sulla Gazzetta Ufficiale il decreto legislativo 5 settembre 2024, n. 129, recante “Adeguamento della normativa nazionale al regolamento (UE) 2023/1114 del Parlamento europeo e del Consiglio, del 31 maggio 2023, relativo ai mercati delle cryptoattività” e che modifica i regolamenti (UE) n. 1093/2010 e (UE) n. 1095/2010 e le direttive 2013/36/UE e (UE) 2019/1937”.

⁷⁰ Vedi cons. 9.

⁷¹ Vedi cons. 10.

⁷² Vedi EUROPEAN BLOCKCHAIN OBSERVATORY AND FORUM, *Demystifying Non-Fungible Tokens (NFTs)*, 29 novembre 2021, p. 27, <https://www.eublockchaininfo.rum.eu/reports>.

⁷³ EUROPEAN UNION BLOCKCHAIN OBSERVATORY AND FORUM, *Legal and Regulatory Framework of Blockchains and Smart Contracts*, cit., p. 26. La piattaforma *blockchain* Ethereum è la più utilizzata in ambito NFT con il noto standard ERC-721.

gestione dei diritti connessi al *token*. Ad esempio, nella prima fattispecie potrebbe ricadere il passaggio nella titolarità di un bene (rappresentato digitalmente da un NFT). La seconda potrebbe comprendere il caso di *asset* di tipo finanziario, come azioni, che pagano automaticamente i dividendi⁷⁴.

Lo *smart contract* potrebbe anche presupporre, come spesso accade, un rapporto contrattuale, in base al quale viene effettuato lo scambio di *tokens* o sono definiti i termini dei diritti relativi al *token*. Si pensi ad uno scambio di libri antichi con criptovalute, in cui il trasferimento è un effetto della conclusione dello *smart legal contract* e la controprestazione in criptovalute un obbligo del soggetto ricevente i libri, oppure alla gestione delle *royalties* connesse ad un'opera soggetta al diritto d'autore riprodotta come NFT⁷⁵.

Queste applicazioni si rivelano imprescindibili nel metaverso, in quanto consentono di riproporre, in chiave dematerializzata, le azioni che si effettuerebbero nel mondo fisico nelle interazioni quotidiane ad opera degli utenti, interagenti nel Metaverso sottoforma di *avatars*.

Altresì, la *blockchain* è ampiamente riconosciuta come una tecnologia fondamentale nell'ambito del metaverso, in quanto *database* in cui registrare in modalità sicura, tracciabile, incorruttibile e trasparente le molteplici transazioni che hanno luogo negli ambienti virtuali⁷⁶. Tale convinzione proviene dall'analisi di alcune caratteristiche tecniche della tecnologia in esame⁷⁷.

In primo luogo, il fatto che essa faccia parte dei sistemi distribuiti contribuisce alla ridondanza dei dati; più nel dettaglio, la disattivazione di un nodo della rete per un qualsiasi motivo (come, appunto, un attacco alla cibersicurezza) non causa la perdita dei dati che sono detenuti nelle altre copie identiche della stessa catena in altri nodi. Pertanto, la *blockchain* garantisce la disponibilità dei dati in un qualsiasi momento, con la permanente accessibilità da qualsiasi punto del metaverso e, potenzialmente, anche da mondi virtuali diversi.

Oltre alla distribuzione, il carattere decentralizzato della *blockchain*, che implica l'aggiornamento delle informazioni del *database* a partire da un meccani-

⁷⁴ EUROPEAN UNION BLOCKCHAIN OBSERVATORY AND FORUM, *Legal and Regulatory Framework of Blockchains and Smart Contracts*, cit., p. 26.

⁷⁵ Come indicato da G. FREZZA, *Blockchain, autenticazione e arte contemporanea*, in *Dir. di Famiglia e delle Persone*, vol. 2020 (II), pp. 491-515.

⁷⁶ EU BLOCKCHAIN OBSERVATORY AND FORUM, *Trend Report of Virtual Worlds (Metaverse)*, 24 May 2024, https://blockchain-observatory.ec.europa.eu/publications/trend-report-virtual-worlds-metaverse_en.

⁷⁷ Vedi EU BLOCKCHAIN OBSERVATORY AND FORUM, *Trend Report of Virtual Worlds (Metaverse)*, cit.; K. GOLDSTEIN, *Blockchain and distributed ledger technology: insurance applications, legal development, and cybersecurity considerations*, in *Connecticut Insurance Law Journal*, 2021 (XXVII), pp. 105-122; C. CATALINI, *Blockchain Technology and Cryptocurrencies: Implications for the Digital Economy, Cybersecurity, and Government*, in *Georgetown Journal of International Affairs*, 2018 (XIX) pp. 36-42.

simo del consenso *peer-to-peer*, e non da un punto centrale, diminuisce la vulnerabilità dell'intero impianto a manipolazioni di vario genere. Inoltre, l'immutabilità amplifica le misure di sicurezza. Infatti, l'alterazione dei dati sarebbe possibile solamente modificando in contemporanea l'*hash* del blocco oggetto di attacco, quelli successivi, e tutte le relative copie, prima dell'aggiunta di un nuovo blocco. Questa operazione richiederebbe una potenza e una velocità di calcolo enormi, con costi esorbitanti rispetto all'obiettivo di aprire falle di sicurezza.

La modalità di concatenazione dei blocchi, peraltro, fornisce quella tracciabilità e trasparenza utili a vagliare qualsiasi informazione registrata *on-chain*, dal suo punto di origine alla storia di tutte le transazioni ad essa connesse, aiutando a rilevare eventuali informazioni false o manipolate.

Distribuzione, decentralizzazione, immutabilità, tracciabilità e trasparenza sono qualità preziose in ambiti complessi e variegati come il metaverso, in cui è fondamentale una gestione attenta e oculata di una smisurata quantità di dati continuamente scambiati tra plurimi soggetti, piattaforme, oggetti dell'IoT, *etc.* Non a caso, la *blockchain* si è diffusa principalmente, e sta avendo il maggior successo e riscontro pratico, in settori in cui quotidianamente avviene la condivisione di una molteplicità di dati tra una eterogeneità di attori, e in cui per questo è cruciale mantenere un elevato livello di affidabilità, accortezza, riduzione di errori di duplicazione dei dati e delle tempistiche di condivisione e scambio dei medesimi. In altri termini, uno strumento affidabile, trasparente e tracciabile come la *blockchain* si rivela particolarmente prezioso in una dimensione virtuale in cui gli utenti devono fidarsi che i loro beni virtuali e le operazioni ad essi connessi si trovino in un ambiente sicuro⁷⁸.

7. Blockchain e self-sovereign identity

La presenza umana nell'ambiente digitale espone a significativi rischi per la protezione dell'identità dell'individuo e della sua sfera privata. È sempre più urgente, dunque, intervenire normativamente affinché si possa garantire uno spazio virtuale sicuro, protetto contro i pericoli legati, ad esempio, all'utilizzo illecito a fini di profitto, alla sorveglianza di massa, alla manipolazione, alle discriminazioni, ai furti di identità, cibersicurezza, alla criminalità informatica, *etc.* A questo fine, sul piano europeo e internazionale si sta procedendo verso la creazione di identità digitali uniche e sicure, sotto l'esclusivo controllo degli utenti, come alternativa al sistema attuale in cui sono i fornitori a rendere disponibili

⁷⁸ EU COMMISSION, JOINT RESEARCH CENTRE, *Next Generation Virtual Worlds: Societal, Technological, Economic and Policy Challenges for the EU*, 2023, <https://publications.jrc.ec.europa.eu/repository/handle/JRC133757>.

account e aree riservate per accedere ai propri prodotti e servizi online. Nel metaverso, in particolare, questa esigenza diviene ancora più pressante, dato il maggior grado di esposizione dell'individuo, che arriva ad interagire sotto forma di avatar, e di condivisione dei suoi dati personali.

La creazione di un'identità digitale univoca e sicura si scontra con l'uso di soluzioni nazionali divergenti. Sul piano internazionale, il *Working Group IV* sul Commercio elettronico dell'Uncitral ha elaborato un *Model Law* per il reciproco riconoscimento delle identità e dei servizi fiduciari⁷⁹. A livello europeo, proprio per affrontare adeguatamente le dinamiche dei mercati e gli sviluppi tecnologici, si è ritenuto necessario procedere all'aggiornamento e al perfezionamento del Regolamento eIDAS, in materia di identità e autenticazione digitali, pur mantenendone l'architettura di base. Il nuovo Regolamento eIDAS 2, infatti, specifica il diritto dei cittadini e dei residenti dell'Unione a un'identità digitale che sia sotto il loro controllo esclusivo e che consenta loro di esercitare i propri diritti nell'ambiente digitale e di partecipare all'economia digitale, per rendere effettivo il quale si esplicita la volontà di istituire un quadro armonizzato relativo all'identità digitale (v. cons. 5 e 6).

La *blockchain* è compatibile con questo disegno normativo. Sono state già citate⁸⁰, in questo senso, la Dichiarazione istitutiva della Blockchain Partnership Europea e la Risoluzione del Parlamento europeo del 3 ottobre 2018, che hanno posto in luce l'opportunità data dalla *blockchain* di superare i vecchi schemi incentrati sul controllo esterno delle identità in favore di un controllo diretto da parte degli interessati. Nel Report "*Blockchain and digital identity*" dello European Blockchain Observatory and Forum⁸¹, la *blockchain* viene ritenuta un efficace strumento di sviluppo di identità digitali *self-sovereign*.

Il Regolamento eIDAS 2, non a caso, disciplina due nuovi strumenti che, pur non facendo diretto riferimento a una specifica tecnologia, potrebbero facilmente basarsi sulla tecnologia *blockchain*. Il primo è il registro elettronico, di cui si è detto *supra*⁸². Il secondo è il portafoglio europeo di identità digitale, definito come «un mezzo di identificazione elettronica che consente all'utente di conservare, gestire e convalidare in modo sicuro dati di identità personale e attestati elettronici di attributi al fine di fornirli alle parti facenti affidamento sulla certificazione e agli altri utenti dei portafogli europei di identità digitale, e di firmare mediante firme elettroniche qualificate o apporre sigilli mediante sigilli

⁷⁹ *Model Law on the Use and Cross-border Recognition on Identity Management and Trust Services*, <https://uncitral.un.org/en/mlit>.

⁸⁰ Vedi *supra*, par. 6.

⁸¹ www.eublockchainforum.eu/sites/default/files/report_identity_v0.9.4.pdf.

⁸² Vedi *supra*, par. 5.

elettronici qualificati» (art. 3, n. 42). La peculiarità del portafoglio europeo è la divulgazione selettiva dei dati personali da parte dell'utente e sotto il proprio esclusivo controllo (v. cons. 15).

La conformità delle soluzioni *blockchain-based* con il nuovo Regolamento eIDAS consentirebbero di realizzare gli obiettivi europei legati all'identità digitale. A riprova di ciò, la Commissione europea, nel delineare la propria Blockchain Strategy, ha riconosciuto il potenziale della *blockchain* di rivoluzionare il modo in cui si condividono le informazioni e si effettuano transazioni online, potendo migliorare il quadro europeo di identità digitale in evoluzione; conseguentemente, la Commissione ha inserito tra i “*gold standard*” per la *blockchain* l'identità digitale, che include la compatibilità della *blockchain* con le normative sulla firma elettronica, come eIDAS, e supporta un *framework* di identità ragionevole, pragmatico, decentralizzato e auto-sovrano.⁸³

⁸³ <https://digital-strategy.ec.europa.eu/it/policies/blockchain-strategy>.

PARTE III – SISTEMI E PRODOTTI

LA PROTEZIONE DEI BENI INFORMATICI ATTRAVERSO IL DIRITTO D'AUTORE

Claudio Di Cocco

SOMMARIO: 1. Diritto d'autore e mercato unico digitale. 2. Il regime di protezione dell'opera dell'ingegno. 3. Diritti patrimoniali, diritti connessi e nuove prerogative relative all'utilizzo di opere on-line. 4. Il diritto morale dell'autore. 5. Eccezioni e limitazioni al diritto d'autore. 6. Le misure tecnologiche di protezione e le informazioni elettroniche sul regime dei diritti. 7. I beni informatici: programmi per elaboratore e banche di dati elettroniche. 7.1. Il regime di protezione dei programmi per elaboratore. 7.2. La tutela delle banche di dati. 7.3. Il diritto del costituente di una banca di dati.

1. Diritto d'autore e mercato unico digitale

Tra gli istituti su cui la rivoluzione digitale ha avuto un impatto significativo rientra certamente il diritto d'autore: tale circostanza è testimoniata dall'attenzione che il legislatore ha dedicato alla relativa disciplina negli ultimi tre decenni, con interventi di significativa portata.

L'esigenza di rivedere la disciplina a tutela del diritto d'autore è stata imposta, in particolare, dallo sviluppo delle moderne tecnologie informatiche e telematiche, quali *in primis* la rete Internet: una realtà, quella digitale, che ha affrancato l'opera dell'ingegno dalla necessità di una sua fissazione su supporto materiale, fino ad un recente passato indispensabile per la circolazione dell'opera stessa.

La rivoluzione informatica non ha solo mutato il contesto di riferimento relativamente alla protezione delle opere dell'ingegno tradizionali, ma ha altresì portato alla nascita dei cc.dd. beni informatici (programmi per elaboratore, banche di dati elettroniche) che, per le loro peculiari caratteristiche, hanno richiesto l'introduzione di una disciplina di tutela *ad hoc*.

Di seguito si andrà a delineare sinteticamente il contenuto della disciplina del diritto d'autore, così come si presenta oggi nel nostro ordinamento nazionale, alla luce delle convenzioni internazionali e dei provvedimenti dell'Unione europea (UE) sul tema, tra cui da ultimo la direttiva (UE) 2019/790 sul diritto

d'autore e sui diritti connessi nel mercato unico digitale¹. Ci si soffermerà poi sul regime di protezione dedicato ai suddetti beni informatici.

A fianco dell'analisi delle principali disposizioni normative, si darà conto dell'attività interpretativa e di indirizzo (sempre più rilevante) della Corte di giustizia dell'UE in materia.

2. Il regime di protezione dell'opera dell'ingegno

I cc.dd. beni immateriali consistono in un'idea intesa come risultato di un processo creativo (c.d. *corpus mysticum*) che si estrinseca in un elemento materiale (c.d. *corpus mechanicum*) e sono oggetto di diritti assoluti. Nella categoria a numero chiuso dei beni immateriali rientrano (oltre ai segni distintivi dell'impresa, le invenzioni industriali, i modelli di utilità, ecc.) quelle creazioni intellettuali definite quali «opere dell'ingegno».

A queste ultime il Codice civile italiano dedica il Capo I, Titolo IX, Libro V, «Del diritto d'autore sulle opere dell'ingegno letterarie ed artistiche»: gli artt. 2575-2583 c.c. contengono l'enunciazione dei principi generali in materia, rinviando alle leggi speciali per le disposizioni di dettaglio. Proprio alla legislazione speciale si deve guardare per ricostruire la disciplina giuridica nazionale del diritto d'autore e, in particolare, alla L. 22 aprile 1941, n. 633 (G.U. 16 luglio 1941, n. 166) di «protezione del diritto d'autore e di altri diritti connessi al suo esercizio» (di seguito «l.d.a.»), come successivamente più volte integrata e modificata.

Tale testo normativo si articola in oltre 200 disposizioni, dedicate alle regole applicabili a qualsiasi creazione intellettuale (letteraria, musicale, ecc.) e a disciplinare nel dettaglio alcune specifiche categorie di opere². Nel proseguo si analizzeranno le disposizioni principali applicabili in via generale, richiamando quelle dedicate a singole opere unicamente laddove di specifico interesse per la presente trattazione.

L'art. 1 l.d.a. definisce l'oggetto della disciplina, stabilendo oggi: «Sono protette ai sensi di questa legge le opere dell'ingegno umano di carattere creativo che appartengono alla letteratura, alla musica, alle arti figurative, all'architettura, al teatro ed alla cinematografia, qualunque ne sia il modo o la forma di espressione, anche laddove create con l'ausilio di strumenti di intelligenza artificiale,

¹ La normativa dedicata al diritto d'autore in ambito italiano, infatti, deriva oggi in buona parte da una pluralità di fonti sovranazionali (Convenzione di Berna; *Universal Copyright Convention*; *Trade-related Aspects of Intellectual Property Rights*-TRIPs; *WIPO Copyright Treaty*-WCT e *WIPO Performances and Phonograms Treaty*-WPPT), così come da una intesa produzione di provvedimenti sul tema del legislatore eurocomunitario, di cui in parte si dirà.

² Per l'ambito di applicazione della l.d.a., si vedano gli artt. 185 ss. l.d.a.

purché costituenti risultato del lavoro intellettuale dell'autore»³. Si noti come il concetto di «opera dell'ingegno» non sia definito espressamente dalla l.d.a. Per «opera dell'ingegno» si può intendere «ogni risultato raggiunto mediante il prevalente impiego delle facoltà della mente umana, ogni frutto di attività psichica, che vi prevalga la psicologia della conoscenza ovvero quella del sentimento»⁴.

Ai sensi del successivo art. 2 l.d.a., appartengono ai suddetti generi una serie di opere, fra le quali: le opere letterarie, drammatiche, scientifiche, didattiche, religiose; le opere e le composizioni musicali, le opere drammatico-musicali; le opere coreografiche e pantomimiche; le opere della scultura, della pittura, del disegno, dell'incisione e delle arti figurative similari, compresa la scenografia; i disegni e le opere dell'architettura; le opere dell'arte cinematografica, muta o sonora; le opere fotografiche; i programmi per elaboratore; le banche di dati; le opere del disegno industriale.

Va segnalato come la giurisprudenza e la dottrina maggioritarie non ritengano l'elencazione ora ricordata di natura tassativa: di conseguenza, un'eventuale opera che non sia compresa in questo elenco non potrà ritenersi a priori esclusa dalla tutela. Proprio per questo motivo, le norme sulle opere dell'ingegno in passato sono state ritenute idonee, ad esempio, a proteggere anche i programmi per elaboratore e le banche di dati, prima della loro espressa considerazione all'interno della l.d.a.

Oltre alle opere create dal nulla (espressione della massima creatività e originalità dell'autore), la normativa protegge anche le opere cc.dd. derivate (art. 4 l.d.a.). L'opera derivata è caratterizzata da un contenuto parzialmente non originale: ai fini della sua tutela come opera dell'ingegno, al contenuto preesistente deve essere affiancata una porzione originale, seppure minima, ovvero il contenuto nel suo complesso deve essere strutturato in modo originale. Nelle opere derivate il carattere creativo è legato all'elaborazione successiva di un'opera preesistente, che può ad esempio consistere: nella trasformazione dell'opera originaria in altra forma letteraria o artistica, nella traduzione in altra lingua, nelle modifiche e aggiunte che determinano un rifacimento sostanziale dell'opera originaria, nell'adattamento, nella riduzione, nella trasformazione in compendi dell'opera originaria.

Affinché la creazione intellettuale sia riconosciuta e tutelata dal diritto d'au-

³ I riferimenti espressi all'ingegno «umano» e alla necessità che, «anche laddove create con l'ausilio di strumenti di intelligenza artificiale», le opere debbano comunque costituire il «risultato del lavoro intellettuale dell'autore» per essere oggetto di protezione attraverso il diritto d'autore, sono stati introdotti dalla L. 23 settembre 2025, n. 132, «Disposizioni e deleghe al Governo in materia di intelligenza artificiale» (G.U. del 25 settembre 2025, n. 223).

⁴ P. GRECO, P. VERCELLONE, *I diritti sulle opere dell'ingegno*, in *Trattato di diritto civile italiano*, diretto da F. VASSALLI, vol. 11, 3, Torino: Utet, 1974, pp. 35-36.

tore è necessaria la sua estrinsecazione nel mondo materiale, cioè che si concretizzi in una “realizzazione esterna”: finché rimane idea astratta, «rappresentazione intellettuale interna» (Cass., 1° febbraio 1962, n. 190), essa non rileva quale opera dell’ingegno e non sarà protetta come bene giuridico.

La forma e il modo di esteriorizzazione della creazione possono essere i più diversi: l’art. 2575 c.c. e l’art. 1 l.d.a., infatti, stabiliscono che le opere dell’ingegno sono tutelate «qualunque ne sia il modo o la forma di espressione», eventualmente anche prescindendo dalla fissazione su un supporto materiale (c.d. opera orale).

Non qualunque espressione intellettuale è ritenuta meritevole di tutela come opera dell’ingegno, bensì solo quella dotata di carattere creativo. Tale attributo non riguarda le idee o le nozioni alla base dell’opera, ma deve investire la forma espressiva dell’opera stessa, cioè la specifica modalità di estrinsecazione di dette idee e nozioni scelta dall’autore. Il concetto giuridico di creatività, così come adottato in ambito di opere d’ingegno, non coincide con quelli estetici o etici di creazione, originalità e novità assoluta, essendo sufficiente che sussista un’individuale e personale espressione dell’idea da parte dell’autore dell’opera. Tuttavia, risulta controverso se il requisito dell’originalità dell’opera, cioè la possibilità di riconoscervi l’impronta della personalità del suo autore, sia sufficiente per accedere alla protezione o se, viceversa, sia necessario anche il carattere della novità dell’opera. In merito, larga parte della giurisprudenza e della dottrina nazionali ritengono che l’opera debba presentarsi anche oggettivamente nuova, risultando così possibile escludere dalla tutela le opere eventualmente identiche (per plagio o per mero incontro fortuito) successivamente realizzate.

Come ricordato, ciò non significa che un’opera derivata da una creazione precedente non sia tutelabile, bensì che per esserlo dovrà anch’essa possedere un grado, seppure minimo, di originalità distintiva.

Pertanto, l’elemento che accomuna tutte le opere dell’ingegno è che esse sono il risultato dell’attività creativa del relativo autore. La creazione dell’opera dell’ingegno, dotata del requisito dell’originalità, è atto necessario e sufficiente affinché l’opera dell’ingegno goda della relativa tutela e siano conseguentemente riconosciuti al suo autore i corrispondenti diritti; ciò in quanto «formano oggetto di diritto di autore le opere dell’ingegno di carattere creativo» (art. 2575 c.c.) e «il titolo originario dell’acquisto del diritto di autore è costituito dalla creazione dell’opera, quale particolare espressione del lavoro intellettuale» (art. 2576 c.c. e art. 6 l.d.a.).

Il contenuto del diritto d’autore, di cui l’autore diviene titolare in seguito alla creazione di un’opera originale, ha una duplice natura: di tipo morale (diritti morali) e di tipo patrimoniale (diritti patrimoniali o diritti di utilizzazione eco-

nomica), di cui si dirà fra breve. Questi diritti insistono sull'opera dell'ingegno intesa nella sua forma espressiva o rappresentativa (sia c.d. 'esterna', ciò che dell'opera è immediatamente percepibile ai sensi, ad esempio la concatenazione delle parole in un racconto; sia c.d. 'interna', cioè come l'autore ha sviluppato e intrecciato i contenuti e le idee nell'opera, ad esempio la trama di un racconto) e non invece sul suo contenuto ideologico (concetti, idee, informazioni, conoscenze, ecc.), che resta escluso dalla tutela e, pertanto, liberamente utilizzabile.

Il principio da ultimo enunciato è di fondamentale importanza e consente di comprendere come la tutela garantita dal diritto d'autore non rappresenti necessariamente, di per sé, un ostacolo alla circolazione della conoscenza, almeno in linea teorica e purché sia effettivamente possibile accedere adeguatamente al contenuto ideologico dell'opera protetta.

L'opera dell'ingegno appartiene al genere dei beni immateriali, ossia di quei beni suscettibili di formare oggetto di facoltà esclusive, a prescindere dall'eventuale incorporazione in un supporto materiale. Occorre, dunque, distinguere l'opera dell'ingegno (bene immateriale) dal supporto che eventualmente la incorpora (bene materiale). Si pensi, ad esempio, all'archetipo delle opere dell'ingegno, l'opera letteraria: un libro, quale bene materiale, è formato da carta, inchiostro e rilegatura, ma nello stesso tempo incorpora l'opera letteraria protetta (bene immateriale), rappresentata dalla forma espressiva di quest'ultima, cioè dalla specifica concatenazione di parole scelta dall'autore per esprimere in modo originale le sue idee (idee che restano escluse dalla protezione).

Per l'ordinamento italiano, come già riferito, l'autore è necessariamente una persona fisica⁵. In alcuni casi, il diritto d'autore (in particolare, le prerogative di natura economica) è però attribuito a particolari persone giuridiche (art. 11 l.d.a.): alle amministrazioni dello Stato, alle province ed ai comuni, laddove le opere siano create e pubblicate sotto il loro nome ed a loro conto e spese. Agli enti citati si affiancano, per comune interpretazione, le regioni, non nominate nel testo normativo in quanto la loro costituzione è stata successiva all'emanazione della stessa l.d.a. Il medesimo diritto spetta agli enti privati che non perseguano scopo di lucro, salvo diverso accordo con gli autori, nonché alle accademie e agli altri enti pubblici culturali limitatamente alla raccolta dei loro atti e sulle loro pubblicazioni.

Una persona giuridica, inoltre, potrà risultare titolare dei diritti patrimoniali sull'opera in altre specifiche ipotesi, nelle quali il legislatore ha voluto proteggere l'investimento economico di alcuni soggetti che operano nella c.d. impresa

⁵ Tale circostanza, di cui già in passato non si è mai dubitato in dottrina e in giurisprudenza, ha trovato oggi espresso riconoscimento all'art. 1 l.d.a., grazie alla novella introdotta dal D.Lgs. 132/2025 in materia di intelligenza artificiale, di cui si è detto alla precedente nota 3.

culturale. Così, i diritti di utilizzazione economica sui programmi per elaboratore, sulle banche di dati e sulle opere del disegno industriale creati dal lavoratore dipendente (e, per interpretazione costante, dall'appaltatore) in esecuzione delle sue mansioni o su istruzioni impartite dal datore di lavoro, sulle riviste o giornali, nonché sulle opere cinematografiche, spettano rispettivamente al datore di lavoro (art. 12-*bis* l.d.a., art. 12-*ter* l.d.a.), all'editore (art. 38 l.d.a.) e al produttore (art. 45 l.d.a.), che spesso possono essere, appunto, persone giuridiche.

Sotto il profilo soggettivo, la titolarità dei diritti sull'opera potrà appartenere ad uno o più soggetti, a seconda delle dinamiche creative e del risultato di queste.

Un'opera dell'ingegno può risultare quale frutto dell'attività creativa di un unico soggetto, a cui competerà pertanto il titolo di autore dell'opera (opera monosoggettiva) in esclusiva.

Un'opera d'ingegno può, altresì, essere il frutto dell'apporto intellettuale originale di più soggetti (opera plurisoggettiva), definendosi «in comunione» o «collettiva» a seconda delle dinamiche sottese alla sua realizzazione e degli esiti di essa.

L'attività creativa posta in essere da diversi autori darà origine a un'opera in comunione qualora i singoli contributi che la compongono risultino inscindibili e indistinguibili nell'opera finale (art. 10 l.d.a.) (ad esempio, un'opera letteraria scritta da due o più autori).

Qui la particolare espressione del lavoro intellettuale originale è rappresentata da un tutto organico, in cui non è possibile scindere ed identificare il contributo dell'uno e dell'altro dei coautori. L'indivisibilità degli apporti creativi reca con sé l'impossibilità di un utilizzo separato del singolo contributo, in quanto i diversi apporti sono destinati a fondersi nell'opera finale, la quale, per la sua stessa esistenza, necessita di tutti i contributi.

Nell'opera in comunione il diritto d'autore appartiene a tutti i coautori secondo parti che si presumono uguali, salvo l'esistenza di una prova scritta in merito a un diverso accordo.

A questa categoria di opere sono applicabili le norme generali sulla comunione, mentre le azioni di difesa del diritto morale sull'opera sono esercitabili individualmente da ciascun coautore. In deroga alle disposizioni generali in materia di comunione, sono previste alcune ipotesi nelle quali è necessario il consenso di tutti i coautori (cfr. art. 10, comma 3, l.d.a.).

Viceversa, l'attività prestata dai singoli autori può diversificarsi a seconda delle singole porzioni realizzate rispetto al progetto finale o al ruolo assunto nella fase di direzione e organizzazione del lavoro creativo, dando origine a un'opera collettiva. In questo caso, i vari contributi hanno e conservano il loro carattere di creazioni autonome anche nell'opera finale: questa risulterà però il

frutto dell'attività del soggetto che ne abbia curato la scelta, il coordinamento e la riunione. È così considerato autore dell'opera collettiva chi ne organizza e dirige la creazione (art. 7, comma 1, l.d.a.). Costituite dalla riunione di opere o di parti di opere, le opere collettive hanno pertanto carattere di creazioni autonome come risultato della scelta e del coordinamento delle porzioni di opere preesistenti a un determinato fine letterario, scientifico, didattico, religioso, politico o artistico. Esse godono della protezione prevista per le opere originali, indipendentemente dai diritti d'autore sulle opere o sulle parti di opere di cui sono composte (art. 3 l.d.a.), che restano impregiudicati. Il coordinatore vanta il diritto d'autore relativamente alla realizzazione di tale attività organizzatrice, mentre i creatori dei singoli contributi (che restano riconoscibili nell'opera finale) conservano i propri diritti sugli stessi: si pensi, ancora una volta, ad un'opera letteraria alla cui stesura partecipino più soggetti, dove alcuni di essi redigono separate e riconoscibili porzioni del testo, mentre un ulteriore soggetto ne coordina l'attività.

In questi casi, la creazione dell'opera è di nuovo sufficiente ad attribuire al suo autore il diritto d'autore a titolo originario, autore la cui esatta identificazione è questione di estremo rilievo anche sul piano pratico: il diritto d'autore non si può acquistare da altri che dal reale titolare di tale prerogativa, dunque *in primis* dall'autore, il che significa che l'atto di trasferimento del diritto da parte di un soggetto non legittimato a disporne risulterà giuridicamente nullo. In merito, si noti come, per espressa previsione dell'art. 8 l.d.a., in via generale sarà reputato autore dell'opera, salva la possibilità di darne prova contraria, chi è in essa indicato come tale nelle forme d'uso (ad esempio, sarà considerato autore di un'opera letteraria a stampa, sino a prova contraria, il soggetto indicato nella sua copertina).

3. Diritti patrimoniali, diritti connessi e nuove prerogative relative all'utilizzo di opere on-line

I diritti di utilizzazione economica riconosciuti all'autore di un'opera dell'ingegno si articolano in una serie di privative che hanno in comune i caratteri della esclusività, in quanto spettanti solo all'autore, e della reciproca autonomia.

L'esclusiva patrimoniale dell'autore, nel suo complesso, si risolve in un diritto di ampia portata che gli consente di trarre dall'opera ogni possibile utilità economica: l'autore, infatti, gode del diritto esclusivo «di utilizzare economicamente l'opera in ogni forma e modo, originale o derivato» (art. 12, comma 2, l.d.a.) nei limiti fissati dalla stessa l.d.a.

L'eventuale cessione di una delle privative economiche dell'autore non implica l'automatica cessione di un'altra: «I diritti esclusivi [...] sono fra loro indi-

pendenti. L'esercizio di uno di essi non esclude l'esercizio esclusivo di ciascuno degli altri diritti» (art. 19 l.d.a.).

L'autonomia dei diritti patrimoniali dell'autore si traduce in una potenziale complessità nella gestione delle relazioni che investono l'opera tutelata e, dal punto di vista pratico, consigliano l'adozione di dettagliate disposizioni contrattuali sulla eventuale cessione o concessione di diritti di utilizzazione economica. In base al citato principio, infatti, resterà nella esclusiva disponibilità dell'autore qualunque forma di utilizzo dell'opera che non sia stata espressamente oggetto di pattuizione.

Una serie di facoltà di utilizzazione economica, come detto esclusive ed autonome fra loro, in cui si articola il diritto patrimoniale d'autore sono espressamente indicate (in via non tassativa) negli artt. da 12 a 18-*bis* l.d.a.

Proprio su queste ultime è intervenuta in modo significativo la direttiva europea 2001/29/CE (G.U.C.E. del 22 giugno 2001, n. L 167/10), avente ad oggetto il diritto d'autore e i diritti connessi nella società dell'informazione (la cui attuazione in Italia è avvenuta con l'emanazione del D.Lgs. 68/2003, G.U. del 11 luglio 2003, n. 159), con l'intento di adeguare l'istituto all'inedito contesto digitale.

Esse consistono oggi:

- nel diritto di pubblicazione (art. 12 l.d.a.);
- nel diritto di riproduzione (art. 13 l.d.a.), cioè la moltiplicazione in copie diretta o indiretta, temporanea o permanente, in tutto o in parte dell'opera, in qualunque modo o forma. Si noti come, salvo quanto disposto in ordine alla responsabilità dei prestatori intermediari⁶, sono tuttavia esentati dal diritto di riproduzione gli atti di riproduzione temporanea privi di rilievo economico proprio che sono transitori o accessori e parte integrante ed essenziale di un procedimento tecnologico, purché eseguiti all'unico scopo di consentire: a) la trasmissione in rete tra terzi con l'intervento di un intermediario, o b) un utilizzo legittimo di un'opera o di altri materiali (art. 68-*bis* l.d.a.). Gli atti di riproduzione in questione, affinché non operi il diritto di privativa, non debbono perciò avere un proprio valore economico e includono gli atti che facilitano la navigazione in rete e la realizzazione di copie *cache*, nonché l'effettivo funzionamento dei sistemi di trasmissione;
- nel diritto di trascrivere (art. 14 l.d.a.), che ha per oggetto l'uso dei mezzi atti a trasformare l'opera orale in opera scritta o riprodurla con uno dei mezzi indicati nel punto precedente;
- nel diritto di rappresentazione, recitazione ed esecuzione in pubblico, co-

⁶ Cfr. artt. 4 ss. del Regolamento (UE) 2022/2065.

munque effettuate, gratuitamente o a pagamento (art. 15 l.d.a.);

– nel diritto di comunicazione al pubblico (art. 16 l.d.a.) su filo o senza filo dell'opera attraverso l'impiego di uno dei mezzi di diffusione a distanza (quali la radio, la televisione ed altri mezzi analoghi) e comprende la comunicazione al pubblico via satellite, la ritrasmissione, nonché le comunicazioni al pubblico codificate con condizioni particolari di accesso. Comprende, altresì, la messa a disposizione del pubblico dell'opera in maniera che ciascuno possa avervi accesso dal luogo e nel momento scelti individualmente (facoltà, questa, che include la tipica modalità con la quale un'opera viene messa a disposizione attraverso la rete Internet: il c.d. *upload*)⁷. Tale diritto non si “esaurisce” con alcun atto di comunicazione al pubblico, ivi compresi gli atti di messa a disposizione del pubblico (cioè non trova applicazione il «principio dell'esaurimento», di cui a seguire si dirà);

– nel diritto di distribuzione (art. 17 l.d.a.), cioè il diritto di mettere in commercio o in circolazione, o comunque a disposizione del pubblico, con qualsiasi mezzo ed a qualsiasi titolo, l'originale dell'opera o gli esemplari di essa (cioè delle copie).

Il diritto di distribuzione dell'originale o di copie dell'opera è, in via generale, soggetto al «principio dell'esaurimento». All'autore spetta il diritto esclusivo di fissare l'opera e di riprodurla in copie e la facoltà in parola gli consente di mettere sul mercato, o comunque in circolazione, l'opera o le copie fisiche di essa: nel caso in cui la prima vendita o il primo atto di trasferimento della proprietà di un supporto incorporante l'opera nell'UE sia effettuato dal titolare del diritto o con il suo consenso, il diritto di distribuzione viene meno, “si esaurisce” appunto, consentendo a chiunque il successivo acquisto e la rivendita di tale supporto incorporante l'opera protetta.

Il principio dell'esaurimento non si applica, viceversa, alla messa a disposizione del pubblico di opere in modo che ciascuno possa avervi accesso dal luogo e nel momento scelti individualmente (cioè tipicamente via Internet), anche nel caso in cui sia consentita la realizzazione di copie dell'opera (c.d. *download*)⁸;

⁷ Sul tema della creazione di collegamenti ipertestuali (i cc.dd. *links*) ad opere dell'ingegno protette disponibili sul *web* e la loro potenziale interferenza con le prerogative riservate agli autori/titolari dei diritti, in particolare con il diritto di messa a disposizione del pubblico, si veda la sentenza della Corte di giustizia dell'Unione europea, 13 febbraio 2014, Causa C-466/12, *Nils Svensson/Sten Sjögren/Madelaine Sablman/Pia Gadd c. Retriever Sverige AB*. In tale caso, la Corte ha ritenuto la realizzazione di un *link* costituire un atto di comunicazione al pubblico: tuttavia, laddove il «pubblico» in questione non risulti «nuovo», secondo la Corte tale atto di comunicazione non richiede un'autorizzazione da parte del titolare del diritto di comunicazione al pubblico.

⁸ Sul punto, si veda nel proseguo quanto da ultimo statuito dalla Corte di giustizia dell'UE.

- nel diritto di traduzione di un'opera (art. 18 l.d.a.), avente per oggetto qualsiasi forma di modificazione, di elaborazione e di trasformazione dell'opera;
- nel diritto di elaborazione (artt. 4 e 18 l.d.a.), cioè di procedere alla trasformazione dell'opera in un'altra forma letteraria o artistica, ovvero a rifacimenti sostanziali, compendi, variazioni musicali, ecc.;
- nel diritto di concedere in noleggio o in prestito l'opera, che consiste nel cedere in uso per un periodo di tempo limitato il supporto in cui l'opera è incorporata, sia che si tratti di originale, sia che si tratti di copia, nel primo caso con lo scopo di ottenere un beneficio economico o commerciale, nel secondo senza tale scopo (art. 18-*bis* l.d.a.).

Tutti i diritti esclusivi facenti capo all'autore hanno per oggetto l'opera nel suo insieme e in ciascuna delle sue parti (art. 19, comma 2, l.d.a.). Pertanto, salvi i casi di c.d. libera utilizzazione (illustrati nel successivo § 5), anche l'uso di una singola porzione di un'opera dell'ingegno deve essere autorizzata dall'autore.

In merito alla durata dei diritti patrimoniali, in generale questi sussisteranno per tutta la vita dell'autore e sino al termine del settantesimo anno solare dopo la sua morte. Si tenga conto che la suddetta durata è soggetta a termini di decorrenza diversi a seconda del tipo di opera e a diverse eccezioni.

I diritti di utilizzazione spettanti agli autori delle opere dell'ingegno (nonché i diritti connessi aventi carattere patrimoniale, di cui si dirà fra breve) possono essere acquistati, alienati o trasmessi in tutti i modi e forme consentiti dalla legge, salva l'applicazione delle norme speciali indicate dalla l.d.a., e possono trasferirsi sia per atto tra vivi, sia *mortis causa*.

L'eventuale cessione di uno o più esemplari dell'opera non comporta, salvo patto contrario o in specifiche ipotesi previste nella l.d.a. (cfr. artt. 89 e 109 l.d.a.), la trasmissione dei diritti di utilizzazione spettanti agli autori dell'opera stessa o ai titolari di diritti connessi.

Sotto il profilo probatorio, la normativa impone che la trasmissione dei diritti di utilizzazione economica debba essere provata per iscritto (art. 110 l.d.a.). Pertanto, il trasferimento della privativa potrà avvenire anche con atto avente forma orale, ma in caso di contestazione sarà l'avente causa (colui che afferma di aver acquisito la relativa privativa) a doverne provare l'avvenuto trasferimento e tale prova potrà essere data solo con atto avente forma scritta.

Accanto ai diritti di utilizzazione economica spettanti all'autore, su alcuni generi di opere la legge riconosce un'ulteriore serie di facoltà aventi un contenuto patrimoniale: i diritti connessi. Questi, contrariamente al diritto d'autore, non spettano al creatore dell'opera dell'ingegno, bensì ad altri soggetti della c.d. impresa culturale (artisti, esecutori, interpreti, fotografi, produttori, ecc.).

I diritti connessi sono estremamente eterogenei e sono costituiti da priva-

tive che, pur avendo ciascuna una diversa natura e un diverso contenuto (oltre che durata), sono accomunate dal fatto di presentare una connessione, diretta o indiretta, con l'esercizio o con l'oggetto del diritto d'autore: sono diritti distinti e diversi dal diritto d'autore, ma ad esso variamente collegati e la cui tutela trova fondamento non in un'attività creativa, bensì in interessi di natura più strettamente economica.

Senza entrare nel merito dell'articolata disciplina di questi diritti, obiettivo che esula dalla presente trattazione e per il quale si rimanda alla dottrina sull'argomento, basti ricordare come ne possano godere gli artisti interpreti ed esecutori (potenziali titolari anche di un diritto di natura morale), i produttori fonografici, il produttore cinematografico, le emittenti radiotelevisive, i realizzatori di edizioni critiche e scientifiche, l'autore di bozzetti teatrali che non costituiscano opere dell'ingegno, il progettista di lavori dell'ingegneria, il fotografo e (secondo i più) il costituente di una banca di dati.

Fra questi diritti, merita qui menzionare il diritto connesso, recentemente introdotto dal D.Lgs. 8 novembre 2021 n. 177 (*G.U.* del 27 novembre 2021, n. 283) di recepimento della direttiva (UE) 2019/790⁹, relativo all'uso di pubblicazioni di carattere giornalistico on-line.

Il nuovo art. 43-*bis* l.d.a. prevede che agli editori di pubblicazioni di carattere giornalistico (di cui viene fornita la definizione al comma 2), per l'utilizzo on-line di queste opere da parte dei prestatori di servizi della società dell'informazione (tra cui, ad esempio, i provider di *news* on-line, gli aggregatori di notizie on-line o i realizzatori di rassegne stampa on-line), siano riconosciuti i diritti esclusivi di riproduzione e comunicazione di cui agli artt. 13 e 16 l.d.a. e, dunque, un equo compenso per tale utilizzo. Agli autori degli articoli giornalistici, gli editori dovranno poi riconoscere una quota tra il 2 e il 5 per cento dell'equo compenso ricevuto. La durata dei diritti in parola è fissata in due anni dalla pubblicazione dell'opera di carattere giornalistico, mentre non sono riconosciuti in caso di utilizzi privati o non commerciali da parte di singoli utilizzatori, né in caso della realizzazione di semplici collegamenti ipertestuali (cc.dd. *links*) o laddove l'utilizzo riguardi «singole parole» o «estratti molto brevi» (cc.dd. *snippets*) della pubblicazione

⁹ Direttiva (UE) 2019/790 del 17 aprile 2019 sul diritto d'autore e sui diritti connessi nel mercato unico digitale e che modifica le direttive 96/9/CE e 2001/29/CE (*G.U.C.E.* 17 maggio 2019, n. L 130). L'obiettivo del nuovo provvedimento europeo è stato quello di adeguare l'istituto alla rapida evoluzione del contesto tecnologico e all'affermarsi di un mercato unico digitale, nonché, nel contempo, di riequilibrare i rapporti (in particolare, economici) fra gli autori, gli operatori dell'industria culturale e i nuovi protagonisti dello scenario: i provider di servizi della società dell'informazione. Nel ribadire la validità dei principi stabiliti dal quadro giuridico dell'Unione sul diritto d'autore, la direttiva interviene su diversi profili, alcuni dei quali nel proseguo saranno illustrati in quanto qui di specifico interesse.

giornalistica (dove per «estratto molto breve» si deve intendere «qualsiasi porzione di tale pubblicazione che non dispensi dalla necessità di consultazione dell'articolo giornalistico nella sua integrità», art. 43-*bis*, comma 7, l.d.a.).

L'uso on-line di opere protette viene poi fatto oggetto di ulteriori disposizioni di particolare interesse, in quanto riguardanti il «prestatore di servizi di condivisione di contenuti online» (PSCC) (artt. 102-*sexies*-102-*decies* l.d.a., anch'essi introdotti dal D.Lgs. 177/2021). Questo è un prestatore di servizi della società dell'informazione che presenta tutti i seguenti requisiti:

- a) ha come scopo principale, o tra i principali scopi, di memorizzare e dare accesso al pubblico a grandi quantità di opere o di altri materiali protetti dal diritto d'autore;
- b) le opere o gli altri materiali protetti sono caricati dai suoi utenti;
- c) le opere o gli altri materiali protetti sono organizzati e promossi allo scopo di trarne profitto direttamente o indirettamente.

Si tratta oggi di una vasta ed importante categoria di prestatori di servizi della società dell'informazione, tra cui rientrano *in primis* i cc.dd. *social networks* (Facebook, Instagram, YouTube, TikTok, ecc.). Per questi PSCC viene stabilito che, quando concedono l'accesso al pubblico a opere protette caricate dai loro utenti, effettuano un atto di comunicazione al pubblico o un atto di messa a disposizione del pubblico ai sensi della l.d.a.: pertanto, gli PSCC devono ottenere preventivamente un'autorizzazione dai titolari dei diritti su tali opere, che includa anche gli atti compiuti dagli utenti che caricano sulla piattaforma del PSCC le opere protette (quando detti utenti non agiscono per scopi commerciali o la loro attività non genera ricavi significativi). In aggiunta, nello svolgere tale attività, al PSCC non si applicherà la limitazione di responsabilità per l'attività di *hosting provider* prevista in via generale dall'art. 6 del Regolamento (UE) 2022/2065. Qualora non sia concessa alcuna autorizzazione per l'uso dell'opera protetta utilizzata dal proprio utente, i PSCC, pur non essendo previsto a loro carico un obbligo generale di sorveglianza sull'attività dei propri utenti, saranno responsabili della violazione del diritto d'autore, a meno che non siano in grado di dimostrare di

- aver compiuto i massimi sforzi per ottenere un'autorizzazione, e
- aver compiuto i massimi sforzi per assicurare che non siano disponibili opere per i quali abbiano ricevuto le informazioni pertinenti e necessarie dai titolari dei diritti; e in ogni caso,
- aver agito tempestivamente, dopo aver ricevuto una segnalazione sufficientemente motivata dai titolari dei diritti, per disabilitare l'accesso o rimuovere dai loro siti web le opere oggetto di segnalazione e aver compiuto i massimi sforzi per impedirne il caricamento in futuro.

L'applicazione del suddetto regime di responsabilità (responsabilità che verrà

valutata caso per caso, in base ad una serie di criteri elencati nella norma, quali la tipologia, il pubblico e la dimensione del servizio, la tipologia di opere, ecc.) viene poi circoscritto attraverso criteri legati al fatturato del PSCC e al numero medio di visitatori unici mensili dei suoi servizi.

Restano esclusi dalla definizione di PSCC, per espressa indicazione normativa, i soggetti senza scopo di lucro (quali enciclopedie on-line – ad esempio, Wikipedia – e repertori didattici o scientifici), le piattaforme di sviluppo e condivisione di software *open source*, i fornitori di servizi di comunicazione elettronica, i mercati online, i servizi *cloud* da impresa a impresa e i servizi *cloud* che consentono agli utenti di caricare contenuti per uso personale.

4. Il diritto morale dell'autore

Accanto e indipendentemente dalla titolarità dei diritti di utilizzazione economica (e, dunque, anche nel caso questi siano stati eventualmente ceduti), l'autore gode del diritto morale sull'opera realizzata (artt. 20-24 l.d.a., 2582 c.c.).

Il diritto morale è posto a presidio della personalità dell'autore ed è caratterizzato dall'essere diritto irrinunciabile, inalienabile e imprescrittibile.

All'autore, in particolare, sono riconosciuti: a) il diritto alla paternità dell'opera; b) il diritto all'integrità dell'opera; c) il diritto di inedito; d) il c.d. diritto di pentimento (esercitabile solo a determinate condizioni).

Il diritto alla paternità dell'opera consente all'autore di rivendicare, cioè di veder riconosciuta, la sua qualità di autore dell'opera e di pretendere che il suo nome sia indicato «nelle forme d'uso» negli esemplari dell'opera o in relazione alle sue utilizzazioni. Questa indicazione, che deve essere riportata su ogni esemplare dell'opera, riguarda tutti gli autori dei contenuti che hanno concorso alla realizzazione dell'opera.

Il diritto all'integrità dell'opera consiste nel diritto dell'autore di opporsi a ogni deformazione, mutilazione o modificazione dell'opera e a ogni altro atto a danno della stessa che rechi pregiudizio al suo onore o alla sua reputazione. La sussistenza della lesione del diritto morale all'integrità dell'opera richiede, quindi, l'accertamento del pregiudizio all'onore o alla reputazione dell'autore, ossia dell'avvenuto detrimento del suo patrimonio morale.

Ulteriore espressione del diritto morale d'autore è il diritto di inedito, cioè la facoltà di non procedere alla pubblicazione della propria opera, diritto che si traduce in un rafforzamento del principio generale di esclusiva disponibilità dell'opera in capo al creatore.

Il c.d. diritto di pentimento consente invece all'autore, qualora concorrano gravi ragioni morali, di ritirare l'opera dal commercio, salvo l'obbligo di corrispondere un indennizzo a coloro che abbiano eventualmente acquistato i diritti

sull'opera medesima (art. 142 l.d.a., art. 2582 c.c.).

In base alle disposizioni vigenti in ambito nazionale (art. 23, comma 1, l.d.a.), il diritto morale sussiste in capo all'autore per l'intera durata della sua vita; successivamente è esercitabile, senza limite di tempo, dal coniuge e dai figli, e, in loro mancanza, dai genitori e dagli altri ascendenti e dai discendenti diretti, o, mancando gli ascendenti ed i discendenti, dai fratelli e dalle sorelle e dai loro discendenti (oltre che, in particolari circostanze, anche dallo Stato: cfr. art. 23, comma 2, l.d.a.).

Infine, sebbene il diritto morale sia inalienabile, l'autore che abbia conosciuto ed accettato eventuali modificazioni da parte di terzi alla propria opera non sarà più ammesso ad agire per impedirne l'esecuzione o per chiederne la soppressione (art. 22 l.d.a.).

5. Eccezioni e limitazioni al diritto d'autore

Si è visto come, in linea generale, qualunque utilizzazione dell'opera dell'ingegno protetta dal diritto d'autore, stante il contenuto e la portata delle prerogative economiche riservate all'autore dalla l.d.a., sia soggetta al previo necessario consenso dell'autore (o del soggetto che abbia da questi acquisito i diritti patrimoniali sull'opera).

Ebbene, nella stessa l.d.a. sono previsti alcuni casi in cui l'utilizzazione dell'opera non soggiace al consenso dell'autore (o del titolare dei diritti patrimoniali), ma può essere liberamente effettuata. Tali ipotesi, tradizionalmente identificate con la locuzione «libere utilizzazioni», sono oggi previste nel Titolo I, Capo V, sotto la rubrica «Eccezioni e limitazioni», agli artt. 65-71 *decies* l.d.a.

I casi di eccezione e limitazione alle prerogative economiche dell'autore costituiscono uno dei fondamentali limiti interni del diritto d'autore (insieme alla durata dei diritti patrimoniali e al principio dell'esaurimento); posti a presidio del bilanciamento fra prerogative private ed interessi collettivi, essi sono volti a garantire, sebbene in una limitata serie di ipotesi, la possibilità di un libero utilizzo dell'opera protetta.

Vediamone brevemente le ipotesi qui di maggiore interesse, così come si delineano oggi alla luce degli interventi da ultimo operati dal D.Lgs. 177/2021 di attuazione della direttiva (UE) 2019/790 e dal D.Lgs. 132/2025 dedicato all'intelligenza artificiale.

In base alle disposizioni della l.d.a., risultano libere, in quanto non necessitano del previo consenso dell'autore (o del titolare dei diritti patrimoniali), le seguenti attività:

a) la riproduzione o comunicazione al pubblico in riviste o giornali, anche radiotelevisivi, degli articoli di attualità di carattere economico, politico o religioso,

pubblicati nelle riviste o nei giornali, oppure radiodiffusi o messi a disposizione del pubblico, e gli altri materiali dello stesso carattere, se la riproduzione o l'utilizzazione non è stata espressamente riservata, purché si indichino la fonte da cui sono tratti, la data e il nome dell'autore, se riportato;

b) la riproduzione o comunicazione al pubblico di opere o materiali protetti utilizzati in occasione di avvenimenti di attualità ai fini dell'esercizio del diritto di cronaca e nei limiti dello scopo informativo, sempre che si indichi, salvo il caso di impossibilità, la fonte, incluso il nome dell'autore, se riportato;

c) la riproduzione o comunicazione al pubblico dei discorsi su argomenti di interesse politico o amministrativo tenuti in pubbliche assemblee o comunque in pubblico, nonché gli estratti di conferenze aperte al pubblico, nei limiti giustificati dallo scopo informativo, nelle riviste o nei giornali anche radiotelevisivi o telematici, purché si indichino la fonte, il nome dell'autore, la data e il luogo in cui il discorso fu tenuto;

d) la riproduzione di opere o brani di opere a fini di pubblica sicurezza, nelle procedure parlamentari, giudiziarie o amministrative, purché si indichino la fonte e, ove possibile, il nome dell'autore;

e) la riproduzione di singole opere o brani di opere per uso personale dei lettori, fatta a mano o con mezzi di riproduzione non idonei a spaccio o diffusione dell'opera nel pubblico;

f) la fotocopia di opere esistenti nelle biblioteche accessibili al pubblico o in quelle scolastiche, nei musei pubblici o negli archivi pubblici, effettuata dai predetti organismi per i propri servizi, senza alcun vantaggio economico o commerciale diretto o indiretto;

g) fermo restando il divieto di riproduzione di spartiti e partiture musicali, la riproduzione per uso personale, nei limiti del quindici per cento di ciascun volume o fascicolo di periodico, escluse le pagine di pubblicità, di opere dell'ingegno effettuata mediante fotocopia, xerocopia o sistema analogo;

h) salvo quanto disposto in ordine alla responsabilità dei prestatori intermediari, i già ricordati atti di riproduzione temporanea privi di rilievo economico proprio che sono transitori o accessori e parte integrante ed essenziale di un procedimento tecnologico, eseguiti all'unico scopo di consentire la trasmissione in rete tra terzi con l'intervento di un intermediario, o un utilizzo legittimo di un'opera o di altri materiali;

i) il prestito (di esemplari a stampa, di fonogrammi e di videogrammi) eseguito dalle biblioteche e discoteche dello Stato e degli enti pubblici, ai fini esclusivi di promozione culturale e studio personale¹⁰;

¹⁰ Sulla possibilità di qualificare, a determinate condizioni, il prestito di un libro elettronico (e-

k) la riproduzione in un unico esemplare, per i servizi delle biblioteche, discoteche e cineteche dello Stato e degli enti pubblici, senza alcun vantaggio economico o commerciale diretto o indiretto, dei fonogrammi e dei videogrammi esistenti presso i suddetti soggetti;

l) l'utilizzo da parte di specifici enti (biblioteche, istituti di istruzione, musei, ecc.) delle cc.dd. opere orfane (opere, specificatamente individuate, di cui nessuno dei titolari dei diritti è stato individuato oppure, anche se uno o più di loro siano stati individuati, nessuno di loro è stato rintracciato, al termine di una ricerca diligente) contenute nelle loro collezioni;

m) il riassunto, la citazione o la riproduzione di brani o di parti di opera e la loro comunicazione al pubblico, se effettuati per uso di critica o di discussione, nei limiti giustificati da tali fini e purché non costituiscano concorrenza all'utilizzazione economica dell'opera; se effettuati a fini di insegnamento o di ricerca scientifica l'utilizzo deve inoltre avvenire per finalità illustrative e per fini non commerciali. Nelle antologie ad uso scolastico la riproduzione non può superare la misura determinata da apposito regolamento, il quale fissa la modalità per la determinazione dell'equo compenso. Il riassunto, la citazione o la riproduzione debbono essere sempre accompagnati dalla menzione del titolo dell'opera, dai nomi dell'autore, dell'editore e, se si tratta di traduzione, del traduttore, qualora tali indicazioni figurino sull'opera riprodotta;

n) la libera pubblicazione attraverso la rete Internet, a titolo gratuito, di immagini e musiche a bassa risoluzione o degradate per uso didattico o scientifico, solo nel caso in cui tale utilizzo non sia a scopo di lucro. Con decreto del Ministro per i beni e le attività culturali saranno definiti i limiti all'uso didattico o scientifico citato;

o) ai portatori di particolari handicap, per uso personale, la riproduzione di opere e materiali protetti o l'utilizzazione della comunicazione al pubblico degli stessi, purché siano direttamente collegate all'handicap, non abbiano carattere commerciale e si limitino a quanto richiesto dall'handicap;

p) la comunicazione o la messa a disposizione destinata a singoli individui, a scopo di ricerca o di attività privata di studio, su terminali aventi tale unica funzione situati nei locali delle biblioteche accessibili al pubblico, degli istituti di istruzione, nei musei e negli archivi, limitatamente alle opere o ad altri materiali contenuti nelle loro collezioni e non soggetti a vincoli derivanti da atti di cessione o da licenza;

q) la riproduzione privata di fonogrammi e videogrammi su qualsiasi suppor-

book) come equiparabile al prestito di un libro tradizionale, si veda la sentenza della Corte di giustizia dell'UE, 10 novembre 2016, procedimento C-174/15, *Vereniging Openbare Bibliotheken c. Stichting Leenrecht*.

to, effettuata da una persona fisica per uso esclusivamente personale, purché senza scopo di lucro e senza fini direttamente o indirettamente commerciali, nel rispetto delle misure tecnologiche poste a tutela dell'opera dal legittimo titolare dei diritti di sfruttamento¹¹. I titolari dei diritti sono tenuti a consentire che, nonostante l'eventuale applicazione delle misure tecnologiche, la persona fisica che abbia acquisito il possesso legittimo di esemplari dell'opera o del materiale protetto, ovvero vi abbia avuto accesso legittimo, possa effettuare una copia privata, anche solo analogica, per uso personale, a condizione che tale possibilità non sia in contrasto con lo sfruttamento normale dell'opera o degli altri materiali e non arrechi ai titolari dei diritti un ingiustificato pregiudizio. Ai titolari dei diritti sull'opera riprodotta spetterà comunque un equo compenso per tale riproduzione privata. La riproduzione, inoltre, non può essere effettuata da terzi. Infine, la libera riproduzione in parola non si applica alle opere o ai materiali protetti messi a disposizione del pubblico in modo che ciascuno possa avervi accesso dal luogo e nel momento scelti individualmente (cioè tipicamente attraverso Internet), quando l'opera è protetta dalle misure tecnologiche di cui all'art. 102 *quater* l.d.a. ovvero quando l'accesso è consentito sulla base di accordi contrattuali;

r) il riassunto, la citazione, la riproduzione, la traduzione e l'adattamento di brani o di parti di opere e di altri materiali e la loro comunicazione al pubblico (accompagnati dalla menzione del titolo dell'opera originaria, dei nomi dell'autore, dell'editore e del traduttore, se tali indicazioni figurino su detta opera) se effettuati con mezzi digitali, esclusivamente per finalità illustrative ad uso didattico, nei limiti di quanto giustificato dallo scopo non commerciale perseguito, nonché sotto la responsabilità di un istituto di istruzione, nei suoi locali o in altro luogo o in un ambiente elettronico sicuro, accessibili solo al personale docente di tale istituto e agli alunni o studenti iscritti al corso di studi in cui le opere o gli altri materiali sono utilizzati.

Resta comunque vietato lo spaccio al pubblico delle copie di cui ai punti e), f), g) e, in genere, ogni utilizzazione in concorrenza con i diritti di utilizzazione economica spettanti all'autore.

Altre eccezioni sono quelle introdotte dal D.Lgs. 177/2021 legate all'attività di «estrazione di testo e di dati» (in inglese, «data mining») (artt. 70-*ter* e 70-*quater* l.d.a.), di particolare rilevanza in quanto investono anche e soprattutto l'attività di addestramento delle intelligenze artificiali¹².

Per «estrazione di testo e di dati» si intende qualsiasi tecnica automatizzata volta ad analizzare grandi quantità di testi, suoni, immagini, dati o metadati in formato digitale con lo scopo di generare informazioni, inclusi modelli, tenden-

¹¹ In merito alle misure tecnologiche di protezione si veda il successivo § 6.

¹² Cfr. art. 53 del Regolamento (UE) 2024/1689, c.d. «Regolamento sull'intelligenza artificiale» (G.U.C.E. L, 2024/1689, del 12 luglio 2024).

ze e correlazioni. Ebbene, agli organismi di ricerca e agli istituti di tutela del patrimonio culturale (entrambi definiti nella norma) viene consentita un'attività di riproduzione laddove ciò avvenga per scopi di ricerca scientifica e ai fini dell'estrazione di testo e di dati da opere o da altri materiali disponibili in reti o in banche di dati cui essi hanno lecitamente accesso, nonché la comunicazione al pubblico degli esiti della ricerca ove espressi in nuove opere originali (artt. 70-ter l.d.a.). Le copie di opere o di altri materiali realizzate a tali fini devono essere memorizzate con un adeguato livello di sicurezza e possono essere conservate e utilizzate unicamente per scopi di ricerca scientifica, ivi inclusa la verifica dei risultati della ricerca. Detto che i titolari dei diritti sono autorizzati ad applicare, in misura non eccedente a quanto necessario allo scopo, misure idonee a garantire la sicurezza e l'integrità delle reti e delle banche dati in cui sono ospitati le opere o gli altri materiali oggetto di riproduzione, eventuali pattuizioni contrattuali che vadano a limitare od escludere tali prerogative per gli organismi di ricerca e gli istituti di tutela del patrimonio culturale saranno nulle *ex lege*.

Per tutti i soggetti diversi dagli organismi di ricerca e dagli istituti di tutela del patrimonio culturale o laddove siano perseguite finalità divergenti dalla sola ricerca scientifica, in materia di *data mining* troverà applicazione una seconda eccezione, prevista oggi dall'art. 70-quater l.d.a. La norma prevede che siano consentite le riproduzioni e le estrazioni da opere o da altri materiali contenuti in reti o in banche di dati cui si ha legittimamente accesso ai fini dell'estrazione di testo e di dati, ma con l'ulteriore condizione determinante che l'utilizzo delle opere e degli altri materiali non sia stato espressamente riservato dai titolari del diritto d'autore e dei diritti connessi nonché dai titolari delle banche dati. Dunque, laddove un titolare non avrà espressamente e chiaramente dichiarato di volersi riservare l'utilizzo della propria opera protetta ai fini del *data mining*, tale attività risulterà lecita da parte di chiunque abbia legittimo accesso a detta opera e qualunque sia la finalità da questi perseguita. Le riproduzioni e le estrazioni eseguite potranno comunque essere conservate solo per il tempo necessario ai fini dell'estrazione di testo e di dati di cui trattasi, con adeguati livelli di sicurezza.

Da ultimo, il D.Lgs. 132/2025 ha introdotto nella l.d.a. anche l'art. 70-septies: la disposizione prevede che le riproduzioni e le estrazioni da opere o da altri materiali contenuti in rete o in banche di dati a cui si ha legittimamente accesso, ai fini dell'estrazione di testo e di dati attraverso modelli e sistemi di intelligenza artificiale, anche generativa, siano consentite in conformità alle disposizioni di cui agli articoli 70-ter e 70-quater l.d.a.¹³.

¹³ Lo stesso D.Lgs. 132/2025 ha poi aggiunto, quale nuova fattispecie penale, la violazione di queste ultime disposizioni alla lett. a-ter) dell'art. 171 l.d.a.

Le eccezioni e limitazioni sopra citate si applicano non solo ai diritti patrimoniali d'autore, bensì, per espressa indicazione, anche ai diritti connessi e al diritto del costituente di una banca di dati.

Una specifica disposizione precisa che le eccezioni e limitazioni ai diritti patrimoniali d'autore, quando sono applicate ad opere o ad altri materiali protetti messi a disposizione del pubblico in modo che ciascuno possa avervi accesso dal luogo e nel momento scelto individualmente (cioè tipicamente attraverso Internet), non devono essere in contrasto con lo sfruttamento normale delle opere o degli altri materiali, né arrecare un ingiustificato pregiudizio agli interessi dei titolari (art. 71 *nonies* l.d.a.). Tale ultimo principio costituisce un limite di ordine generale per qualunque utilizzazione libera dell'opera dell'ingegno nell'ambito di Internet e la sua concreta portata è al centro del dibattito dottrinale.

Ponendosi quali eccezioni ai diritti di sfruttamento economico dell'opera da parte dell'autore, le norme in materia di libere utilizzazioni sono state tradizionalmente ritenute di natura speciale, facendone discendere coerentemente una impossibilità di applicazione in via analogica o di una loro interpretazione estensiva, dovendo esse trovare applicazione solo nei casi tassativamente indicati dalla legge. Tale interpretazione, sebbene aderente al dato normativo, è stata recentemente criticata e va affermandosi una tesi propensa a ritenere i casi di libera utilizzazione non come "eccezioni", bensì quali limiti connaturati alle prerogative dell'autore, indispensabili per un corretto e bilanciato funzionamento dello stesso istituto del diritto d'autore.

Si noti come le ipotesi di eccezione e limitazione presentate attengano esclusivamente alla sfera patrimoniale del diritto d'autore: la tutela dei diritti a difesa della personalità dell'autore (diritto morale) può esercitarsi in ogni tempo, anche se è scaduto il termine di protezione stabilito dalla legge per i diritti patrimoniali, se sono intervenute altre cause di decadenza dei diritti economici o anche se l'opera è stata impiegata nei modi consentiti dalle norme in materia di eccezioni e limitazioni. Anche in quest'ultima ipotesi, pertanto, rimarranno pienamente applicabili le prerogative morali dell'autore.

6. Le misure tecnologiche di protezione e le informazioni elettroniche sul regime dei diritti

Lo sviluppo delle tecnologie digitali ha profondamente inciso sulla realtà nella quale la disciplina del diritto d'autore deve operare: ha aperto la strada a nuove forme di creazione e riproduzione delle tradizionali opere dell'ingegno; ha consentito la nascita di nuovi beni (programmi per elaboratore, banche di dati elettroniche), oggi tutelati a loro volta quali opere dell'ingegno; ha rivoluzionato gli aspetti legati alla circolazione delle opere dell'ingegno a livello planetario, attraverso la rete Internet.

Le possibilità e le modalità di sfruttamento delle opere sono state significativamente incrementate da queste tecnologie. Nello stesso tempo le caratteristiche del dato digitale, la facilità con la quale può essere riprodotto, duplicato, manipolato e trasmesso (con costi irrisori) hanno comportato un parallelo aumento dei casi di violazione dei diritti d'autore. Il fenomeno, generalmente indicato con l'espressione "pirateria", ha assunto in alcune fasi dimensioni allarmanti, in particolare rispetto a taluni tipi di opere (musicali, cinematografiche, programmi per elaboratore, videogiochi, ecc.).

Da qui l'esigenza, sempre più sentita dagli operatori, di affiancare alla disciplina giuridica di protezione (spesso impotente nell'impedire o anche solo nel perseguire efficacemente le violazioni) una tutela di tipo tecnologico.

I sistemi tecnico-informatici di protezione si sono così evoluti e diffusi nel mercato, sino a diventare strumenti di ordinario utilizzo per interi settori della c.d. industria culturale. Il riconoscimento della loro importanza per garantire la tutela dei diritti d'autore ha trovato riscontro anche a livello normativo a partire dalla metà degli anni Novanta.

Ad operare l'adeguamento della disciplina internazionale sul diritto d'autore alle tecnologie digitali e telematiche (introducendo il c.d. *digital copyright*) sono stati i già ricordati trattati elaborati in seno alla OMPI nel 1996 (WCT, WPPT).

Oltre al principio generale che impone di riconoscere all'autore, nel mondo digitale di Internet, le medesime prerogative sulla sua opera valide per il "mondo fisico" (da cui il diritto di messa a disposizione del pubblico, del quale si è già detto), l'elemento qui di specifico interesse è l'introduzione di una disciplina di tutela delle misure tecnologiche di protezione¹⁴.

Il testo del WCT, pur senza definire le misure tecnologiche (come invece avviene nella direttiva 2001/29/CE), ne sanziona l'alterazione (art. 11) e disciplina gli obblighi in materia di informazioni sulla gestione dei diritti (art. 12). Disposizioni analoghe sono contenute agli artt. 18 e 19 del WPPT.

Ai principi contenuti nei suddetti trattati in Europa si è data attuazione con la direttiva 2001/29/CE e il D.Lgs. 68/2003 ha provveduto in merito ad inserire gli artt. 102-*quater* e 102-*quinquies* nella l.d.a. Queste norme rispettivamente legittimano espressamente i titolari di diritti d'autore e di diritti connessi ad apporre sulle opere o sui materiali protetti misure tecnologiche di protezione (misure che comprendono «tutte le tecnologie, i dispositivi o i componenti che, nel normale corso del loro funzionamento, sono destinati a impedire o limitare atti

¹⁴ Si noti come una disciplina in merito alle misure tecnologiche di protezione del programma per elaboratore era già stata introdotta in Europa dalla direttiva 91/250/CEE (oggi direttiva 2009/24/CE): a livello italiano, si vedano le tuttora vigenti norme previste dall'art. 161, comma 4, e 171-*bis*, comma 1, l.d.a.

non autorizzati dai titolari dei diritti», art. 102 *quater* l.d.a.) e informazioni elettroniche sul regime dei diritti (che possono essere fatte apparire nella eventuale comunicazione al pubblico delle opere stesse o del materiale protetto e possono contenere anche indicazioni circa i termini o le condizioni d'uso dell'opera o dei materiali). Corrispondentemente a tali facoltà, riservate ai titolari dei diritti, sono state introdotte, agli artt. 171-*ter* e 174-*ter* l.d.a., specifiche sanzioni penali ed amministrative a salvaguardia delle misure tecnologiche di protezione (nel caso dell'art. 171-*ter* l.d.a., purché «efficaci», cioè nel caso in cui l'uso dell'opera o del materiale protetto sia controllato dai titolari tramite l'applicazione di un dispositivo di accesso o di un procedimento di protezione, ovvero sia limitato mediante un meccanismo di controllo delle copie¹⁵) e delle informazioni elettroniche sul regime dei diritti¹⁶.

Si noti come, sebbene il legislatore eurocomunitario abbia richiesto agli Stati membri di prevedere un'adeguata protezione giuridica anche contro l'elusione di efficaci misure tecnologiche (svolta da persone consapevoli, o che si possano ragionevolmente presumere consapevoli, di perseguire tale obiettivo; art. 6 direttiva 2001/29/CE), tale disposizione non sia stata attuata in Italia: nella l.d.a è così presente una norma che sanziona le condotte attinenti agli strumenti e ai servizi «che abbiano la prevalente finalità o l'uso commerciale di eludere efficaci misure tecnologiche» ovvero «siano principalmente progettati, prodotti, adattati o realizzati con la finalità di rendere possibile o facilitare l'elusione» di dette misure, (art.171-*ter*, comma 1, l.d.a., lett. f)-*bis*; c.d. *anti-device provision*), ma non si rinviene, invece, una *anti-circumvention provision*, cioè una norma che sanziona la sola elusione della misura tecnologica di protezione, prescindendo da un utilizzo abusivo dell'opera protetta (cfr. art. 174-*ter*, comma 1, l.d.a.). Del resto, forti critiche sono state sollevate in merito alla formulazione delle suddette norme europee in ordine all'introduzione di fattispecie presuntive. In particolare, con riferimento specifico agli artt. 6 e 7 della direttiva 2001/29/CE, si è fatto notare come la direttiva sia andata ben oltre la mera implementazione delle corrispondenti disposizioni del *WIPO Copyright Treaty-WCT*, prevedendo una tutela anche

¹⁵ Il concetto di «efficacia» della misura tecnologica richiede altresì un livello minimo di sicurezza della misura, capace di garantire che l'elusione non possa avvenire se non attraverso un'attività intenzionalmente diretta a realizzare tale risultato. In merito alla nozione di «efficace misura tecnologica» si veda la sentenza della Corte di giustizia dell'UE, 23 gennaio 2014, Causa C-355/-12, *Nintendo Co. Ltd/Nintendo of America Inc./Nintendo of Europe GmbH c. PC Box Srl/9Net Srl*.

¹⁶ Vedi l'art. 171-*ter*, comma 1, l.d.a., lett. f)-*bis* e h), così come introdotte dal D.Lgs. 68/2003. Si veda altresì l'art. 174-*ter*, comma 1, l.d.a. in materia di sanzione amministrativa pecuniaria e sanzioni accessorie. Si noti come in quest'ultimo articolo non si faccia riferimento a misure tecnologiche «efficaci» e, pertanto, la disposizione si dovrà applicare in ogni caso, laddove misure tecnologiche (di qualunque genere) siano presenti.

contro le cc.dd. attività preparatorie al vero e proprio aggiramento delle protezioni tecnologiche.

Da ultimo, si noti come l'adozione di misure tecnologiche di protezione possa interferire con l'esercizio di una eccezione o limitazione prevista dalla l.d.a., impedendo di fatto al soggetto legittimato di eventualmente usufruire di detta eccezione o limitazione. In merito, l'art. 71-*quinquies* l.d.a. prevede in via generale che i titolari di diritti che abbiano apposto le misure tecnologiche sono «tenuti alla rimozione delle stesse, per consentire l'utilizzo delle opere o dei materiali protetti, dietro richiesta dell'autorità competente, per fini di sicurezza pubblica o per assicurare il corretto svolgimento di un procedimento amministrativo, parlamentare o giudiziario», nonché «ad adottare idonee soluzioni, anche mediante la stipula di appositi accordi con le associazioni di categoria rappresentative dei beneficiari, per consentire l'esercizio delle eccezioni di cui agli articoli 55, 68, commi 1 e 2, 69, comma 2, 70, comma 1, 71-*bis* e 71-*quater*, su espressa richiesta dei beneficiari» e sempre che questi «abbiano acquisito il possesso legittimo degli esemplari dell'opera o del materiale protetto, o vi abbiano avuto accesso legittimo ai fini del loro utilizzo». Ebbene, a tale ultimo obbligo i titolari dei diritti non sono tenuti in relazione alle opere o materiali «messi a disposizione del pubblico in modo che ciascuno vi possa avere accesso dal luogo o nel momento scelto individualmente [cioè on-line, via Internet; *n.d.r.*], quando l'accesso avvenga sulla base di accordi contrattuali» (art. 71-*quinquies*, comma 3, l.d.a.). Stante la frequenza con cui tale ultima condizione si realizza nel *web*, dove la pubblicazione di contenuti protetti è il più delle volte accompagnata dalla previsione di condizioni contrattuali per l'accesso e l'utilizzo dei contenuti, si comprende facilmente come la disciplina vigente limiti oggi fortemente le prerogative dell'utente legittimo dell'opera a favore del relativo titolare dei diritti¹⁷.

7. I beni informatici: programmi per elaboratore e banche di dati elettroniche

La tutela del diritto d'autore è nata e si è sviluppata in relazione alle opere di natura letteraria ed artistica. Lo stesso requisito di accesso alla tutela, cioè il carattere creativo dell'opera come espressione della personalità dell'autore, richiama la figura dell'autore quale "artista" ed è concetto intimamente legato alla natura artistico-culturale dell'opera. La qualifica di opera dell'"ingegno" ne consente una distinzione da altre opere a loro volta frutto di inventiva (quali i mo-

¹⁷ Per una disposizione dello stesso tenore in materia di copia privata di fonogrammi e videogrammi, si veda il precedente § 5.

delli industriali, le invenzioni, ecc., tutelate da diversa disciplina¹⁸), se ed in quanto se ne consideri il legame con il “genio” artistico dell'autore.

Sviluppata intorno all'opera letteraria, la disciplina a tutela del diritto d'autore ha però conosciuto, con il passare del tempo, un progressivo allargamento del suo ambito di applicazione a favore di opere via via sempre più distanti dal requisito di una piena e significativa creatività artistica. Al contempo, si è assistito ad un graduale abbassamento della soglia di creatività richiesta per accedere alla tutela.

Lo sviluppo delle moderne tecnologie informatiche ha portato tale processo sino a quelle che, secondo alcuni, sono conseguenze censurabili. Ciò risulta evidente in riferimento ai programmi per elaboratore e alle banche di dati elettroniche, nuovi beni informatici frutto della rivoluzione digitale.

A seguito della crescente importanza economica di tali beni è emersa l'esigenza di individuare un regime di tutela adeguato a garantire i legittimi interessi degli operatori del settore rispetto a condotte che potessero vanificarne gli investimenti. La risposta del legislatore è stata, come meglio vedremo, quella di estendere espressamente la disciplina del diritto d'autore anche a questi nuovi beni. Tuttavia, la loro natura appare distante da quella di un'opera artistica, quale un poema o una sinfonia musicale, e del tutto differenti risultano le loro caratteristiche peculiari (ivi comprese le destinazioni d'uso) e le relative esigenze di tutela. Per tali ragioni, per il software e per le banche di dati è stata coniata in dottrina la definizione di «opere utili», per distinguerli appunto dalle tradizionali opere più propriamente artistiche. Le opere utili sono caratterizzate non tanto dalla creatività, bensì dalla loro funzionalità e utilità: nel loro caso, il concetto stesso di creatività risulta necessariamente compresso, sino a divenire, secondo alcuni, un mero elemento negativo, rappresentato dal riscontro della non copiatura, cioè quale semplice «diversità dai precedenti»¹⁹.

7.1. Il regime di protezione dei programmi per elaboratore

Il dibattito sulla scelta effettuata dal legislatore è tutt'altro che sopito innanzitutto per i programmi per elaboratore, sebbene questi per primi abbiano ricevuto una disciplina di protezione inquadrata nell'ambito del diritto d'autore.

La normativa nazionale in materia è stata introdotta con il D.Lgs. 518/1992 (G.U. del 31 dicembre 1992, n. 306) di attuazione della direttiva 91/250/CEE (oggi sostituita dalla direttiva 2009/24/CE, G.U.C.E. del 5 maggio 2009, n. L

¹⁸ In ambito nazionale v. D.Lgs. 10 febbraio 2005, n. 30, «Codice della proprietà industriale» (G.U. 4 marzo 2005, n. 52).

¹⁹ Cfr. M. ORLANDI, *Motori di ricerca e diritto d'autore*, in *AIDA*, 1998, p. 275.

111/16) ed ha stabilito che i programmi per elaboratore sono protetti «come opere letterarie ai sensi della Convenzione di Berna sulla tutela delle opere letterarie ed artistiche» (art. 1, comma 2, l.d.a.). La stessa scelta è stata operata nei ricordati trattati internazionali TRIPs e WCT.

L'opportunità di ricorrere alla disciplina di protezione delle opere dell'ingegno, assimilando il software all'opera letteraria ai fini della sua tutela, ha sollevato da subito forti perplessità, in considerazione dell'evidente ed innegabile diversità fra le due opere.

Secondo quanto disposto dal novellato testo dell'art. 2 l.d.a., la tutela si estende ai programmi «in qualsiasi forma espressi purché originali», mentre ne restano esclusi «le idee ed i principi che stanno alla base di qualsiasi elemento di un programma, compresi quelli alla base delle sue interfacce», in ossequio al generale principio del diritto d'autore per cui la portata dell'esclusiva riconosciuta al titolare del diritto è limitata alla sola forma espressiva dell'opera protetta²⁰.

Si noti come il legislatore europeo – a differenza, ad esempio, di quello nordamericano – non abbia provveduto ad introdurre una specifica definizione normativa di programma per elaboratore. Il concetto di software desumibile dalla direttiva 91/250/CEE (oggi 2009/24/CE) è comunque piuttosto ampio, comprendendo i «programmi in qualsiasi forma, compresi quelli incorporati nell'hardware» ed inoltre il «materiale preparatorio per la progettazione del programma» (Considerando n. 7 e art. 1 della direttiva 2009/24/CE).

La protezione investe la forma espressiva del software, qualunque essa sia: risultano quindi tutelati sia il codice sorgente (cioè l'insieme delle istruzioni scritte dal programmatore in un determinato linguaggio di programmazione), sia il codice oggetto (cioè l'insieme delle istruzioni del programma tradotte in linguaggio macchina, ovvero sia in codice binario, l'unico comprensibile dall'elaboratore), così come qualunque tipo di software (sistemi operativi, programmi applicativi, ecc.) ed i relativi materiali preparatori (quali, ad esempio, i diagrammi di flusso, le descrizioni di sequenza, le specifiche funzionali)²¹.

Il requisito affinché il programma per elaboratore possa godere della protezione è stato espressamente individuato nell'essere «originale quale risultato di

²⁰ La dottrina italiana maggioritaria ritiene siano esclusi dalla tutela, proprio in base a detto principio, anche gli algoritmi matematici utilizzati nel programma: cfr. L.C. UBERTAZZI (a cura di), *Commentario breve alle leggi su proprietà intellettuale e concorrenza*, Padova: Cedam 2019, p. 1840. Si veda, però, quanto detto nel proseguo a proposito della tutela degli stessi algoritmi di coordinamento e organizzazione di una banca di dati elettronica.

²¹ L'interfaccia utente grafica non costituisce, invece, una forma di espressione di un programma per elaboratore: si veda la sentenza della Corte di giustizia dell'UE, 22 dicembre 2010, procedimento C-393/09 (domanda di pronuncia pregiudiziale proposta dal Nejvyšší správní soud - Repubblica ceca) *Bezpečnostní softwarová asociace - Svaž softwarové ochrany c. Ministerstvo kultury*.

creazione intellettuale dell'autore» (art. 2, n. 8, l.d.a.). Si tratta di un requisito di creatività specifico, differenziato rispetto a quello generale, che pare voler indicare un'originalità di tipo esclusivamente soggettivo. Si è voluta così garantire la tutela del programma per elaboratore che risulti frutto di un'attività dell'autore e non di una mera azione di copiatura. Come evidenziato in dottrina, a motivo della natura funzionale del software, l'applicazione del criterio tradizionale di creatività avrebbe altrimenti provocato l'automatica esclusione della maggior parte dei programmi per elaboratore dalla tutela d'autore.

Del resto, nella programmazione l'autore spesso non farà altro che selezionare gli elementi funzionali più adatti a risolvere un dato problema tecnico. Si è così sostenuto che l'originalità di un programma potrà sussistere solo se effettivamente ricorra una «sufficiente libertà di scelta fra più varianti» ugualmente utilizzabili per risolvere il problema: in caso contrario, se le alternative risultassero invece esigue, tanto da comportare scelte praticamente obbligate fra una ristretta cerchia di possibilità, l'originalità non potrà che mancare²².

Laddove il programma sia dotato di quel minimo di creatività (soggettiva) richiesta, risulteranno tutelati le istruzioni contenute nel codice sorgente e nel codice oggetto (i cc.dd. elementi letterali), nonché la struttura, l'organizzazione e la sequenza delle istruzioni (i cc.dd. elementi non letterali) ed anche i materiali preparatori per la progettazione del programma stesso.

La titolarità dei diritti d'autore sul programma spetterà all'autore di questo, secondo i generali principi sanciti nei primi articoli della l.d.a. che abbiamo illustrato.

Essendo spesso un'opera plurisoggettiva, alla cui creazione collaborano più soggetti, i diritti d'autore potranno appartenere a colui che ha coordinato la realizzazione del software, se opera collettiva, oppure congiuntamente a tutti i co-autori, se opera in comunione. Potrà, inoltre, trovare applicazione l'art. 4 l.d.a., quando il software si presenti quale opera creativa frutto dell'elaborazione di opere preesistenti.

Si è già detto come in ambito nazionale il diritto d'autore sia attribuito in via generale alla persona fisica dell'autore, mentre le ipotesi di titolarità *ab origine* in capo a persone giuridiche costituisca un'eccezione. Fra queste va annoverata l'ipotesi disciplinata dall'art. 12-*bis* l.d.a., introdotto dal D.Lgs. 518/1992. La norma dispone che i diritti di utilizzazione economica sui programmi per elaboratore creati dal lavoratore dipendente, in esecuzione delle sue mansioni o su istruzioni impartite dal datore di lavoro, spettino a quest'ultimo.

²² Così G. GUGLIELMETTI, *L'invenzione di software. Brevetto e diritto d'autore*, Milano: Giuffrè, 1997, pp. 257-258.

In merito al diritto morale, la sua titolarità rimarrà invece, in ogni caso, in capo al singolo autore persona fisica, oppure alle persone fisiche qualificate come coautori, secondo le disposizioni relative all'eventuale specie di opera plurisoggettiva a cui il programma apparterrà.

All'autore (o agli autori) del programma sono riconosciuti, oltre ai diritti morali, i diritti esclusivi di effettuare o autorizzare (art. 64-*bis* l.d.a.):

a) la riproduzione, permanente o temporanea, totale o parziale, del programma per elaboratore con qualsiasi mezzo o in qualsiasi forma. Si noti che, nella misura in cui operazioni quali il caricamento, la visualizzazione, l'esecuzione, la trasmissione o la memorizzazione del programma per elaboratore richiedano una riproduzione, anche tali operazioni sono soggette all'autorizzazione del titolare dei diritti;

b) la traduzione, l'adattamento, la trasformazione e ogni altra modificazione del programma per elaboratore, nonché la riproduzione dell'opera che ne risulti, senza pregiudizio dei diritti di chi modifica il programma;

c) qualsiasi forma di distribuzione al pubblico, compresa la locazione, del programma per elaboratore originale o di copie dello stesso.

La prima vendita di una copia del programma nell'UE da parte del titolare dei diritti, o con il suo consenso, esaurisce il diritto di distribuzione di detta copia all'interno dell'Unione (principio dell'esaurimento), ad eccezione del diritto di controllare l'ulteriore locazione del programma o di una copia dello stesso (locazione alla quale viene tradizionalmente ricondotto il contratto tipicamente utilizzato per la distribuzione del software: la c.d. licenza d'uso)²³.

Oltre ai generali casi di eccezione e limitazione già presentati e salvo patto contrario, non sono invece soggette all'autorizzazione del titolare dei diritti le attività di cui alle precedenti lett. a) e b) poste in essere da parte del legittimo acquirente, allorché siano necessarie per l'uso del programma per elaboratore conformemente alla sua destinazione, inclusa la correzione degli errori (art. 64-*ter* l.d.a.).

All'utente legittimo, inoltre, non potrà essere impedito contrattualmente di effettuare una copia di riserva del programma, qualora tale copia sia necessaria per il suo uso. Questi può altresì, senza l'autorizzazione del titolare dei diritti,

²³ Sulla qualificazione dei contratti di licenza d'uso di programmi per elaboratore e sull'applicazione in via generale del principio dell'esaurimento al diritto di distribuzione anche sulle copie di un programma messo a disposizione on-line (di cui, cioè, venga effettuato il c.d. *download*), si veda l'importante decisione della Corte di giustizia europea, 3 luglio 2012, causa C-128/11, *UsedSoft GmbH c. Oracle International Corp.*

Sempre sul tema del principio dell'esaurimento applicato ai programmi per elaboratore si veda anche la sentenza della Corte di giustizia dell'UE, 12 ottobre 2016, causa C-166/15, *Aleksandrs Ranks e Juris Vasiljevičs*.

osservare, studiare o sottoporre a prova il funzionamento del programma, allo scopo di determinare le idee ed i principi su cui è basato ogni elemento del programma stesso, qualora compia tali atti durante operazioni di caricamento, visualizzazione, esecuzione, trasmissione o memorizzazione del programma che ha il diritto di eseguire. Le eventuali clausole contrattuali pattuite in violazione di tali ultime facoltà sono considerate nulle.

All'utente legittimo di un software viene riconosciuto, unicamente al ricorrere di specifiche condizioni, anche il diritto di compiere il c.d. *reverse engineering* o decompilazione del programma (art. 64-*quater* l.d.a.).

Decompilare un software, cioè eseguire su di esso il c.d. *reverse engineering*, significa operare quelle operazioni necessarie a ricostruire il codice sorgente (cioè il programma scritto attraverso una serie di istruzioni in un linguaggio di programmazione comprensibile all'essere umano) partendo dal codice oggetto (cioè il programma "compilato" nel formato comprensibile, e quindi eseguibile, dall'elaboratore elettronico, il linguaggio macchina o binario). Attraverso tale operazione si possono così apprendere, grazie alla disponibilità del codice sorgente, il contenuto 'informativo' del software, la sua struttura e le sue caratteristiche.

L'autorizzazione del titolare dei diritti a compiere la decompilazione non è richiesta unicamente qualora la riproduzione del codice del programma e la traduzione della sua forma (la decompilazione, appunto) siano indispensabili all'utente legittimo per ottenere le informazioni necessarie per conseguire l'interoperabilità (cioè la compatibilità) con un proprio programma per elaboratore creato autonomamente.

Tale attività di decompilazione è subordinata alle seguenti condizioni:

- che l'analisi del programma sia eseguita solo dal licenziatario o da altri che abbia il diritto di usare una copia del programma;
- che le informazioni necessarie per conseguire l'interoperabilità non siano già diversamente accessibili;
- che le predette attività siano limitate alle parti del programma originale necessarie per conseguire l'interoperabilità.

Inoltre, le informazioni ottenute mediante il *reverse engineering* non dovranno essere:

- utilizzate a fini diversi dal raggiungimento dell'interoperabilità;
- comunicate a terzi;
- utilizzate per lo sviluppo, la produzione e la commercializzazione di un programma per elaboratore sostanzialmente simile a quello decompilato.

Se quella presentata sommariamente è la disciplina di tutela dei programmi per elaboratore nel nostro ordinamento (non diversa, nei suoi contenuti essen-

ziali, da quella prevista negli altri paesi europei e nei trattati internazionali), vanno rilevate alcune conseguenze della scelta operata dal legislatore.

La previsione di un criterio di accesso alla tutela *ad hoc*, rappresentato da una creatività soggettiva di basso livello, fa sì che, nella pratica, qualunque programma per elaboratore, che non sia il frutto di un mero plagio e che non si presenti del tutto banale, possa assurgere ad opera dell'ingegno e godere della relativa tutela. Questa consente all'autore di disporre delle ampie prerogative patrimoniali e morali previste dalla l.d.a., non diversamente da quanto avviene per qualunque altra opera dell'ingegno. Tuttavia, come già segnalato, i programmi per elaboratore si differenziano nettamente dagli altri generi di opere tradizionalmente protette dal diritto d'autore: la possibilità di distribuire il programma nella sola versione eseguibile (il codice oggetto, a sua volta tutelato), unita ai limitati casi di decompilazione consentiti, il più delle volte finisce per impedire del tutto l'accesso alle idee e ai principi alla base del programma per elaboratore. Idee e principi che dovrebbero, invece, risultare liberamente utilizzabili, in quanto esclusi e sottratti alla tutela d'autore, secondo il generale principio espressamente ribadito anche per il software all'art. 2 l.d.a.

Le ripercussioni della scelta operata dal legislatore appaiono tanto più discutibili se si considerano le dinamiche accelerate dell'odierno mercato del software e le conseguenti esigenze specifiche di circolazione del "sapere informatico" necessarie per garantire lo sviluppo di nuovi prodotti.

Sotto questo profilo, appare del tutto incongrua anche la durata della protezione garantita dalla disciplina sui diritti patrimoniali (70 anni dalla morte dell'autore): in un mercato in cui l'obsolescenza di un prodotto software si manifesta spesso (nella migliore delle ipotesi) nell'arco di pochi anni, tale durata supera di gran lunga qualunque reale esigenza di protezione di un programma, ma nello stesso tempo potenzialmente ne inibisce la circolazione libera (e l'accesso al codice sorgente) per un lunghissimo lasso di tempo.

Del resto, la scelta operata dal legislatore per i programmi per elaboratore ha sollevato forti dubbi già all'indomani dell'approvazione della direttiva 91-/250/CEE, facendo poi emergere una posizione apertamente favorevole ad una revisione del regime di tutela adottato²⁴.

²⁴ L'alternativa di una protezione dei programmi per elaboratore attraverso il brevetto, quali «invenzioni», risulta espressamente esclusa dall'art. 45 del Codice della proprietà industriale (D.Lgs. 30/2005), in ossequio al divieto di brevettazione del software «in quanto tale» contenuto nell'art. 52 della Convenzione sul Brevetto Europeo (ratificata in Italia con L. 26 maggio 1978, n. 260, *G.U.* 7 giugno 1978, n. 156). La proposta di direttiva per l'introduzione nell'UE di una tutela di tipo brevettuale per i programmi per elaboratore (Proposta di direttiva del Parlamento europeo e del Consiglio relativa alla brevettabilità delle invenzioni attuate per mezzo di elaboratori elettronici, 2002/C 151 E/05, COM2002 92 def. — 2002/0047COD), presentata dalla Commissione il

Proprio l'ingessatura che reca con sé la disciplina vigente, anche sotto il profilo del rigido controllo che attraverso di essa le multinazionali informatiche cercano di imporre, ha fatto emergere iniziative come quella dell'*Open Source* (la distribuzione di software nella sua versione in codice sorgente), volta a superare la visione strettamente proprietaria del diritto d'autore, a facilitare una creazione collaborativa e la condivisione del sapere informatico.

7.2. La tutela delle banche di dati

La disciplina di protezione delle banche di dati è stata introdotta con la direttiva 96/9/CE (G.U.C.E. del 27 marzo 1996, n. L 077) concernente la protezione legale delle banche di dati, poi attuata a livello nazionale con il D.Lgs. 6 maggio 1999, n. 169 (G.U. del 15 giugno 1999, n. 138).

Il legislatore europeo, inserendosi nel solco già tracciato a livello internazionale, ancora una volta ha optato per un inquadramento del nuovo bene giuridico fra le opere dell'ingegno tutelate dal diritto d'autore.

Il D.Lgs. 169/1999 ha così nuovamente novellato il testo della l.d.a., modificandone l'art. 1 per inserirvi «le banche di dati che per la scelta o la disposizione del materiale costituiscono una creazione intellettuale dell'autore». La formulazione consente di individuare due tipi di banche di dati tutelabili: quelle in cui i contenuti sono stati selezionati in modo originale dall'autore (cc.dd. banche di dati selettive), e quelle in cui, pur non risultando creativa tale selezione, risulti originale la disposizione dei materiali all'interno dell'opera (cc.dd. banche di dati non selettive).

In ossequio al generale principio che vede tutelata unicamente la forma espressiva dell'opera dell'ingegno, la tutela della banca di dati in base al diritto d'autore non si estende al suo contenuto e lascia impregiudicati i diritti esistenti sullo stesso. Della banca di dati, quale opera dell'ingegno, sarà pertanto protetta la sola forma espressiva rappresentata dalla sua struttura²⁵.

A differenza di quanto avvenuto in materia di programmi per elaboratore, il legislatore comunitario ha introdotto una specifica definizione normativa di banca di dati, inserita dal D.Lgs. 169/1999 nell'art. 2, n. 9, l.d.a.: «una raccolta di opere, dati o altri elementi indipendenti sistematicamente o metodicamente disposti ed individualmente accessibili grazie a mezzi elettronici o in altro modo». La definizione risulta articolata e comprende sia le banche di dati elettroniche,

20 febbraio 2002, è stata bocciata il 6 luglio 2005 dal Parlamento europeo a larghissima maggioranza.

²⁵ Si noti come il legislatore, per la banca di dati, non abbia ripercorso quanto fatto all'atto dell'introduzione fra le opere dell'ingegno dei programmi per elaboratore, espressamente equiparati alle opere letterarie ai fini della loro protezione.

sia le banche di dati di altro tipo (segnatamente cartaceo), sebbene la disciplina tradisca in diversi suoi contenuti l'originaria impostazione, inizialmente pensata per le sole banche di dati elettroniche.

In relazione al concetto di «indipendenza» contenuto nella definizione, questo pare potersi ricavare a contrario: il requisito dell'indipendenza degli elementi di una banca di dati non sussisterà laddove fra loro sia riscontrabile una correlazione simile a quella esistente fra gli elementi inseriti in opere come quella audiovisiva, cinematografica, letteraria o musicale, correlazione che fa acquistare significato ad elementi (fotogrammi, note, ecc.) altrimenti privi di particolare valore se singolarmente considerati (cfr. Considerando n. 17 della direttiva 96/9/CE).

In merito all'ulteriore requisito di una disposizione sistematica o metodica degli elementi, questo vale certamente ad escludere raccolte non ordinate o puramente casuali di elementi. Come chiarito nel Considerando n. 21 della direttiva 96/9/CE, non si richiede, però, che i dati siano anche «fisicamente» memorizzati in forma organizzata, risultando sufficiente che i materiali siano ordinati in uno o più indici, o che siano accompagnati da codici che ne consentano la catalogazione e il reperimento secondo un criterio prestabilito, o che siano coordinati secondo collegamenti di tipo ipertestuale.

Infine, l'accessibilità individuale dei dati è da intendersi come possibilità di accedere alla singola informazione in modo diretto e consente di distinguere le banche di dati dalle semplici raccolte di dati.

Anche per la banca di dati l'accesso alla tutela del diritto d'autore richiederà la verifica del ricorrere dell'originalità dell'opera e cioè che la banca di dati risulti quale creazione dell'ingegno propria dell'autore (cfr. art. 3, comma 1, direttiva 96/9/CE)²⁶.

L'originalità della banca di dati potrà risultare dalla scelta dei materiali inseriti nell'opera, avendo riguardo ad eventuali precedenti raccolte del medesimo tipo, oppure dalla originale «disposizione del materiale», purché questa risulti sistematica o metodica.

Sulla ricostruzione del significato da attribuire al concetto di «disposizione del materiale» soccorre l'esperienza maturata in ambito statunitense, alla quale il legislatore europeo si è ispirato.

In particolare, il termine “disposizione” può essere ricondotto ai concetti di “coordination” (coordinamento) e “arrangement” (organizzazione) rinvenibili nel *Title 17, Sect. 101* dell'*US Code*, così come modificato dal *Copyright Act* del

²⁶ La formulazione, ripresa nell'art. 1 l.d.a. («creazione intellettuale dell'autore»), non è diversa da quella adottata in riferimento ai programmi per elaboratore: dunque, anche in questo caso si tratterebbe di un'originalità di tipo soggettivo.

1976. Secondo l'elaborazione dottrinale e giurisprudenziale statunitense, l'elemento del "coordinamento" ricorrerebbe quando si siano creati una serie di collegamenti a struttura reticolare fra i dati (per mezzo, ad esempio, dell'inserimento di rinvii, note, ecc.), mentre l'"organizzazione" sarebbe da ricercarsi in un determinato ordine sequenziale di disposizione dei dati (come, ad esempio, un ordine cronologico, tematico, ecc.).

In base a questa ricostruzione, il concetto di «disposizione del materiale» comprenderebbe il requisito del coordinamento e/o dell'organizzazione dei dati, risultando la mancanza assoluta di entrambi come ostativa alla protezione della banca di dati quale opera dell'ingegno.

Va verificato, però, come tale concetto possa essere applicato in particolare alle banche di dati elettroniche.

Queste, infatti, da un punto di vista informatico (ed operando una semplificazione utile ai nostri scopi) si presentano normalmente composte da tre fondamentali elementi: la struttura fisica di memorizzazione dei dati (primo livello), lo schema (secondo livello) e i programmi utilizzati per la fruizione della banca di dati (terzo livello). Tra l'utente-fruitori della banca di dati e le memorie contenenti fisicamente i dati (la struttura fisica della banca di dati) viene interposto uno "schema", che altro non è che un programma realizzato in un apposito linguaggio. Quando un utente inoltra una richiesta di accesso ad una data informazione attraverso il programma di gestione della banca di dati elettronica, questa viene interpretata ed evasa dal *Data Base Management System-DBMS* in base allo schema: è quest'ultimo che indirizzerà il sistema verso il dato richiesto.

In realtà, infatti, i dati contenuti nella struttura fisica di una banca di dati elettronica non rispettano alcuna particolare disposizione: in questo caso è lo schema (cioè un software) a dare forma a una data disposizione dei materiali e non la struttura fisica di memorizzazione.

Si può ulteriormente distinguere fra il programma preposto alla organizzazione e coordinamento dei dati (lo schema, appunto) e i programmi destinati a fare da interfaccia con l'utente per consentirgli di fruire della banca di dati (che abbiamo indicato come terzo livello della banca di dati elettronica): questi ultimi potranno essere differenti, pur rimanendo immutato lo schema.

Alla luce di quanto esposto, risulta necessario interpretare il requisito (di accesso alla tutela) dell'organizzazione e del coordinamento di una banca di dati elettronica (cioè la «disposizione del materiale») in connessione non con la struttura fisica dei dati, bensì con la componente software che abbiamo definito come lo schema.

Le disposizioni di cui agli artt. 1, comma 3, e 2, lett. a), della direttiva 96/9/CE, che parrebbero escludere dalla protezione riservata alla banca di dati

elettronica le sue componenti software in quanto tali, devono essere interpretate tenendo presente quanto appena accennato; cioè vanno intese necessariamente nel senso che solo le componenti software finalizzate alla “costituzione” della banca di dati e al suo “funzionamento” sono escluse dalla tutela, mentre invece i programmi per elaboratore intrinsecamente legati al contenuto stesso della banca di dati (lo schema) vi rientrano a pieno titolo.

Questa interpretazione, che consente di salvaguardare il contenuto delle norme in commento, risulta avallata dal testo del Considerando n. 20 della direttiva 96/9/CE, dove si rinviene un chiaro riferimento all’interdipendenza tra tutela della banca di dati e tutela dei suoi algoritmi ipertestuali e di interrogazione ed estrazione: «la tutela prevista dalla presente direttiva può applicarsi anche agli elementi necessari per il funzionamento o la consultazione di determinate banche di dati, come ad esempio il tesoro e i sistemi di indicizzazione».

Analizzato cosa debba intendersi per originalità della banca di dati, vediamo ora brevemente il regime di tutela.

La titolarità dei diritti d’autore sulla banca di dati, così come per il software, spetterà all’autore di questa, secondo i generali principi sanciti nei primi articoli della l.d.a.

Essendo la banca di dati tipicamente un’opera plurisoggettiva, alla cui creazione collaborano normalmente più soggetti, anche in questo caso i diritti d’autore potranno appartenere a colui che ha coordinato la realizzazione della banca di dati, se opera collettiva, oppure congiuntamente a tutti i coautori, se opera in comunione. Potrà, inoltre, trovare applicazione l’art. 4 l.d.a. laddove la banca di dati si presenti quale opera creativa frutto dell’elaborazione di opere preesistenti.

Si è visto come in ambito nazionale il diritto d’autore sia attribuito in via generale a persone fisiche e le ipotesi di titolarità *ab origine* in capo a persone giuridiche costituiscono un’eccezione. Fra queste va annoverata l’ipotesi ora disciplinata dal già ricordato art. 12-*bis* l.d.a., così come da ultimo modificato dal D.Lgs. 169/1999: la norma dispone che i diritti di utilizzazione economica sulle banche di dati create dal lavoratore dipendente, in esecuzione delle sue mansioni o su istruzioni impartite dal datore di lavoro, spettino a quest’ultimo.

In merito al diritto morale, la sua titolarità rimarrà, in ogni caso, in capo al singolo autore persona fisica, oppure alle persone fisiche qualificate come autori secondo le disposizioni relative all’eventuale specie di opera plurisoggettiva a cui la banca di dati apparterrà.

Il contenuto dei diritti patrimoniali sulla banca di dati è disciplinato dall’art. 64-*quinquies*, l.d.a., così come introdotto dal D.Lgs. 169/1999.

Sulla propria banca di dati, all’autore è riconosciuto il diritto esclusivo di eseguire o autorizzare:

- la riproduzione permanente o temporanea, totale o parziale, con qualsiasi mezzo e in qualsiasi forma;
- la sua traduzione, il suo adattamento, una sua diversa disposizione e ogni altra modifica, oltre a qualsiasi riproduzione, distribuzione, comunicazione, presentazione o dimostrazione in pubblico dei risultati di queste operazioni;
- qualsiasi forma di distribuzione al pubblico dell'originale o di copie della banca di dati;
- qualsiasi presentazione, dimostrazione o comunicazione al pubblico della banca di dati, ivi compresa la sua trasmissione effettuata con qualsiasi mezzo e in qualsiasi forma.

Anche il contenuto dei diritti patrimoniali riservati all'autore della banca di dati va naturalmente interpretato alla luce della ridefinizione dei concetti di «riproduzione», «comunicazione al pubblico» e «distribuzione» operata dal D.Lgs. 68/2003 di attuazione della direttiva 2001/29/CE di cui si è dato conto.

A tal proposito, si noti come quanto da ultimo stabilito in materia di non operatività del principio dell'esaurimento in relazione ai diritti di comunicazione al pubblico (che comprende la messa a disposizione del pubblico) e di distribuzione, in via generale e per qualunque opera sia trasmessa attraverso la rete Internet, sia stato preceduto da disposizione analoga a suo tempo introdotta proprio dalla direttiva 96/9/CE per le banche di dati. In riferimento alla consultazione *on-line* delle banche di dati elettroniche, la direttiva in parola ha stabilito, infatti, come la trasmissione *on-line* di una banca di dati non costituisca una consegna di beni (nemmeno nel caso l'utente sia autorizzato ad un *download* della banca di dati, cioè a memorizzarne una copia), bensì una «prestazione di servizi», risultando pertanto sottratta al principio dell'esaurimento (cfr. Considerando n. 33 della direttiva 96/9/CE).

Quanto indicato dal legislatore comunitario ha trovato un puntuale riscontro nella disciplina nazionale: l'art. 64-*quinquies*, lett. c), l.d.a. attribuisce all'autore della banca di dati il diritto esclusivo di distribuzione al pubblico dell'originale o di copie della banca di dati e limita l'applicazione del principio dell'esaurimento comunitario solo all'ipotesi della «prima vendita di una copia nel territorio dell'UE da parte del titolare del diritto o con il suo consenso».

In relazione alle prerogative dell'autore della banca di dati previste dall'art. 64 *quinquies* l.d.a., il D.Lgs. 169/1999 ha altresì specificatamente previsto come non siano soggette ad autorizzazione da parte del titolare dei diritti (art. 64-*sexies* l.d.a.):

- l'accesso o la consultazione della banca di dati quando abbiano esclusivamente finalità didattiche o di ricerca scientifica, non svolte nell'ambito di una impresa e nei limiti di quanto giustificato dallo scopo non commerciale perse-

guito, purché si indichi la fonte. Se l'operazione comporta, però, la riproduzione permanente della totalità o di una parte sostanziale del contenuto, tale attività sarà soggetta all'autorizzazione dell'eventuale relativo titolare del diritto del costituente²⁷;

– l'impiego della banca di dati per fini di sicurezza pubblica o per effetto di una procedura amministrativa o giurisdizionale;

– per l'utente legittimo, la riproduzione permanente o temporanea, totale o parziale, con qualsiasi mezzo e in qualsiasi forma della banca di dati, qualsiasi presentazione, dimostrazione o comunicazione in pubblico della banca di dati, ivi compresa la trasmissione effettuata con qualsiasi mezzo e in qualsiasi forma, nonché qualsiasi riproduzione, distribuzione, comunicazione, presentazione o dimostrazione in pubblico dei risultati delle operazioni di traduzione, di adattamento, di una diversa disposizione e di ogni altra modifica, se tali attività sono necessarie per l'accesso al contenuto della stessa banca di dati e per il suo normale impiego. L'utente legittimo, autorizzato a utilizzare solo una parte della banca di dati, potrà naturalmente porre in essere le attività ora indicate in riferimento esclusivamente alla porzione di banca di dati per la quale è stato autorizzato all'utilizzo (art. 64-*sexies*, comma 2, l.d.a.). Le clausole contrattuali eventualmente pattuite in violazione di queste facoltà sono da considerarsi nulle ai sensi dell'art. 1418 c.c. (art. 64-*sexies*, comma 3, l.d.a.).

A queste ipotesi, lo si ricorda, si aggiungono oggi anche quelle relative al c.d. *data mining* previste dagli artt. 70-*ter*, 70-*quater* e 70-*septies* l.d.a., di cui si è detto al precedente § 5.

L'ultimo comma dell'art. 64-*sexies*, l.d.a. chiarisce come le disposizioni contenute in detto articolo «non possono essere interpretate in modo da consentire che la loro applicazione arrechi indebitamente pregiudizio al titolare del diritto o entri in conflitto con il normale impiego della banca di dati».

Va qui notato come il legislatore italiano, nel dare attuazione alla direttiva 96/9/CE con il D.Lgs. 169/1999, abbia ritenuto di limitare i casi di libera utilizzazione in merito alle banche di dati, operando in materia una scelta restrittiva rispetto alle facoltà riservate agli Stati membri dalla direttiva comunitaria. Nel D.Lgs. 169/1999 non ritroviamo attuata, ad esempio, la disposizione che fa riferimento alla deroga relativa alla libera utilizzazione «per fini privati di una banca di dati non elettronica» (art. 6, comma 2, lett. a, della direttiva 96/9/CE).

Per quanto attiene all'impiego della banca di dati per «finalità didattiche o di ricerca scientifica», la norma comunitaria esclude l'applicazione del principio dell'autorizzazione «sempre che l'utente legittimo indichi la fonte dalla quale i

²⁷ In merito, si veda il successivo § 7.3.

dati informativi sono stati tratti e la loro utilizzazione sia limitata a quanto giustificato dallo scopo non commerciale perseguito», ma, a differenza di quanto indicato nell'art. 64-*sexies* l.d.a., non subordina tale impiego a qualsivoglia autORIZZAZIONE nel caso questo includa la riproduzione permanente della totalità o di una parte sostanziale del contenuto della banca di dati (cioè interferisca con il «diritto del costitutore», di cui si dirà a seguire).

7.3. Il diritto del costitutore di una banca di dati

Si è detto come l'applicabilità anche alle banche di dati (così come al software) della tutela d'autore fosse stata sostenuta, sia dalla dottrina sia dalla giurisprudenza, già prima del loro espresso inserimento fra i generi di opere dell'ingegno protette. Il legislatore, confermando il diritto d'autore quale regime di protezione della forma espressiva della banca di dati, si è dunque inserito in un solco da tempo ampiamente tracciato. Tuttavia, le esigenze del settore delle banche di dati, in particolare elettroniche, non avrebbero potuto trovare un adeguato riscontro solo in tale tipo di tutela. Molte delle banche di dati elettroniche realizzate già a partire dai primi anni ottanta risultavano (e sempre più risultano oggi) prive di qualunque originalità, seppure intesa quale semplice riconoscibilità dell'impronta personale dell'autore. Spesso una qualsivoglia selezione dei materiali era (ed è) tendenzialmente assente, in quanto, sfruttando le sempre più significative capacità di memorizzazione e gestione informatica dei dati, le banche di dati si caratterizzavano per la loro tendenziale esaustività.

Dunque, le banche di dati andavano sempre più contraddistinguendosi non per la loro originalità nella scelta e/o disposizione dei materiali, bensì per lo sforzo necessario a reperirne e predisporne i contenuti, rappresentati tipicamente da un insieme di informazioni e dati. L'esigenza di poter garantire una protezione non solo all'eventuale sforzo creativo dell'autore, ma anche e soprattutto all'investimento economico e di risorse necessario per la realizzazione stessa della banca di dati (quand'anche questa non fosse risultata creativa), si andava appalesando vieppiù come un requisito indispensabile per lo stesso sviluppo del mercato dell'editoria elettronica.

A tali istanze il legislatore comunitario ha dato risposta con la già citata direttiva 96/9/CE. Infatti, non solo, come abbiamo visto, le banche di dati sono state ammesse espressamente a godere della protezione offerta dal diritto d'autore, ma è stato altresì introdotto un nuovo diritto, attribuito al «costitutore» di una banca di dati, volto a tutelare l'investimento necessario per realizzarla, verificarla o presentarla, attraverso una protezione del contenuto stesso della banca di dati. Proprio questo diritto *sui generis* (secondo l'espressione scelta dal legislatore comunitario) o diritto del costitutore (secondo la locuzione adottata dal

D.Lgs. 169/1999) rappresenta l'elemento più innovativo della disciplina a tutela delle banche di dati.

Un diritto, quello del costitutore, che si presenta del tutto indipendente dall'eventuale diritto d'autore esistente sulla medesima banca di dati e totalmente svincolato dalla sussistenza del requisito della creatività previsto per quest'ultimo.

L'obiettivo dichiarato del diritto *sui generis* è quello di tutelare il costitutore di una banca di dati, cioè il soggetto che «prende l'iniziativa e si assume il rischio di effettuare gli investimenti»²⁸, «contro l'appropriazione dei risultati ottenuti investendo nella ricerca e raccolta del contenuto della banca di dati»²⁹. Per questa ragione, la tutela mediante tale diritto non è applicabile a qualsiasi banca di dati, ma solo ed esclusivamente a quelle la cui realizzazione (in particolare per l'attività di costituzione, verifica o presentazione) abbia richiesto un «investimento rilevante sotto il profilo qualitativo o quantitativo», investimento che potrà consistere non solo nell'impegno di mezzi finanziari, ma anche di «tempo, lavoro ed energia» (Considerando n. 40 della direttiva 96/9/CE).

In ambito nazionale, la sua disciplina di dettaglio è ora contenuta nel Titolo II-*bis* l.d.a. (artt. 102-*bis* e 102-*ter*), introdotto dal D.Lgs. 169/1999³⁰.

Il «costitutore» è definito all'art. 102-*bis*, comma 1, l.d.a. come il «soggetto che effettua investimenti rilevanti per la realizzazione di una banca di dati, ovvero per la sua verifica o presentazione, impegnando a tal fine mezzi finanziari, tempo o lavoro»³¹.

L'esatta individuazione del significato da attribuire al concetto di «investimento rilevante» risulta di estrema importanza, non solo in quanto requisito di accesso alla tutela del diritto del costitutore, ma perché, come vedremo fra breve, può incidere anche sulla sua durata.

La valutazione sulla rilevanza dell'investimento si ritiene non debba essere

²⁸ Considerando n. 41 della direttiva 96/9/CE.

²⁹ Motivazioni del Consiglio, n. 14, lett. a) (G.U.C.E. 30 ottobre 1995, n. C 288, p. 26).

³⁰ La collocazione sistematica e le sue caratteristiche fanno propendere per un'assimilazione del diritto del costitutore ai diritti connessi, sebbene la dottrina non sia unanime sul punto.

³¹ Cosa si debba intendere per investimento collegato alla «realizzazione» di una banca di dati o viceversa alla «verifica» di essa è stato chiarito dalla stessa Corte di giustizia dell'UE: il primo «indica i mezzi destinati alla ricerca di elementi esistenti e alla loro raccolta nella detta banca di dati. Essa non comprende i mezzi impiegati per la creazione degli elementi costitutivi del contenuto di una banca di dati»; mentre la verifica del contenuto «riguarda i mezzi destinati, al fine di assicurare l'affidabilità dell'informazione contenuta nella detta banca di dati, al controllo dell'esattezza degli elementi ricercati, all'atto della costituzione di questa banca di dati nonché durante il periodo di funzionamento della stessa. I mezzi destinati ad operazioni di verifica nel corso della fase di creazione di elementi successivamente raccolti in una banca di dati non rientrano in questa nozione» (sentenza della Corte di giustizia dell'UE, 9 novembre 2004, procedimento C-203/02, *The British Horseracing Board Ltd e.a. c. William Hill Organization Ltd*).

effettuata in senso assoluto, bensì calibrata in rapporto al settore di appartenenza, al livello degli investimenti normalmente effettuati da altri soggetti appartenenti al medesimo settore o dal medesimo soggetto (in precedenza, in contemporanea ed anche successivamente) per operazioni analoghe.

Nella direttiva 96/9/CE si fa riferimento ad un «investimento rilevante» sotto il profilo «qualitativo o quantitativo» (art. 7, direttiva 96/9/CE). Il criterio “qualitativo” appare di difficile determinazione, non essendo specificato in cosa concretamente si sostanzia: potrebbe forse ritenersi che l’investimento possa dirsi in tal senso “rilevante” in considerazione della qualità dello sforzo di tipo organizzativo o intellettuale, o per la particolare complessità nel reperimento delle informazioni. Apparentemente di più facile determinazione sembra il criterio della rilevanza quantitativa, in relazione al quale, come ricordato, si dovranno tenere in considerazione il livello degli investimenti finanziari normalmente effettuati nel settore di appartenenza, lo sforzo organizzativo e di risorse umane mediamente impiegate per la realizzazione di quel determinato tipo di banca di dati, ecc.

Se ricorre l’investimento rilevante, al costituente sarà riservato il «diritto [...] di vietare le operazioni di estrazione ovvero reimpiego della totalità o di una parte sostanziale del contenuto della banca di dati» (art. 102-*bis*, comma 3, l.d.a.).

L’art. 102-*bis* l.d.a. definisce l’«estrazione» come «il trasferimento permanente o temporaneo della totalità o di una parte sostanziale del contenuto di una banca di dati su un altro supporto con qualsiasi mezzo o in qualsivoglia forma» (art. 102-*bis*, comma 1, lett. b, l.d.a.).

Per «reimpiego» si intende invece «qualsiasi forma di messa a disposizione del pubblico della totalità o di una parte sostanziale del contenuto della banca di dati mediante distribuzione di copie, noleggio, trasmissione effettuata con qualsiasi mezzo e in qualsiasi forma» (art. 102-*bis*, comma 1, lett. c, l.d.a.)³².

L’estrazione o il reimpiego ripetuti e sistematici, anche se aventi ad oggetto parti non sostanziali del contenuto della banca di dati, non sono comunque consentiti qualora presuppongano operazioni contrarie alla normale gestione della banca di dati o arrechino un pregiudizio ingiustificato al costituente (art. 102-*bis*, comma 9, l.d.a.).

³² Il contenuto ed il significato da attribuire alle nozioni di «estrazione» e «reimpiego» sono stati a loro volta chiariti dalla Corte di giustizia dell’UE: «Le nozioni di estrazione e di reimpiego [...] si riferiscono a qualsiasi operazione non autorizzata di appropriazione e di diffusione al pubblico di tutto il contenuto di una banca di dati o di una parte di essa. Queste nozioni non presuppongono un accesso diretto alla banca di dati di cui trattasi. Il fatto che il contenuto della banca di dati sia stato reso accessibile al pubblico dal costituente o con il suo consenso non pregiudica il diritto di quest’ultimo di vietare le operazioni di estrazione e/o di reimpiego relative alla totalità o ad una parte sostanziale del contenuto di una banca di dati» (sentenza della Corte di giustizia dell’UE, 9 novembre 2004, procedimento C-203/02, *The British Horseracing Board Ltd e.a. c. William Hill Organization Ltd*).

L'identificazione di cosa debba intendersi per «parte sostanziale del contenuto» di una banca di dati è questione a sua volta di estrema rilevanza, in quanto perno dell'intera disciplina, e pone problemi interpretativi di non immediata soluzione.

Sul punto il soccorso che viene dal legislatore è assai modesto, poiché questi fa di nuovo riferimento unicamente ad una valutazione che deve avvenire in termini «qualitativi o quantitativi».

In dottrina gli approcci in merito alla ricostruzione della nozione di parte sostanziale sono stati diversi, stante l'apparente elasticità dei suddetti criteri.

A chiarire (in parte) il significato di tale locuzione è stata, ancora una volta, la Corte di giustizia dell'UE, la quale, in una vertenza avente ad oggetto il diritto *sui generis*, ha avuto modo di chiarire come: «La nozione di parte sostanziale, valutata sotto il profilo quantitativo, [...] si riferisce al volume dei dati estratti e/o reimpiegati della banca di dati e deve essere valutata in relazione al volume del contenuto totale della banca di dati»; mentre «la nozione di parte sostanziale, valutata sotto il profilo qualitativo, [...] si riferisce alla rilevanza dell'investimento collegato al conseguimento, alla verifica o alla presentazione del contenuto dell'oggetto dell'operazione di estrazione o di reimpiego, indipendentemente dal fatto che tale oggetto rappresenti una parte quantitativamente sostanziale del contenuto generale della banca di dati tutelata»³³.

Il legislatore nazionale, in ottemperanza a quanto stabilito nella direttiva 96/9/CE, ha esplicitato come il diritto del costituente sussista a prescindere «dalla tutelabilità della banca di dati a norma del diritto d'autore o di altri diritti» e comunque «senza pregiudizio dei diritti sul contenuto o su parti di esso» (art. 102-*bis*, comma 3, l.d.a.).

Il diritto è riconosciuto ai soli cittadini di uno Stato membro dell'UE o residenti abituali nel territorio della stessa (art. 102-*bis*, comma 4, l.d.a.). Qualora il costituente sia un'impresa o società, al fine di accertare la sussistenza del diritto occorre verificare che la stessa sia stata costituita secondo la normativa di uno Stato membro dell'UE e che abbia la sede sociale, l'amministrazione centrale o il centro d'attività principale all'interno dell'Unione; qualora la società o l'impresa abbia all'interno dell'UE soltanto la propria sede sociale, deve sussistere un legame effettivo e continuo tra l'attività della medesima e l'economia di uno degli Stati membri (art. 102-*bis*, comma 5, l.d.a.).

Al diritto del costituente si applica il principio dell'esaurimento comunitario: l'art. 102-*bis*, comma 2, l.d.a. stabilisce come la prima vendita di una copia della

³³ Sentenza della Corte di giustizia dell'UE, 9 novembre 2004, procedimento C-203/02, *The British Horseracing Board Ltd e.a. c. William Hill Organization Ltd*.

banca di dati effettuata o consentita dal titolare del diritto del costituente in uno Stato membro dell'UE esaurisca il diritto di controllare la rivendita della copia nel territorio dell'Unione.

Infine, il comma 10 dell'art. 102-*bis* l.d.a. esplicita come il diritto del costituente possa essere acquistato o trasmesso in tutti i modi e forme consentiti dalla legge.

Il termine di durata fissato per il diritto del costituente è di quindici anni, da computarsi dal 1° gennaio dell'anno successivo alla data di completamento della costituzione della banca di dati. Per le banche di dati in qualunque modo messe a disposizione del pubblico prima dello scadere di detto periodo, il diritto del costituente si estinguerà trascorsi quindici anni dal 1° gennaio dell'anno successivo alla data della prima messa a disposizione del pubblico (art. 102-*bis*, commi 5 e 6, l.d.a.). I due termini paiono potersi cumulare fra loro, consentendo così al diritto del costituente di poter durare teoricamente sino ad un massimo di circa 30 anni dalla data di completamento della costituzione della banca di dati.

Nel caso, però, in cui vengano «apportate al contenuto della banca di dati modifiche o integrazioni sostanziali comportanti nuovi investimenti rilevanti», un autonomo termine di durata della protezione (di ulteriori 15 anni) decorrerà «dal momento del completamento o della prima messa a disposizione del pubblico della banca di dati così modificata o integrata, e come tale espressamente identificata» (art 102-*bis*, comma 8, l.d.a.).

In merito, resta da capire se, in tale ultima ipotesi, il nuovo termine di protezione investirà l'intera banca di dati o viceversa unicamente le parti nuove o modificate che abbiano richiesto un investimento rilevante per la loro realizzazione; o ancora se si possa ritenere che la rinnovata tutela si debba applicare integralmente alla banca di dati così come revisionata o modificata attraverso un nuovo investimento rilevante, ma che nel contempo divenga liberamente utilizzabile (allo scadere del relativo termine di protezione) la precedente versione, dalla quale sarà dunque lecito estrarre e reimpiegare anche parti sostanziali del suo contenuto, sebbene eventualmente in parte coincidente con quello della nuova versione della banca di dati³⁴. Quest'ultima interpretazione, in particolare, avrebbe il pregio di limitare la portata della disposizione in parola e di evitare possibili effetti distorsivi in termini di appropriazione definitiva dei contenuti e ostacolo alla loro circolazione. Il regime adottato in merito alla durata del diritto del costituente, infatti, è stato da subito criticato per il rischio che possa divenire uno strumento per conservare nel tempo, potenzialmente all'infinito, le relative prerogative, in contrasto con il generale principio

³⁴ M. BERTANI, *Impresa culturale e diritti d'esclusiva*, Milano: Giuffrè, 2000, pp. 356 ss.

di limitazione temporale nella durata delle privative patrimoniali nel diritto d'autore.

Le attività consentite all'utente legittimo della banca di dati sul suo contenuto, attività non soggette all'autorizzazione del titolare del diritto del costituente, sono previste all'art. 102-ter l.d.a.: il costituente di una banca di dati messa per qualsiasi motivo a disposizione del pubblico non può impedire le attività di «estrazione o reimpiego di parti non sostanziali, valutate in termini qualitativi e quantitativi, del contenuto della banca di dati per qualsivoglia fine effettuate dall'utente legittimo». Nel caso in cui l'utente sia autorizzato ad estrarre o reimpiegare soltanto una parte della banca di dati, la norma citata si applicherà solo a quella specifica parte della banca di dati. Le eventuali clausole contrattuali pattuite in violazione di dette possibilità sono da considerarsi nulle (art. 102-ter, comma 3, l.d.a.).

In relazione a queste facoltà dell'utilizzatore legittimo riemerge l'importanza del concetto di «parte sostanziale del contenuto» e dei criteri qualitativi e quantitativi che dovrebbero consentirne l'identificazione.

L'utente legittimo di una banca di dati messa in qualsiasi modo a disposizione del pubblico sarà comunque soggetto ad una limitazione di ordine generale, che consiste nel non poter «eseguire operazioni che siano in contrasto con la normale gestione della banca di dati o che arrecchino un ingiustificato pregiudizio al costituente della banca di dati», così come nel non dover arrecare «pregiudizio al titolare del diritto d'autore o di un altro diritto connesso relativo ad opere o prestazioni contenute in tale banca» (art. 102-ter l.d.a.).

Tra gli atti non soggetti al principio del previo consenso del costituente vi è il prestito al pubblico, quando effettuato dalle biblioteche e discoteche dello Stato e degli enti pubblici, il quale non costituisce in alcun caso, per espressa previsione, un atto di estrazione o di reimpiego (art. 102-bis, comma 1, lett. b e lett. c, l.d.a.).

L'art. 71-decies l.d.a., così come introdotto dal D.Lgs. 68/2003, ha inoltre previsto espressamente come le eccezioni e limitazioni al diritto d'autore contenute nel Capo V, Titolo I, della l.d.a. si applichino anche al diritto del costituente. Tale scelta è stata accolta favorevolmente, in quanto, all'indomani dell'emanazione della direttiva 96/9/CE, le preoccupazioni dei commentatori si concentrarono proprio sui possibili effetti monopolistici del diritto del costituente. Un'applicazione rigida delle disposizioni contenute nel testo comunitario, accompagnate dalla riaffermazione del diritto d'autore come *ius excludendi*, faceva temere che il diritto del costituente potesse divenire uno strumento per imporre una "esclusiva sulle idee", capace di frenare la creazione di nuovi prodotti e quindi, in definitiva, di limitare non solo la libera concorrenza, ma ancor prima la circolazione del sapere.

Il riferimento alla «parte sostanziale» oggetto di estrazione o reimpiego (così come la previsione di deroghe al diritto in esame previste dall'art. 9 della direttiva 96/9/CE), rivela come la tutela concessa dalla direttiva 96/9/CE non voglia, in realtà, importare pericolose forme di monopolio sull'informazione, in quanto ciò che si tutela non è il contenuto della banca dati in quanto tale («il diritto di impedire l'estrazione e/o il reimpiego non autorizzati non costituisce in alcun modo un'estensione della tutela del diritto d'autore a semplici fatti o dati», Considerando n. 45 della direttiva 96/9/CE), ma il contenuto in quanto frutto di un investimento che chiede di essere remunerato. La stessa preoccupazione emerge anche nel Considerando n. 47 della direttiva 96/9/CE, dove si ribadisce come «la protezione sulla base del diritto «sui generis» non deve essere esercitata in modo tale da favorire gli abusi di posizione dominante, con particolare riguardo alla creazione e diffusione di nuovi prodotti e servizi a valore aggiunto di ordine intellettuale, documentale, tecnico, economico o commerciale».

Pertanto, alla luce delle indicazioni del legislatore europeo e, in particolare, del contenuto del Considerando n. 46 della stessa direttiva 96/9/CE³⁵, il diritto *sui generis* dovrebbe insistere sull'esito degli investimenti rilevanti per la costituzione della banca di dati o di una sua parte e non, invece, sulle diverse informazioni contenute nella banca di dati stessa³⁶.

³⁵ «L'esistenza di un diritto di impedire l'estrazione e/o il reimpiego non autorizzati della totalità o di una parte sostanziale di opere, dati o elementi di una banca di dati non dà luogo alla creazione di un nuovo diritto su queste stesse opere, dati o elementi», Considerando n. 46 della direttiva 96/9/CE.

³⁶ La giurisprudenza di merito italiana ha identificato il diritto *sui generis* come il «diritto sull'insieme dei contenuti (quali elementi preesistenti alla stessa banca di dati)» (Trib. Catania, 8 gennaio 2001, in *AIDA* 2001, 796, p. 610 ss., con note di M. BERTANI, p. 614).

LA REGOLAZIONE DELL'INTELLIGENZA ARTIFICIALE NELL'UE: L'AI ACT

Giuseppe Contissa, Marco Billi

SOMMARIO: 1. L'intelligenza artificiale tra etica e diritto. 2. La legge sull'IA e l'approccio basato sul rischio. 2.1. Definizione di intelligenza artificiale. 2.2. Pratiche vietate. 3. Sistemi ad alto rischio. 3.1. Classificazione. 3.2. Requisiti essenziali. 3.3. La procedura di valutazione della conformità. 3.4. La valutazione d'impatto sui diritti fondamentali. 3.5. Sistemi a basso rischio. 4. La regolamentazione dei modelli di IA con finalità generali. 5. Applicazione e sanzioni. 6. Spazi di sperimentazione normativa.

1. L'intelligenza artificiale tra etica e diritto

Negli ultimi anni, l'Intelligenza Artificiale (IA) ha visto una rapida crescita in diversi ambiti della vita sociale. Le tecnologie e i sistemi basati su IA sono sempre più utilizzati non solo in settori tecnologici altamente specializzati, ma anche in prodotti e servizi di uso comune che coinvolgono un'ampia gamma di attività personali, sociali, e produttive.

A fronte degli enormi vantaggi, l'impiego di queste tecnologie comporta una serie di rischi per i diritti e le libertà fondamentali, così come per la salute e la sicurezza.

Le istituzioni europee hanno quindi riconosciuto la necessità di elaborare una base normativa comune che tenga conto delle implicazioni umane, etiche e socioeconomiche dell'IA in linea con i principi e i valori europei.

A partire dal 2017, sono state avviate diverse iniziative volte a definire i contenuti di tale quadro regolatorio, inserite all'interno di un programma più ampio che comprende anche la disciplina della gestione dei dati, del mercato digitale e della robotica. In particolare, il Consiglio europeo dell'ottobre 2017 ha sottolineato l'urgenza di affrontare le nuove tendenze tecnologiche, tra cui l'intelligenza artificiale, garantendo al contempo un elevato livello di protezione

dei dati, dei diritti digitali e degli standard etici, invitando la Commissione a elaborare un approccio europeo all'IA¹.

Nell'aprile 2018, la Commissione europea ha presentato una "Strategia europea sull'IA"² incentrata su tre aree principali: (1) la promozione della ricerca, dello sviluppo tecnologico e delle applicazioni industriali relative all'IA; (2) il sostegno al quadro socioeconomico interessato da questi sviluppi tecnologici; (3) la definizione di un «quadro etico e giuridico adeguato basato sui valori dell'Unione e coerente con la Carta dei diritti fondamentali dell'Unione europea».

Parallelamente, la Commissione ha istituito un "gruppo di esperti di alto livello" sull'IA, che nell'aprile 2019 ha pubblicato gli "Orientamenti etici per un'IA affidabile"³. Il documento identifica tre principi fondamentali per un'IA affidabile: liceità, etica e robustezza. Sulla base di questi principi, il gruppo di esperti ha individuato i sette requisiti che un sistema di IA affidabile dovrebbe soddisfare:

1. Azione e sorveglianza umane: garantire che i sistemi di IA responsabilizzino gli esseri umani, consentendo loro di prendere decisioni informate.
2. Robustezza tecnica e sicurezza: garantire l'affidabilità e la sicurezza dei sistemi di IA per prevenire danni.
3. Riservatezza e governance dei dati: proteggere i dati delle persone e garantire il mantenimento della privacy durante tutto il ciclo di vita del sistema di IA.
4. Trasparenza: promuovere la comprensibilità e l'accessibilità delle operazioni e dei processi decisionali dei sistemi di IA, al fine di rafforzare la fiducia e la consapevolezza degli utenti.
5. Diversità, non discriminazione ed equità: garantire che i sistemi di IA trattino tutte le persone in modo equo e non perpetuino pregiudizi.
6. Benessere sociale e ambientale: garantire che l'IA contribuisca positivamente alla società e all'ambiente.
7. Responsabilità: istituire meccanismi per garantire la responsabilità e l'accountability dei sistemi di IA e dei loro risultati.

¹ Conclusioni del Consiglio Europeo di Bruxelles, 19 Ottobre 2017 (OR. en) EUCO 14/17 CO EUR 17 CONCL 5 <http://data.consilium.europa.eu/doc/document/ST-14-2017-INIT/-en/pdf>

² Commissione europea, Comunicazione «Intelligenza artificiale per l'Europa», COM/2018/-237 definitivo.

³ Gruppo di esperti di alto livello della Commissione europea sull'IA affidabile, Orientamenti etici per un'IA affidabile, 2019.

Seguendo queste linee guida, nel febbraio 2020 la Commissione europea ha pubblicato il Libro bianco sull'intelligenza artificiale⁴. Il documento descrive in dettaglio le opzioni strategiche definite nel 2018, integrando l'obiettivo di una tecnologia affidabile con la promozione dell'"eccellenza" europea nella ricerca e nell'industria. Per quanto riguarda il quadro giuridico, il Libro bianco dà priorità agli interventi sui diritti fondamentali e sulla governance dei dati, sulla sicurezza e la responsabilità, sull'armonizzazione e su una legislazione efficace.

2. La legge sull'IA e l'approccio basato sul rischio

Al termine del percorso sintetizzato nella sezione precedente, il 21 aprile 2021, la Commissione europea ha proposto un regolamento che stabilisce norme armonizzate in materia di intelligenza artificiale⁵. La proposta ha seguito un laborioso iter legislativo fino al cosiddetto trilogio, in cui i rappresentanti del Parlamento europeo, del Consiglio dell'Unione europea e della Commissione europea hanno negoziato per raggiungere un accordo definitivo. Dopo discussioni su molti punti controversi, è stato infine adottato dal Parlamento europeo il 14 marzo 2024 e pubblicato il 12 luglio 2024 nella Gazzetta ufficiale dell'UE come regolamento (UE) 2024/1689⁶.

Il Regolamento 2024/1689 (regolamento sull'intelligenza artificiale o "AI Act") adotta un "approccio basato sul rischio"⁷ poiché punta a prevenire e mitigare i rischi derivanti dall'uso dell'IA. Tipicamente, allo scopo di determinare le norme applicabili, una regolamentazione basata sul rischio tiene conto sia del livello del rischio (es. alto, medio, basso), sia delle caratteristiche del rischio correlato a una specifica pratica o utilizzo a cui è destinato il bene oggetto di regolazione. Almeno in linea di principio, i vincoli e i requisiti stabiliti dalla legge dovrebbero applicarsi solo nella misura necessaria a prevenire o mitigare tali rischi.

⁴ Commissione europea, Libro bianco sull'intelligenza artificiale – Un approccio europeo all'eccellenza e alla fiducia, COM 2020, 65 definitivo.

⁵ Commissione europea, Proposta di regolamento che stabilisce norme armonizzate in materia di intelligenza artificiale (Legge sull'intelligenza artificiale); COM (2021) 206 definitivo.

⁶ Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce norme armonizzate in materia di intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e delle direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828.

⁷ Per una prospettiva più ampia sull'approccio basato sul rischio della legge sull'IA, T. MAHLER, *Between Risk Management and Proportionality: The Risk-Based Approach in the EU's Artificial Intelligence Act Proposal*, in *Nordic Yearbook of Law and Informatics*, 2021; M. EBERS, *Truly Risk-Based Regulation of Artificial Intelligence-How to Implement the EU's AI Act*, 2024, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4870387.

Seguendo questo approccio, il regolamento distingue quattro livelli di rischio per i sistemi di IA per scopi specifici e due livelli di rischio per i sistemi di IA per finalità generali, ciascuno associato a regimi giuridici diversi.

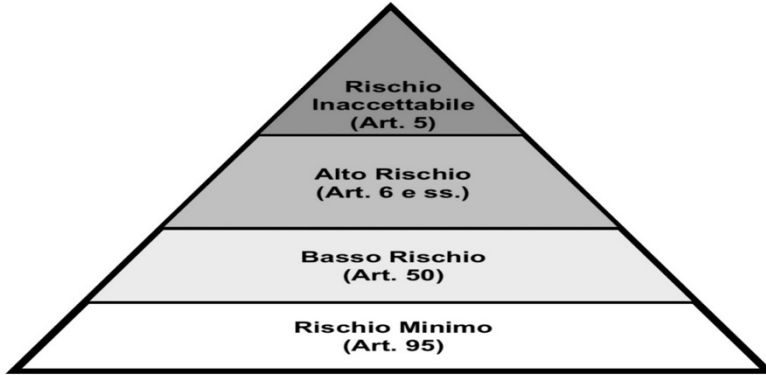


Fig. 1. La piramide del rischio

Il primo livello è rappresentato da alcune pratiche (cioè, impiego dei sistemi di IA) che sono considerate così critiche per il rischio che implicano, da dover essere vietate. Il regolamento non assegna esplicitamente un livello di rischio a queste pratiche, ma dal punto di vista della gestione del rischio si potrebbe dire che presentano rischi “inaccettabili” a causa del loro livello eccessivo.

A un livello inferiore si trovano i sistemi di IA “ad alto rischio”. Si tratta di sistemi che comportano rischi significativi per la salute, la sicurezza e i diritti fondamentali delle persone. I sistemi di IA ad alto rischio sono soggetti a severi requisiti normativi, come l’obbligo per il fornitore di conformarsi ad alcuni requisiti essenziali.

Al terzo livello si trovano i sistemi di IA “a basso rischio”. Questi sistemi presentano un rischio inferiore rispetto ai sistemi di IA ad alto rischio, ma richiedono comunque specifici obblighi di trasparenza. I fornitori di sistemi di IA a rischio limitato devono garantire che gli utenti siano consapevoli di interagire con l’IA o con contenuti generati dall’IA, il che include una chiara informativa sulla natura, la funzionalità e i risultati dell’IA.

Infine, l’ultimo livello comprende i sistemi di IA “a rischio minimo”. Questi sistemi sono considerati i più sicuri e meno suscettibili di causare danni o conseguenze non desiderabili. Esempi di sistemi di IA a rischio minimo includono filtri antispam, riconoscimento di immagini, motori di ricerca basati sull’IA e strumenti di analisi dei dati di base. Tuttavia, i fornitori di questi sistemi sono

incoraggiati a aderire a codici di condotta volontari che applicano tutti o molti dei requisiti previsti per i sistemi di IA ad alto rischio.

Accanto a questa classificazione basata sul rischio dei sistemi di IA per scopi specifici, il regolamento ha introdotto una classificazione diversa per i modelli di IA per finalità generali. L'introduzione di questa seconda classificazione è stata determinata dall'adozione improvvisa e diffusa di tecnologie basate su AI per finalità generali, come l'IA generativa e i modelli linguistici di grandi dimensioni (LLM). In risposta a questo sviluppo, i legislatori dell'UE hanno deciso di introdurre norme sui modelli di IA "semplici" per finalità generali e norme specifiche per i «modelli di IA per finalità generali con rischio sistemico».

2.1. Definizione di intelligenza artificiale

Il regolamento fornisce una definizione ampia di sistema di IA, inteso come:

«un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali»⁸.

Questa definizione ha sostituito quella originariamente proposta⁹ dalla Commissione ed è allineata a quella adottata a livello internazionale dall'OCSE¹⁰. La definizione è stata inoltre oggetto di un'apposita linea guida pubblicata dalla Commissione¹¹.

⁸ Articolo 3, paragrafo 1, AI Act.

⁹ La definizione di "intelligenza artificiale" proposta dalla Commissione europea era «software sviluppato con una o più delle tecniche e degli approcci elencati nell'allegato I e in grado, per una data serie di obiettivi definiti dall'uomo, di generare output quali contenuti, previsioni, raccomandazioni o decisioni che influenzano gli ambienti con cui interagiscono». L'allegato I comprendeva tecniche relative a tre approcci generali all'IA: apprendimento automatico (apprendimento supervisionato e non supervisionato, apprendimento per rinforzo), approcci basati sulla logica e modelli di conoscenza esplicita (come i sistemi esperti) e approcci statistici (come la stima bayesiana).

Questo approccio alla definizione di IA è stato criticato, ed in seguito scartato, perchè sarebbe stato da un lato troppo ampio, includendo potenzialmente tecnologie che non sono tipicamente considerate IA, e dall'altro troppo restrittivo, portando all'esclusione di alcuni sistemi automatizzati sviluppati attraverso la programmazione procedurale, che possono anche funzionare indipendentemente dalla supervisione umana. Inoltre, i confini poco chiari tra le tecniche elencate avrebbero ulteriormente complicato l'identificazione dell'IA per gli operatori di mercato.

¹⁰ OCSE, Raccomandazione del Consiglio sull'intelligenza artificiale, 2019.

¹¹ Comunicazione della Commissione – Orientamenti della Commissione sulla definizione di sistema di intelligenza artificiale stabilita dal regolamento (UE) 2024/1689 (regolamento sull'IA). Bruxelles, 29.7.2025 C(2025) 5053 definitivo.

Il primo termine utilizzato nella definizione è quello di sistema “automatizzato”: ciò si riferisce al fatto che il funzionamento dei sistemi di IA prevede lo sviluppo e l’uso di macchine. Il termine “macchina” può a sua volta essere inteso come comprendente i componenti sia hardware che software che consentono il funzionamento del sistema di IA.

Il secondo elemento della definizione si riferisce al fatto che il sistema è «progettato per funzionare con livelli di autonomia variabili». A tale riguardo, il considerando 12 dell’AI Act chiarisce che i sistemi di IA sono progettati per funzionare con «un certo grado di autonomia di azione rispetto al coinvolgimento umano e di capacità di funzionare senza l’intervento umano».

Tuttavia, né l’AI Act né le linee guida chiariscono i dubbi su quale sia il grado minimo di indipendenza necessario affinché un sistema sia classificato come sistema di IA, né offrono una guida per identificare diversi “livelli” di autonomia, nonostante il fatto che le stesse linee guida ritengano tale identificazione importante soprattutto «per l’elaborazione misure di sorveglianza umana o di attenuazione dei rischi del sistema»¹².

2.2. Pratiche vietate

L’articolo 5 stabilisce alcune pratiche vietate che costituiscono il livello più elevato di rischio associato ai sistemi di IA. Il regolamento impone un divieto generale di tali pratiche, con alcune eccezioni specifiche.

- Manipolazione subliminale: vieta i sistemi di IA che utilizzano tecniche subliminali o metodi manipolatori al di là della coscienza di una persona che distorcono il comportamento, compromettono il processo decisionale e causano danni significativi.
- Sfruttamento delle vulnerabilità: vieta i sistemi di IA che sfruttano le vulnerabilità dovute all’età, alla disabilità o a specifiche situazioni sociali/economiche che causano danni significativi distorcendo il comportamento di individui o gruppi vulnerabili.
- Social scoring: vieta i sistemi di IA che valutano o classificano gli individui in base al comportamento sociale o alle caratteristiche personali, portando a un trattamento dannoso o ingiusto non correlato al contesto dei dati originali o sproporzionato rispetto al comportamento.
- Valutazione del rischio relativa a persone fisiche: vieta ai sistemi di IA di effettuare valutazione del rischio per prevedere comportamenti criminali basandosi esclusivamente sulla profilazione o sui tratti della personalità, sostenen-

¹² *Ibidem*, par. 21.

do invece la valutazione umana basata su fatti oggettivi relativi all'attività criminale.

- Creazione di banche dati di riconoscimento facciale: vieta ai sistemi di IA di creare o ampliare database di riconoscimento facciale attraverso lo scraping non mirato di immagini da Internet o da filmati di telecamere a circuito chiuso (CCTV).
- Riconoscimento delle emozioni nei luoghi di lavoro e nell'istruzione: vieta ai sistemi di IA di inferire le emozioni nei luoghi di lavoro e nelle istituzioni educative, consentendone l'uso solo per motivi medici o di sicurezza al fine di prevenire l'uso improprio dei dati emotivi.
- Categorizzazione biometrica: vieta ai sistemi di IA di classificare le persone sulla base di dati biometrici per dedurre la razza, le opinioni politiche, l'appartenenza sindacale, le credenze religiose, la vita sessuale o l'orientamento sessuale, prevenendo la discriminazione e l'uso improprio di dati personali sensibili.
- Identificazione biometrica in tempo reale negli spazi pubblici: vieta ai sistemi di IA di utilizzare l'identificazione biometrica remota in tempo reale in spazi accessibili al pubblico a fini di applicazione della legge, con eccezioni consentite per situazioni critiche come la ricerca di persone scomparse o la prevenzione di minacce imminenti.

3. Sistemi ad alto rischio

Seguendo un approccio basato sul rischio, il regolamento identifica i sistemi di IA ad alto rischio. Questi sono soggetti a una serie di disposizioni relative al loro sviluppo, alla loro vendita e alla loro diffusione nel mercato dell'UE. L'obiettivo è garantire che i rischi per la sicurezza, la salute e la protezione dei diritti fondamentali associati a tali sistemi siano mitigati senza ostacolarne inutilmente l'adozione.

3.1. Classificazione

I sistemi di IA ad alto rischio sono definiti nell'articolo 6, che prevede due condizioni alternative per la loro classificazione.

In primo luogo, un sistema è considerato ad alto rischio se costituisce un prodotto disciplinato dai regolamenti di armonizzazione del “Nuovo quadro legislativo”¹³ dell'Unione europea o la componente di sicurezza di tale prodotto.

¹³ Il “Nuovo quadro legislativo” (NLF) è un insieme di misure adottate dall'Unione europea per migliorare il mercato interno dei beni e rafforzare le condizioni per l'immissione sul mercato

I regolamenti sono elencati nell'allegato I e comprendono, tra gli altri, la direttiva 2009/48/CE sulla sicurezza dei giocattoli e il regolamento (UE) 2017/-745 sui dispositivi medici.

In secondo luogo, un sistema è considerato ad alto rischio se rientra in uno dei casi d'uso di cui all'allegato III. Tale allegato raggruppa vari tipi di sistemi in otto macroaree:

1. Sistemi biometrici, compresi quelli per l'identificazione delle persone, la categorizzazione basata su attributi sensibili e la categorizzazione delle emozioni;
2. Sistemi per la gestione e il funzionamento di infrastrutture critiche, come il traffico stradale;
3. Sistemi per l'istruzione e la formazione professionale;
4. Sistemi per l'occupazione, la gestione dei lavoratori e l'accesso al lavoro autonomo;
5. Sistemi per l'accesso a servizi privati essenziali (ad esempio, accesso al credito, polizze assicurative) e a prestazioni e servizi pubblici essenziali e fruizione degli stessi;
6. Sistemi utilizzati nelle forze dell'ordine;
7. Sistemi utilizzati nella gestione delle migrazioni, nelle richieste di asilo e nel controllo delle frontiere;
8. Sistemi per l'amministrazione della giustizia e i processi democratici¹⁴.

La seconda condizione è tuttavia soddisfatta con un'eccezione. L'articolo 7, paragrafo 3, concede al fornitore di un sistema di IA elencato nell'allegato III la possibilità di dimostrare che il sistema non presenta rischi significativi. I casi in cui si presume che un sistema non presenti un rischio significativo sono specificati dal regolamento e comprendono una serie di condizioni alternative, ad esempio quando il sistema è destinato a svolgere un compito procedurale limitato o quando il sistema è destinato a eseguire un compito preparatorio per una valutazione pertinente ai fini dei casi d'uso elencati nell'allegato III.

dell'UE di un'ampia gamma di prodotti. Esso fornisce un quadro comune per la commercializzazione dei prodotti, affrontando aspetti quali la valutazione della conformità, l'accreditamento, la sorveglianza del mercato e il marchio CE. Il NLF mira a migliorare la sicurezza dei prodotti, garantire una concorrenza leale e rimuovere gli ostacoli al commercio all'interno dell'UE.

¹⁴ Ad esempio, questa categoria comprende: (a) sistemi di IA destinati a essere usati da un'autorità giudiziaria o per suo conto per assistere un'autorità giudiziaria nella ricerca e nell'interpretazione dei fatti e del diritto e nell'applicazione della legge a una serie concreta di fatti, o a essere utilizzati in modo analogo nella risoluzione alternativa delle controversie; (b) sistemi di IA destinati a essere utilizzati per influenzare l'esito di un'elezione o di un referendum o il comportamento di voto delle persone fisiche nell'esercizio del loro voto alle elezioni o ai referendum.

Una regola generale stabilisce che qualsiasi sistema di IA che si basi sulla profilazione delle persone è sempre classificato come “ad alto rischio”.

Se si ritiene che un sistema di IA elencato nell'allegato III non debba essere considerato ad alto rischio, il fornitore dell'IA deve documentare la relativa valutazione prima che il sistema sia immesso sul mercato o messo in servizio, ed è comunque soggetto all'obbligo di registrazione di cui all'articolo 49, paragrafo 2¹⁵. Le autorità nazionali competenti possono chiedere al fornitore di fornire la documentazione relativa alla valutazione e possono contestare il ricorso all'eccezione da parte del fornitore.

La Commissione europea è autorizzata a adottare atti delegati per integrare, modificare o rimuovere i sistemi di IA ad alto rischio elencati nell'allegato III.

La possibilità di introdurre un nuovo sistema nell'allegato III o di modificare uno esistente è limitata ai casi in cui il nuovo sistema rientri in uno dei settori già presenti e comporti rischi per la salute, la sicurezza o i diritti fondamentali e «tale rischio è equivalente o superiore al rischio di danno o di impatto negativo [a quelli già inclusi]». Sono previsti alcuni criteri per effettuare tale valutazione di equivalenza, tra cui la finalità del sistema di IA, l'uso del sistema, la natura e la quantità dei dati trattati, l'autonomia del sistema e la possibilità per gli esseri umani di prevalere sulla decisione del sistema, il potenziale impatto negativo su individui o gruppi, lo squilibrio di potere e lo stato di vulnerabilità tra l'utente e le persone coinvolte.

3.2. Requisiti essenziali

Per i sistemi di IA ad alto rischio, il regolamento delinea alcuni requisiti essenziali negli articoli da 9 a 15.

L'articolo 9 impone ai fornitori di sistemi di IA ad alto rischio di istituire un sistema di gestione dei rischi¹⁶. Ciò comporta l'identificazione, l'analisi e la mitigazione dei rischi per la sicurezza, la salute e i diritti fondamentali durante tutto il ciclo di vita del sistema. In particolare, il fornitore deve effettuare una triplice analisi: identificare i rischi ragionevolmente prevedibili per la salute, la sicurezza o i diritti fondamentali; stimare i rischi considerando sia l'uso improprio previsto che quello prevedibile; adottare misure per mitigare i rischi identificati. Il ri-

¹⁵ Prima di immettere sul mercato o mettere in servizio un sistema di IA che il fornitore ha concluso non essere ad alto rischio a norma dell'articolo 6, paragrafo 3, il fornitore o, ove applicabile, il rappresentante autorizzato si registra o registra tale sistema nella banca dati dell'UE di cui all'articolo 71.

¹⁶ J. SCHUETT, *Risk Management in the Artificial Intelligence Act*, in *European Journal of Risk Regulation*, 2023, pp. 1-19.

schio accettabile rimane indefinito, ma implica che i benefici superino gli effetti dannosi.

Successivamente, l'articolo 10 richiede che i sistemi di IA ad alto rischio che utilizzano tecniche che prevedono l'uso di dati per l'addestramento di modelli di IA soddisfino i criteri di qualità per i dati utilizzati nell'addestramento, nella convalida e nei test. I fornitori devono implementare pratiche di gestione dei dati adeguate allo scopo del sistema, tenendo conto delle scelte di progettazione, della raccolta dei dati e delle attività di preparazione. I dati devono essere pertinenti, rappresentativi e il più possibile completi e privi di errori.

Il regolamento impone inoltre il monitoraggio e la correzione delle distorsioni nei dati. In questo caso, il trattamento di categorie particolari di dati ai sensi dell'articolo 9 del GDPR è considerato lecito, se necessario, per identificare e correggere queste distorsioni.

Gli articoli 11-13 introducono requisiti di trasparenza per i sistemi di IA ad alto rischio¹⁷. L'articolo 11 del regolamento richiede una documentazione tecnica dettagliata che dimostri la conformità ai requisiti essenziali. L'articolo 12 impone la registrazione automatica degli eventi ("log") di sistema e la loro conservazione per garantire la tracciabilità. L'articolo 13 garantisce la trasparenza affinché il loro funzionamento sia sufficientemente trasparente da consentire a chi lo utilizza di interpretare l'output del sistema e utilizzarlo adeguatamente. Esso specifica la necessità di fornire istruzioni chiare e informazioni pertinenti sulla finalità, le capacità, i limiti e i potenziali rischi del sistema.

L'articolo 14 richiede che i sistemi di IA ad alto rischio siano progettati con strumenti di interfaccia uomo-macchina adeguati a un efficace controllo umano. Tale supervisione dovrebbe avere l'obiettivo di prevenire o ridurre al minimo i rischi per la salute, la sicurezza o i diritti fondamentali.

Infine, i sistemi di IA ad alto rischio devono essere progettati in modo da mantenere un'adeguata accuratezza, robustezza e cibersecurity durante tutto il loro ciclo di vita (articolo 15). Le metriche di accuratezza devono essere incluse nelle istruzioni per l'uso. I sistemi devono essere resistenti agli errori e ai guasti tecnici e le misure di sicurezza informatica devono proteggere da alterazioni non autorizzate.

¹⁷ P. HACKER, J. PASSOTH, *Varieties of AI Explanations Under the Law. From the GDPR to the ALA, and Beyond*, in A. HOLZINGER ET AL. (eds.), *xxAI – Beyond Explainable AI. International Workshop, Held in Conjunction with ICML 2020, July 18, 2020, Vienna, Austria, Revised and Extended Papers*, Cham: Springer, 2022, pp. 343-373.

3.3. La procedura di valutazione della conformità

L'articolo 16 chiarisce che la responsabilità di garantire la conformità dei sistemi di IA ad alto rischio ai requisiti essenziali spetta al fornitore. Si tratta della persona fisica o giuridica che sviluppa un sistema di IA (o lo fa sviluppare) e lo immette sul mercato o lo mette in servizio con il proprio nome o marchio, a titolo oneroso o gratuito¹⁸.

L'obbligo di conformità si configura come un obbligo di mezzi, il che significa che i fornitori devono fare tutto il possibile per applicare tali requisiti durante le fasi di progettazione, sviluppo e implementazione, tenendo conto della finalità prevista del sistema e dello stato dell'arte.

I fornitori dispongono di un margine di discrezionalità nella scelta delle modalità di attuazione di tali requisiti, potendo alternativamente definire soluzioni proprie oppure fare riferimento alle norme armonizzate adottate a livello europeo.

Le norme armonizzate sono norme tecniche elaborate dagli organismi europei di normazione e approvate dalla Commissione mediante la pubblicazione del loro riferimento nella Gazzetta ufficiale dell'Unione europea.

Ai sensi dell'articolo 40 del regolamento, la conformità alle norme di armonizzazione comporta una presunzione di conformità ai requisiti essenziali del regolamento. Anche se, *de jure*, la loro adozione è volontaria, la presunzione di conformità costituisce un incentivo decisivo ad adottarle, rendendole di fatto vincolanti.

Il regolamento introduce inoltre ulteriori obblighi per i fornitori, tra cui la dotazione di un sistema di gestione della qualità (articolo 17), la conservazione della documentazione (articolo 18) e dei registri ("log") generati automaticamente (articolo 19) e la cooperazione con le autorità di vigilanza del mercato (articolo 21).

I fornitori devono garantire che il sistema sia sottoposto alla procedura di valutazione della conformità appropriata prima della sua immissione sul mercato o della sua messa in servizio, come indicato all'articolo 43¹⁹.

- Per i sistemi ad alto rischio elencati nell'allegato I, sezione A (quelli coperti dal «nuovo quadro legislativo»), i fornitori devono seguire le procedure di valutazione della conformità richieste da tali regolamenti.

¹⁸ Articolo 4, paragrafo 3, AI Act.

¹⁹ J. MÖKANDER, M. AXENTE, F. CASOLARI, L. FLORIDI, *Valutazioni di conformità e monitoraggio post-commercializzazione: una guida al ruolo dell'auditing nella proposta di regolamento europeo sull'IA*, in *Minds and Machines*, 2022 (32,2), 241-68.

- Per i sistemi biometrici elencati nell'allegato III, punto 1, i fornitori possono optare per una valutazione di conformità esterna o interna se applicano norme armonizzate. Se le norme non sono applicate o non esistono, è obbligatoria una valutazione di conformità esterna, che coinvolge un "organismo notificato" e che soddisfa determinati requisiti organizzativi, di gestione della qualità e di risorse.
- Per i sistemi ad alto rischio elencati nell'allegato III, punti da 2 a 8, i fornitori devono seguire una valutazione di conformità basata sul controllo interno, garantendo la conformità del sistema di gestione della qualità, della documentazione tecnica e del monitoraggio successivo all'immissione sul mercato con l'articolo 72. Dopo una valutazione positiva, i fornitori devono rilasciare una dichiarazione di conformità UE, apporre il marchio CE e registrare il sistema nella banca dati dell'UE istituita secondo le disposizioni del regolamento.

3.4. La valutazione d'impatto sui diritti fondamentali

L'articolo 26 elenca gli obblighi dell'utilizzatore del sistema (deployer). Questi è una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo che utilizza un sistema di IA sotto la propria autorità, tranne nel caso in cui il sistema di IA sia utilizzato nel corso di un'attività personale non professionale²⁰.

Il deployer deve adottare misure tecniche e organizzative per garantire l'uso dei sistemi di IA ad alto rischio in conformità con le istruzioni per l'uso, il monitoraggio del sistema durante l'uso e la registrazione dei log.

Inoltre, il deployer dei sistemi ad alto rischio elencati nell'allegato III, che sono soggetti al diritto pubblico o sono enti privati che forniscono servizi pubblici, devono effettuare una valutazione d'impatto sui diritti fondamentali (FRIA).²¹ Questo obbligo si estende ai deployer privati che utilizzano sistemi ad alto rischio per l'accesso a servizi di interesse pubblico essenziali e per la valutazione del merito creditizio.

La FRIA, ispirata alla valutazione d'impatto sulla protezione dei dati del GDPR, comprende tre componenti: (1) descrivere l'uso previsto del sistema, compresi il periodo di utilizzo, la frequenza e le persone/gruppi interessati; (2) valutare i rischi specifici di danno che incidono sui diritti fondamentali; (3) attuare misure di controllo umano e di mitigazione dei rischi.

²⁰ Cfr. articolo 3, paragrafo 4, AI Act.

²¹ A. MANTELERO. *La valutazione d'impatto sui diritti fondamentali (FRIA) nella legge sull'IA: origini, obblighi giuridici ed elementi chiave per un modello di riferimento*, in *Computer Law & Security Review*, 2024 (54).

3.5. Sistemi a basso rischio

L'articolo 50 riguarda quattro sistemi di IA specifici per i quali sono previsti determinati obblighi di trasparenza.

Il primo gruppo descritto nell'articolo 50 si riferisce in generale ai sistemi «destinati a interagire direttamente con persone fisiche». Sebbene la definizione appaia alquanto ambigua, la disposizione è stata concepita per affrontare le applicazioni di chatbot basate sull'IA. In questo caso, il fornitore del sistema deve garantire che le persone fisiche siano consapevoli di interagire con un'IA. L'obbligo non si applica quando l'interazione è evidente dalle circostanze e dal contesto di utilizzo.

Il secondo gruppo è rappresentato dai sistemi che generano contenuti audio, immagini, video o testi sintetici. In questo caso, i fornitori devono garantire, per mezzo di tecniche efficaci, che i risultati siano contrassegnati in un formato leggibile da una macchina e riconoscibili come generati o manipolati artificialmente. Questo obbligo non si applica se il sistema di IA assiste la modifica standard, non altera in modo sostanziale i dati di input o la semantica, o è utilizzato per l'individuazione, la prevenzione, l'indagine o il perseguimento di reati penali.

Il terzo gruppo comprende i sistemi di riconoscimento delle emozioni e di categorizzazione biometrica. Questi sistemi interpretano i dati biometrici e formulano valutazioni sulle persone. La prima categoria può includere sistemi di IA che applicano tecniche di analisi delle emozioni o di profilazione psicografica. La seconda categoria può includere alcuni dispositivi indossabili come Apple Watch o Fitbit, che utilizzano dati biometrici per valutare lo stato di salute degli utenti, nonché sistemi di riconoscimento vocale (come Siri o Alexa) o sistemi di riconoscimento facciale.

Infine, il quarto gruppo di sistemi di cui all'articolo 50 si riferisce alla pratica dei “deep fake”. Tale pratica è definita come l'uso dell'IA per generare o manipolare contenuti di immagini, audio o video che assomigliano molto a persone, luoghi, oggetti o altre entità o eventi esistenti e che potrebbero apparire falsamente autentici o veritieri a una persona. L'obbligo derivante da un sistema che genera o manipola “deep fake” è di rendere noto che il contenuto è stato generato o manipolato artificialmente. Tale obbligo non si applica se l'uso è autorizzato dalla legge per accertare, prevenire, indagare o perseguire reati.

4. La regolamentazione dei modelli di IA con finalità generali

Come anticipato, gli emendamenti del Parlamento europeo includevano alcune norme specifiche per i modelli di IA con finalità generali. Queste disposizioni creano, di fatto, un regime giuridico parallelo e autonomo per questo tipo

di sistemi di IA. Tali modelli, infatti, non si inseriscono agevolmente nella logica dei sistemi di IA destinati a scopi specifici, come quelli elencati nell'allegato III del regolamento, pur presentando potenziali rischi significativi per la sicurezza, la salute e la tutela dei diritti fondamentali.

I “modelli di IA per finalità generali” sono definiti come modelli di IA in grado di svolgere con competenza un'ampia gamma di compiti e di essere integrati in vari sistemi o applicazioni a valle.

Seguendo l'approccio basato sul rischio, il regolamento collega tali sistemi a due sottoregimi giuridici: uno per tutti i modelli e uno specifico per i modelli che presentano un “rischio sistemico”. Secondo il considerando 110, un “rischio sistemico” si riferisce a incidenti gravi e conseguenze significative per la salute pubblica, la sicurezza, i processi democratici e la sicurezza pubblica ed economica, tra gli altri.

L'articolo 51 classifica un modello di IA per uso generico come avente un rischio sistemico quando (a) ha “capacità di impatto elevato”²² o (b) la Commissione decide che ha capacità o impatto equivalenti a quelli di cui alla lettera a), tenendo conto dei criteri di cui all'allegato XIII²³.

Per quanto riguarda i regimi giuridici, i fornitori di modelli di IA “semplici” per finalità generali devono conservare la documentazione tecnica, fornire informazioni aggiornate agli utilizzatori dei sistemi di IA, attuare una politica di conformità alle leggi dell'UE sul diritto d'autore e sui diritti ad esso connessi, e rendere pubblico un riassunto dettagliato dei contenuti della formazione.

I fornitori di modelli di IA per finalità generali che comportano un “rischio sistemico” devono inoltre identificare il rischio sistemico, condurre valutazioni con protocolli e strumenti allo stato dell'arte, compresi i “test contraddittori (adversarial testing)”²⁴ e svolgere valutazioni e misure di mitigazione dei rischi.

A tal fine l'UE predispone il codice di buone pratiche sull'IA per finalità generali, uno strumento volontario, preparato da esperti indipendenti in un processo multipartecipativo, concepito per aiutare l'industria a rispettare gli obblighi della legge sull'IA per i fornitori di modelli di IA per finalità generali. I fornitori di modelli di IA che lo firmano volontariamente possono dimostrare di

²² Le capacità ad impatto elevato sono definite come quelle che eguagliano o superano i modelli di IA generici più avanzati, con un possibile indicatore pari a 10^{25} FLOPS (operazioni in virgola mobile al secondo, ovvero una misura delle prestazioni di un computer).

²³ I criteri includono il numero di parametri, la dimensione del set di dati, la potenza di calcolo, la multimodalità, le attività che il modello è in grado di svolgere, l'impatto sul mercato e gli utenti registrati.

²⁴ I test contraddittori, i quali introducono piccole perturbazioni nei dati di input per ingannare il sistema di IA, aiutano a identificare potenziali vulnerabilità e a garantire la robustezza dei modelli di IA contro manipolazioni dannose.

rispettare la legge sull'IA aderendo al codice. Ciò ridurrà i loro oneri amministrativi e garantirà loro una maggiore certezza del diritto rispetto a quanto accadrebbe se dimostrassero la conformità con altri metodi.

Il codice, composto da tre capitoli scritti separatamente: trasparenza, diritto d'autore e sicurezza²⁵. I capi sulla trasparenza e sul diritto d'autore offrono a tutti i fornitori di modelli di IA per finalità generali un modo per dimostrare il rispetto dei loro obblighi ai sensi dell'articolo 53 della legge sull'IA. I capi sulla sicurezza sono pertinenti solo per il piccolo numero di fornitori dei modelli più avanzati, quelli soggetti agli obblighi della legge sull'IA per i fornitori di modelli di IA per finalità generali con rischio sistemico a norma dell'articolo 55 della legge sull'IA.

Se si verifica un incidente grave, i fornitori devono registrarlo e segnalarlo alla Commissione e alle autorità nazionali. La conformità è incentivata attraverso codici di condotta monitorati dall'Ufficio IA e dal Comitato IA.

5. Applicazione e sanzioni

Il regolamento istituisce un complesso sistema di governance multilivello, articolato sia a livello dell'Unione europea sia a livello nazionale.

A livello dell'UE, il regolamento istituisce due nuovi organismi, il Comitato europeo per l'intelligenza artificiale e l'Ufficio europeo per l'Intelligenza Artificiale.

Il Comitato europeo per l'intelligenza artificiale è incaricato di garantire una cooperazione efficace tra le autorità nazionali competenti, anche attraverso la condivisione delle migliori pratiche, e di sostenere l'azione della Commissione europea mediante l'elaborazione di pareri, raccomandazioni e orientamenti interpretativi.

L'Ufficio europeo per l'IA, istituito all'interno della Commissione europea, funge da centro nevralgico per le competenze in materia di IA in tutta l'UE. La sua responsabilità principale è quella di monitorare e far rispettare le disposizioni sui modelli di IA per finalità generali. Inoltre, all'Ufficio IA è affidato il compito di promuovere lo sviluppo e l'uso di un'IA affidabile e di favorire la cooperazione internazionale.

Gli Stati membri, da parte loro, devono designare una o più autorità nazionali competenti per vigilare sull'applicazione e il rispetto del regolamento.

²⁵ Il codice è stato pubblicato il 10 luglio 2025. È integrato da orientamenti della Commissione sui concetti chiave relativi ai modelli di IA per finalità generali. La Commissione e il comitato per l'IA hanno confermato che il codice è uno strumento volontario adeguato affinché i fornitori di modelli GPAI dimostrino la conformità alla legge sull'IA. <https://digital-strategy.ec.europa.eu/it/policies/contents-code-gpai>

Tali autorità possono richiedere informazioni e accedere alla documentazione dei fornitori, sollecitare l'adozione di misure correttive e ritirare il sistema dal mercato.

Per quanto riguarda gli strumenti di governance aggiuntivi, il titolo VII del regolamento istituisce una banca dati per i sistemi di IA ad alto rischio presso la Commissione europea. Tale banca dati raccoglierà informazioni importanti sulle caratteristiche e le finalità dei sistemi, le certificazioni pertinenti e l'identità del fornitore.

Quanto al regime sanzionatorio, il regolamento adotta un'impostazione analoga a quella del GDPR, demandando agli Stati membri la definizione delle sanzioni applicabili entro soglie massime predeterminate.

Le sanzioni amministrative per le violazioni delle pratiche vietate in materia di IA, come indicato all'articolo 5, possono raggiungere fino a 35 milioni di euro o il 7% del fatturato annuo mondiale totale del trasgressore, a seconda di quale sia l'importo più elevato. Per altre violazioni imputabili agli operatori o agli organismi notificati, le sanzioni possono arrivare fino a 15 milioni di euro o al 3% del fatturato annuo mondiale totale.

Inoltre, la fornitura di informazioni errate, incomplete o fuorvianti alle autorità può comportare sanzioni fino a 7,5 milioni di euro o all'1% del fatturato annuo totale a livello mondiale.

Nel determinare l'ammontare delle ammende, le autorità devono tenere conto di vari fattori, tra cui la natura e la gravità della violazione, le dimensioni e il fatturato dell'operatore, l'eventuale reiterazione della violazione e la collaborazione dell'operatore con le autorità.

Infine, il regolamento prevede due rimedi individuali a tutela delle persone interessate, rivolti rispettivamente all'autorità di controllo competente e al responsabile dell'implementazione dei sistemi di IA ad alto rischio.

In primo luogo, l'articolo 85 conferisce alle persone fisiche o giuridiche interessate da una violazione del regolamento sull'IA il diritto di presentare un reclamo all'autorità di vigilanza del mercato competente.

In secondo luogo, le persone fisiche soggette a decisioni basate su sistemi di IA ad alto rischio (salvo alcune eccezioni) che hanno un impatto giuridico o significativo sulla loro salute, sicurezza o diritti fondamentali hanno diritto a ricevere dal deployer spiegazioni chiare sul ruolo del sistema di IA nel processo decisionale e sugli elementi chiave della decisione.

6. Spazi di Sperimentazione Normativa

Il capo VI dell'AI Act introduce gli spazi di sperimentazione normativa per l'intelligenza artificiale ("*regulatory sandbox*"), concepiti come strumenti di gover-

nance flessibile volti a favorire lo sviluppo di sistemi di IA innovativi nel rispetto del quadro regolatorio dell'Unione.

In particolare, l'articolo 57 prevede che gli Stati membri assicurino l'istituzione di almeno uno spazio di sperimentazione normativa per l'IA a livello nazionale, affidandone l'operatività alle autorità competenti designate. Tali spazi possono essere istituiti anche congiuntamente da più Stati membri, al fine di promuovere approcci coordinati e ridurre il rischio di frammentazione regolatoria. Accanto agli spazi di sperimentazione nazionali, il regolamento consente l'istituzione di ulteriori sandbox a livello regionale o locale, nonché iniziative congiunte tra autorità competenti di diversi Stati membri.

Sotto il profilo funzionale, gli spazi di sperimentazione normativa sono definiti come ambienti controllati, finalizzati a promuovere l'innovazione e a facilitare lo sviluppo, l'addestramento, la sperimentazione e la convalida di sistemi di IA innovativi, per un periodo di tempo limitato e prima della loro immissione sul mercato o messa in servizio (Articolo 3, paragrafo 55). L'accesso allo spazio di sperimentazione è subordinato alla definizione di un "piano dello spazio di sperimentazione", concordato tra il fornitore o il potenziale fornitore del sistema di IA e l'autorità competente, che disciplina le modalità della sperimentazione, i suoi obiettivi e le condizioni di svolgimento. Nell'ambito di tali spazi possono essere previste anche prove in condizioni reali, purché soggette a controlli adeguati.

Un elemento centrale del modello delineato dall'AI Act è il ruolo attivo delle autorità competenti, le quali sono chiamate a fornire orientamenti, supervisione e sostegno ai partecipanti allo spazio di sperimentazione. In tale contesto, le autorità devono contribuire all'individuazione e alla valutazione dei rischi, in particolare quelli connessi ai diritti fondamentali, alla salute e alla sicurezza, nonché alla definizione e alla verifica dell'efficacia delle misure di attenuazione adottate.

Le modalità dettagliate di istituzione e funzionamento degli spazi di sperimentazione normativa sono ulteriormente precisate dall'articolo 58, che attribuisce alla Commissione il potere di adottare atti di esecuzione volti a stabilire principi comuni applicabili in tutta l'Unione (la versione finale è prevista per Giugno 2026). Tali principi riguardano, in particolare, i criteri di ammissibilità e selezione dei partecipanti, le procedure di domanda, partecipazione, monitoraggio ed uscita dallo spazio di sperimentazione, nonché i termini e le condizioni applicabili ai soggetti coinvolti, inclusi il contenuto del piano di sperimentazione e della relazione finale di uscita.

Infine, il regolamento prevede specifiche esenzioni e flessibilità in materia di utilizzo dei dati nell'ambito degli spazi di sperimentazione normativa²⁶, al fine di agevolare lo sviluppo e il test dei sistemi di IA innovativi, nel rispetto delle garanzie previste dal diritto dell'Unione. Parallelamente, l'AI Act contempla anche la possibilità di effettuare prove di sistemi di IA ad alto rischio in condizioni reali al di fuori degli spazi di sperimentazione normativa²⁷, purché siano soddisfatte le condizioni e le salvaguardie stabilite dal regolamento, confermando un approccio volto a bilanciare promozione dell'innovazione e tutela degli interessi pubblici fondamentali.

²⁶ Cfr Articolo 59, AI Act.

²⁷ Cfr Articolo 60, AI Act.

LA DECISIONE AUTOMATICA E LA SUA SPIEGAZIONE TRA GDPR E AI ACT*

Francesca Lagioia, Giovanni Sartor

SOMMARIO: 1. Le decisioni automatiche. 2. Spiegabilità e Intelligenza Artificiale. 3. Art. 22 GDPR: il divieto di decisioni automatiche. 4. Art. 22 GDPR: eccezioni e misure di salvaguardia. 5. Art. 22 GDPR: un diritto alla spiegazione?. 6. Art. 86 AIA: un diritto alla spiegazione?. 7. Art. 86 AIA. Il coordinamento con altre normative.

1. Le decisioni automatiche

L'intelligenza artificiale permette di automatizzare i processi decisionali anche in ambiti che richiedono scelte complesse, basate su numerosi fattori e su criteri non rigidamente predeterminati. Ciò può migliorare la qualità delle decisioni pubbliche e private, ma comporta nuovi rischi. In questa sezione delineiamo la relazione tra intelligenza artificiale e decisione automatica. Nella successiva approfondiamo il tema della spiegazione, nelle sezioni da 3 a 7, esaminiamo le disposizioni europee più pertinenti: l'Art. 22 del Regolamento Generale sulla protezione dei dati (GDPR) e l'Art. 86 del Regolamento sull'Intelligenza Artificiale (AI-Act).

1.1. Il dibattito sui rischi della decisione automatica

È in corso un ampio dibattito su potenzialità e rischi delle decisioni algoritmiche. Diversi studi hanno mostrato come, in molti settori, previsioni e decisioni automatizzate siano più precise ed efficaci di quelle umane, riducendo sia gli errori (specie nell'interpretare dati statistici), sia l'incidenza di pregiudizi – per esempio, etnici, sociali e di genere – da cui spesso siamo affetti. In molti ambiti – dagli investimenti, al reclutamento di personale, alla concessione della libertà vigilata – le determinazioni algoritmiche spesso superano, rispetto ai consueti criteri valutativi, quelle di esperti umani.

* Il presente contributo è un risultato del progetto ERC-Advanced “CompuLaw” (Grant Agreement No 833647).

Altri hanno posto l'accento sulle possibilità di errore e discriminazione. È vero che solo in rari casi gli algoritmi assumono decisioni esplicitamente discriminatorie, la cosiddetta discriminazione diretta, basando le proprie previsioni su caratteristiche (predittori) vietate, come razza, etnia o genere. Più frequentemente le determinazioni algoritmiche possono comportare una discriminazione indiretta, cioè avere un impatto sfavorevole sproporzionato su individui appartenenti a certi gruppi, senza una giustificazione accettabile. Ciò si verifica poiché molti sistemi basati su metodi di apprendimento automatico imparano dagli esempi su cui sono stati addestrati (secondo le tecnologie dell'apprendimento supervisionato), e quindi tendono a riprodurre pregi e difetti di tali esempi, inclusa la propensione all'errore e al pregiudizio. Così, un sistema per il reclutamento, addestrato su esempi di decisioni passate in cui donne e minoranze siano state discriminate, riprodurrà la stessa logica. Il pregiudizio all'interno di un insieme di addestramento può essere presente anche se le informazioni che costituiscono i dati di ingresso del sistema (i predittori) non comprendono caratteristiche discriminatorie il cui uso sia giuridicamente vietato, come etnia o genere. Ciò può verificarsi ogni qual volta esista una correlazione tra caratteristiche discriminatorie e alcuni predittori. Supponiamo, ad esempio, che un responsabile delle risorse umane non abbia mai assunto candidati di una certa etnia a causa di un suo pregiudizio e che gli individui appartenenti a tale etnia abitino per lo più in certi quartieri della città. Un insieme di addestramento basato sulle decisioni di tale dirigente insegnerebbe a non selezionare gli individui residenti in quei quartieri, comportando il mancato accoglimento di tutte le domande di assunzione provenienti da coloro che appartengano all'etnia discriminata.

In altri casi, un insieme di addestramento può essere parziale e contenere pregiudizi rispetto a un certo gruppo, poiché il raggiungimento del risultato desiderato (ad esempio, certe prestazioni lavorative) è approssimato mediante un *proxy* (un elemento sostitutivo) che produce un impatto discriminatorio indiretto su quel gruppo. Supponiamo, ad esempio, che le future prestazioni lavorative dei dipendenti (obiettivo di interesse nei processi di assunzione) siano misurate considerando unicamente il numero di ore spese in ufficio. Tale criterio potrebbe comportare una valutazione peggiore delle donne rispetto agli uomini, qualora in passato le donne abbiamo speso meno ore in ufficio, a causa di impegni familiari più intensi. Il sistema assocerebbe correttamente al genere femminile una minore propensione al lavoro straordinario, ma risulterebbe viziato dal collegamento di tale propensione ad una minore capacità lavorativa (senza considerare altri fattori, molto più significativi).

In altri casi, errori e discriminazioni possono derivare da pregiudizi impliciti nella scelta dei fattori sulla base dei quali il sistema formula le proprie conclu-

sioni (le “predizioni”), i cosiddetti predittori. Determinazioni inique e ingiuste possono derivare dall’uso di attributi vantaggiosi applicabili ai soli membri di un certo gruppo (ad esempio, il fatto di aver frequentato certe scuole o università, socialmente selettive).

L’ingiustizia può anche derivare dall’uso di predittori basati su giudizi e valutazioni umane distorte, faziose, o parziali (come lettere di raccomandazione che favoriscono certe categorie di candidati). Infine, errori e discriminazioni possono risultare dal fatto che gli esempi forniti al sistema non riflettono la composizione statistica della popolazione. Quindi, tali esempi possono condurre a determinazioni scorrette e discriminatorie rispetto a certi gruppi, che in passato non hanno avuto modo di rivestire certe posizioni (in particolare posizioni di responsabilità). Supponiamo ancora, per esempio, che nella valutazione di domande per ottenere la libertà condizionale, la presenza di precedenti penali a carico del reo abbia un peso sfavorevole, e che i membri di certi gruppi (ad esempio coloro che appartengono a una certa etnia o che professano un certo credo religioso) siano soggetti a controlli più rigorosi e stringenti, tali che la loro attività criminale sia più spesso scoperta e conseguentemente condannata. Per i membri di tale gruppo, ciò comporterebbe generalmente una valutazione meno favorevole rispetto ai membri di altri gruppi, a parità di condizioni.

I membri di un certo gruppo possono anche subire discriminazioni quando quel gruppo è rappresentato solo da un sottoinsieme molto piccolo dell’insieme di addestramento. Ciò ridurrà l’accuratezza delle previsioni (si consideri, ad esempio, il caso di un’azienda che abbia assunto poche donne in passato e utilizzi i propri registri storici delle assunzioni come insieme di addestramento).

La possibilità di usare sistemi automatici per valutazioni e decisioni sugli individui – diminuendo il costo di tali valutazioni e decisioni, e accrescendo i fattori su cui esse si possono basare – ne accresce la quantità e la pervasività. In generale, grazie all’intelligenza artificiale, qualsiasi tipo di dato personale può essere usato per analizzare, prevedere e influenzare il comportamento di un individuo, un’opportunità che trasforma i dati in merce preziosa. Le informazioni che un tempo non venivano raccolte, o erano scartate, poiché prive di valore – ad esempio tracce di attività online – sono ora diventate una risorsa. Attraverso le tecnologie dell’IA – in combinazione con tutti i dispositivi e i sensori che tracciano quotidianamente ogni attività umana – gli individui possono essere costantemente sorvegliati e influenzati, in casi e contesti molto più numerosi, sulla base di un insieme più ampio di caratteristiche personali (che spaziano dalle condizioni economiche e di salute, al luogo di residenza, alle scelte di vita personali, fino al comportamento online e offline, ecc.). Correlando i dati che riguardano gli individui con classificazioni e previsioni corrispondenti, l’intel-

ligenza artificiale aumenta il potenziale della profilazione, vale a dire, la possibilità di inferire nuove informazioni su individui e gruppi e di compiere valutazioni e adottare decisioni su tale base. Essere soggetti a una persistente osservazione e valutazione genera una pesante pressione psicologica e incide sull'autonomia personale, anche quando esista una correlazione statistica tra le caratteristiche della persona interessata, e la valutazione/previsione che giustifica una certa determinazione. Inoltre, la disponibilità di valutazioni automatiche – efficienti, economiche, e apparentemente oggettive, anche quando prive di una motivazione comprensibile all'uomo – può avere i seguenti impatti: da un lato le persone possono essere trattate in modo iniquo, senza tener conto delle speciali circostanze che le riguardano, dall'altro lato, le contestazioni da parte degli interessati possono essere respinte o ostacolate, anche quando giustificate, poiché interferiscono con l'operatività del sistema, causando costi e incertezze.

1.2. Opportunità oltre ai rischi?

Se è vero che i sistemi algoritmici, e in particolare quelli basati sull'apprendimento automatico, possono riprodurre o anche esacerbare le iniquità esistenti, è anche vero che i processi algoritmici sono più controllabili di quelli sottesi alle decisioni umane, e possono essere migliorati e ingegnerizzati in modo da prevenire risultati iniqui.

Non possiamo qui approfondire il tema della valutazione comparativa di decisioni umane e decisioni algoritmiche. Quello che è certo è che oggi è superata l'idea che solo le decisioni di routine possano essere affidate agli algoritmi, e non quelle che coinvolgono condizioni di incertezza, discrezionalità e valutazioni, anche rispetto agli individui. I sistemi di intelligenza artificiale hanno dimostrato di poter operare con successo anche in ambiti in cui mancano criteri precisi e univoci, e quindi anche in settori tradizionalmente affidati all'intuizione umana, affinata con l'esperienza (per esempio, nella diagnosi medica, negli investimenti finanziari, nella concessione del credito, ecc.). L'alternativa al processo decisionale automatizzato non sono le decisioni perfette ma le decisioni umane con tutti i loro difetti e le loro imperfezioni. Anche un sistema algoritmico imperfetto potrebbe essere più giusto ed equo di un essere umano colmo di pregiudizi. Ciò non significa che in qualsiasi settore e ambito di attività la macchina prevalga sull'uomo. Quando è necessario affrontare questioni nuove, sviluppare soluzioni innovative, cogliere attitudini, preferenze e interessi umani, la mente dell'uomo è insostituibile. La sfida per il futuro è trovare le migliori combinazioni tra intelligenza umana e artificiale, valutazioni umane e valutazioni automatizzate, integrandole fra loro, e tenendo conto delle potenzialità di ciascuna. Inoltre, l'intelligenza artificiale può essere utilizzata per controllare le sue stesse

applicazioni, così da individuare eventuali difetti nei meccanismi della decisione automatica, e aiutare nella predisposizione di contestazioni.

2. Spiegabilità e Intelligenza Artificiale

La spiegabilità delle decisioni automatiche è da tempo al centro del dibattito sull'etica e il diritto dell'intelligenza artificiale. Per esempio, nel rapporto dell'High Level Expert Group, la spiegabilità (explicability) rappresenta uno dei quattro principi etici fondamentali dell'IA affidabile (trustworthy), accanto al rispetto dell'autonomia umana, la prevenzione dei danni e l'equità. Tale principio costituisce un aspetto centrale del requisito della trasparenza (accanto a tracciabilità e comunicazione).

Di seguito, esaminiamo l'importanza della spiegabilità, illustrandone il rilievo socio-giuridico e considerandone le diverse tipologie e funzioni.

2.1. Il valore socio-giuridico della spiegazione

L'esigenza che le decisioni sugli individui siano accompagnate da spiegazioni è supportata da numerose ragioni: prevenire l'arbitrarietà e accrescere la legittimità delle decisioni, favorirne la contestabilità e consentire la correzione di errori; stimolare il perfezionamento dei processi decisionali; promuovere l'*accountability* e la responsabilizzazione dei decisori. La spiegabilità contribuisce anche alla fiducia nei confronti dei sistemi meritevoli di affidamento (c.d. *trustworthy*). Il suo valore morale e giuridico deriva, dal fatto che spiegazioni adeguate rafforzano l'"agentività" dei destinatari, cioè la loro capacità di agire autonomamente. Per reagire consapevolmente a una decisione automatica – accettandola, contestandola, o chiedendone il riesame – occorre conoscerne sia gli elementi (le ragioni) fattuali sia quelli normativi-valutativi su cui essa si fonda. Gli elementi fattuali riguardano le situazioni reali-empiriche su cui la decisione poggia e i fatti ulteriori inferiti da tali situazioni. Per esempio, nel caso di un sistema che preveda il rischio di recidiva di un imputato e suggerisca le misure da applicare, l'imputato ha l'esigenza di conoscere quali elementi fattuali sono stati utilizzati nel calcolo del suo punteggio di rischio (e.g., precedenti penali, livello di istruzione, situazione lavorativa, uso di sostanze stupefacenti) e con quali inferenze (e.g., determinazione della probabilità di recidiva mediante metodi statistici o reti neurali). Ciò può consentirgli di valutare, almeno in parte, la correttezza degli elementi fattuali e la ragionevolezza delle inferenze. Inoltre, l'imputato è interessato a conoscere in considerazione di quali obiettivi (e.g., protezione dei terzi, riabilitazione del reo) il suo livello di rischio abbia giustificato l'adozione di una certa misura, per esempio, un maggior periodo di detenzione,

o la soggezione a controlli più incisivi. Alla luce degli elementi appena indicati l'imputato potrà deliberare se accettare la decisione o contestarla nelle sedi opportune.

2.2. Tipologie e funzioni della spiegazione nei sistemi di Intelligenza Artificiale

Quanto più sistemi di IA formulano predizioni o decisioni rilevanti per gli individui e per la società, tanto più è importante che siano spiegate. Tuttavia, non sempre la spiegazione è semplice o persino possibile. A questa esigenza si contrappongono, infatti, i più recenti sviluppi dell'IA, quelli basati su tecniche avanzate di apprendimento automatico. Tali tecniche permettono la realizzazione di sistemi con prestazioni elevatissime, che tuttavia presentano una struttura estremamente complessa e il cui funzionamento non si svolge secondo ragionamenti comprensibili all'uomo (sistemi opachi). Così, esigenze di prestazione e spiegabilità sono in tensione ogniqualevolta i sistemi più opachi forniscano le prestazioni più elevate. Di qui la necessità di conciliare le due esigenze, in diversi ambiti applicativi. Per esempio, potremmo ritenere che le prestazioni siano prioritarie in ambito medico, mentre la spiegabilità sia preminente nelle decisioni giuridiche ed amministrative.

Nella comunità scientifica il tema è affrontato da due prospettive principali.

La prima, di tipo modellistico, è rivolta agli esperti di IA, e mira a chiarire il funzionamento generale del sistema, cioè a illustrare come, e in base a quali fattori e processi di elaborazione, a certi tipi di input corrispondano certi tipi di output.

La seconda, di tipo socio-comunicativo, mira a fornire agli interessati (utenti o destinatari) informazioni significative, che consentano loro di conoscere e valutare le ragioni delle decisioni che li riguardano.

Al centro della ricerca sulla spiegabilità di tipo modellistico vi sono i seguenti metodi:

i) Costruzione di modelli trasparenti. Tali modelli possono sostituire quelli opachi qualora ciò non comporti prestazioni notevolmente inferiori. Alternativamente, i modelli trasparenti possono affiancarsi a quelli opachi, riproducendone le funzionalità, seppure con una certa approssimazione. Nel secondo caso, la spiegazione del funzionamento del sistema opaco si può ottenere attraverso l'esame del corrispondente modello trasparente. È il caso, per esempio, di un albero decisionale o un insieme di regole, la cui attivazione riproduca il funzionamento di una rete neurale.

ii) Ispezione del modello opaco. Consiste nell'estrarre rappresentazioni di un sistema opaco, che consentano di coglierne proprietà rilevanti. Tra tali proprietà, ad esempio, la sensitività del modello a variazioni dell'input (quali mutamenti

dell'input comportano cambiamenti significativi e dell'output) o l'identificazione delle componenti responsabili di specifici aspetti dell'output. Per esempio, nel primo caso quali variazioni nel patrimonio e nell'età di un individuo influiscano nella determinazione della sua affidabilità creditizia e, nel secondo, quali neuroni si attivino quando si giunge a concedere o a respingere una richiesta di credito.

La spiegazione di tipo socio-comunicativa si articola lungo due dimensioni, la spiegazione generalista (che illustra il funzionamento del sistema, senza considerarne l'applicazione al caso concreto) e la spiegazione individualizzata (basata sui dati della persona).

La spiegazione generalista consiste in una descrizione del funzionamento del sistema. Idealmente, comprende i seguenti elementi:

i) I predittori (le categorie di dati di input) che il sistema prende in considerazione (ad esempio, per una richiesta di prestito: reddito, sesso, patrimonio, lavoro del richiedente) e quali valori per tali predittori favoriscano o sfavoriscano l'esito sperato;

ii) I valori-soglia che determinano un esito positivo o negativo (ad esempio, il punteggio da raggiungere affinché il prestito sia concesso);

iii) La conseguenza prevista a fronte della valutazione/decisione automatizzata (ad esempio, l'approvazione o il rifiuto della richiesta di prestito) iv) Il ruolo della predizione o decisione rispetto all'intero processo decisionale (per esempio, il modo in cui il punteggio di affidabilità creditizia assegnato incide sulla decisione del funzionario competente, in concorso con quali elementi ulteriori, come eventuali garanzie fornite da terzi).

La spiegazione individualizzata, invece, si basa sull'elaborazione dei dati relativi alla persona e mira a chiarire come quei dati conducano alla decisione adottata. Tra i metodi più efficaci, possiamo ricordare i seguenti:

i) Spiegazione contrastiva. Specifica quali valori di input hanno fatto la differenza, determinando, nel caso concreto, l'adozione della decisione (ad esempio, il prestito rifiutato sarebbe stato accettato qualora il reddito avesse raggiunto una certa soglia);

ii) Spiegazione causale. Si concentra sulle cause, piuttosto che su correlazioni meramente statistiche (ad esempio, il rifiuto di un prestito può essere spiegato causalmente dalla situazione finanziaria del richiedente, non dal tipo di attività su Facebook che è comune ai mutuatari inaffidabili);

iii) Spiegazione sociale. Adotta un approccio interattivo e conversazionale, in cui le informazioni sono veicolate adattandole alle convinzioni e alle capacità di comprensione del destinatario (per esempio, la banca potrà dare informazioni diverse all'investitore professionale e al comune cittadino).

La spiegazione è un valore sia per le decisioni umane sia per quelle automatiche. Tuttavia, in entrambi i casi, la spiegabilità presenta limiti e comporta costi, seppure diversi. Al riguardo è importante la distinzione tra spiegazioni generaliste e individualizzate.

Le prime comportano un costo fisso (la predisposizione *ex ante* della spiegazione) e un costo marginale vicino a 0 (i costi di comunicare la spiegazione, possibilmente selezionando gli aspetti più rilevanti per il destinatario).

Le seconde, accanto al costo fisso, possono comportare un elevato costo marginale (il costo di estrarre, elaborare e presentare specifici elementi relativi al caso concreto).

Nel caso delle decisioni umane, l'efficacia di ciascuna spiegazione dipende in modo significativo dalle capacità, disponibilità e inclinazioni del decisore. In ogni caso, a ogni spiegazione individualizzata debbono essere dedicate significative risorse di tempo ed energia.

Quanto più la decisione si basa su parametri non rigidamente prefissati, tanto più la spiegazione riflette criteri astratti, che potrebbero essere applicati in modi diversi.

Diversamente, nel caso delle decisioni automatiche, una volta che si sia realizzato un meccanismo per generare spiegazioni individualizzate, anche il costo marginale delle singole spiegazioni tenderà a 0. Quindi, in linea di principio, ogni decisione potrebbe essere accompagnata da una spiegazione individualizzata.

Tuttavia, la predisposizione di un meccanismo per generare spiegazioni individualizzate potrebbe rivelarsi costoso. Da un lato, lo sviluppo di un software per la spiegazione può richiedere un investimento notevole. Dall'altro lato, la possibilità di sviluppare spiegazioni dettagliate e significative dipende dalla tecnologia adottata nel processo decisionale. Come osservato in precedenza, spesso accade che i sistemi che garantiscono maggiore accuratezza – come le reti neurali profonde – siano quelli meno spiegabili. In tali casi, bisogna affrontare il difficile bilanciamento tra esigenze di accuratezza e trasparenza, e determinare quale riduzione nelle prestazioni del sistema sia accettabile a fronte di una maggiore spiegabilità.

Abbiamo visto come, anche per i sistemi opachi è possibile offrire spiegazioni, seppure limitate alla relazione tra possibili input e output del sistema (ad esempio, tramite spiegazione contrastiva). Ne discende che, la spiegabilità potrebbe fondare solo un obbligo di migliore sforzo (*Best Effort*). La spiegazione deve essere sviluppata nella misura in cui ciò sia possibile senza compromettere eccessivamente l'efficacia del sistema e senza generare costi insostenibili (non compatibili con le risorse disponibili e le esigenze di commercializzazione).

Lo scenario appena descritto è stato superato, almeno in parte, grazie ai grandi modelli linguistici (large language models-LLM). È vero che sviluppare una spiegazione significativa sulla base del funzionamento interno agli LLM (che consistono di enormi reti neurali profonde) sembra una sfida impossibile. Tuttavia, gli LLM offrono nuove possibilità: visto che sono capace di interagire con noi in linguaggio naturale, perché non chiedere loro di spiegare i propri risultati? Al riguardo diverse prospettive sono possibili. Data la novità del tema, sul quale non vi sono ancora contributi specificamente giuridici, ci limiteremo ad alcune considerazioni generali. La risposta di questi sistemi è guidata dalla richiesta-suggerimento (*prompt*) fornito dall'utente. Al riguardo si può distinguere tra lo 0-shot prompting, basato solo sulla conoscenza generale del sistema (Qual è la capitale della Francia?) e l'n-shot prompting, che include uno o più esempi di risposta corretta a quesiti simili (Berlino è la capitale della Germania. Qual è la capitale della Francia?). Presentando all'LLM esempi opportuni, si avranno risposte che riflettono quegli esempi. Per ottenere spiegazioni, oltre a fornire esempi, può essere utile ricorrere alla strategia della catena di ragionamento (*chain of thought*), in cui oltre a fornire al sistema un quesito, si specificano i passaggi attraverso i quali si è risolto un caso simile, o semplicemente si chiede al sistema di ragionare passo dopo passo. Inoltre si può chiedere al sistema di adottare un ruolo particolare (e.g., quello di un giudice o di un avvocato), così da sviluppare ragionamenti corrispondenti a quel ruolo. Gli LLM mostrano sorprendenti competenze nel giustificare le proprie conclusioni, che sollevano questioni alle quali è difficile trovare una risposta. Ci si può chiedere in che misura il procedimento passo dopo passo rifletta il ragionamento dell'LLM per raggiungere le proprie conclusioni o se invece si tratti di una razionalizzazione *ex post*. Altre tecniche, ancor più sofisticate sono state sviluppate per indirizzare l'LLM nel ragionamento e nella giustificazione, come quella dell'albero di pensieri, dove si chiede all'LLM di sviluppare diversi argomenti e confrontarli.

3. Art. 22 GDPR: il divieto di decisioni automatiche

Le considerazioni fin qui sviluppate ci possono guidare nell'analisi e nell'interpretazione della disciplina europea. Tale disciplina non esclude l'uso dell'intelligenza artificiale, ma ne regola l'uso affinché sia compatibile con i valori del diritto.

La norma che più direttamente affronta il tema è l'Art. 22 GDPR. Tale norma mira a consentire all'interessato di esercitare un controllo effettivo sulle decisioni che lo riguardano. Inoltre, si propone di limitare i rischi di trattamento automatico iniquo o discriminatorio. L'articolo 22 corrisponde al precedente articolo 15 della Direttiva del 1995, sulla cui base era stato emanato l'articolo 14

del nostro vecchio codice Privacy. Tali norme avevano suscitato un notevole interesse nella dottrina, ma avevano trovato scarsissima applicazione nella pratica del diritto. Solo negli anni più recenti, grazie all'IA, la decisione automatica ha acquisito rilievo giuridico e sociale, divenendo un tema centrale della regolazione della protezione dei dati e dell'IA stessa.

Rispetto alle precedenti norme, l'Art. 22 presenta alcune significative novità: (a) il riferimento alla profilazione, quale elemento del processo automatizzato, (b) la necessità che il consenso sia esplicito, (c) il diritto di ottenere un intervento umano e di esprimere il proprio punto di vista e contestare la decisione, e (d) il divieto di basare la decisione su dati sensibili. La nuova disposizione, destinata ad operare in un contesto socio-tecnologico in cui le decisioni automatizzate sono sempre più frequenti e significative, sta già avendo un significativo impatto sulle pratiche commerciali e amministrative. La stessa Corte di Giustizia, come vedremo, ha avuto modo di occuparsene.

3.1. Il divieto di decisioni automatizzate

Il primo comma dell'articolo 22 GDPR stabilisce che l'interessato «ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione», che produca effetti giuridici, o incida in modo significativo, sull'interessato stesso.

Si è osservato che tale formulazione, richiamando un “diritto”, potrebbe essere interpretata nel senso di conferire il potere di opporsi a tali decisioni, che sarebbero generalmente ammissibili fintanto che l'interessato non vi si opponga. È tuttavia preferibile l'opinione secondo cui l'articolo 22(1) introduce un divieto rivolto ai titolari del trattamento: le decisioni basate unicamente sul trattamento automatizzato sono quindi vietate, salvo i casi in cui rientrino in una delle eccezioni di cui al comma 2, anche in assenza di un'opposizione da parte dell'interessato.

Questa interpretazione è stata accolta dal Gruppo di Lavoro dell'Articolo 29, secondo cui «di norma, esiste un divieto generale di prendere decisioni individuali completamente automatizzate, compresa la profilazione, che abbiano effetti giuridici, o similmente significativi». L'art. 21, par. 1 parrebbe invece assumere la liceità di inferenze automatiche in assenza di opposizione, prevedendo espressamente il diritto di opporsi alla profilazione, senza la necessità di addurre specifiche motivazioni, nei casi in cui il trattamento si fondi sulle ragioni di cui all'articolo 6(1) lett. e) (esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri) o f) (interesse legittimo). Le due disposizioni si riconciliano considerando che non tutte le profilazioni sono decisioni vietate dall'articolo 22. Non rientrano infatti nell'ambito applicativo della norma

le inferenze (profilazioni) sugli individui che non conducano a decisioni, né quelle che pur comportando decisioni non abbiano l'importanza e la significatività richieste.

3.2. Le condizioni per il divieto

Per l'applicazione del divieto di cui all'Art. 22, par. 1, è necessario che si verifichino tre condizioni: (1) deve essere presa una decisione, (2) tale decisione deve essere basata esclusivamente sul trattamento automatizzato, e (3) deve avere effetti giuridici, o in ogni caso significativi, sull'interessato. È dubbio se sia necessaria un'ulteriore condizione, vale a dire che (4) l'elaborazione includa la profilazione.

La prima condizione – che sia stata presa una decisione – richiede che si adotti una determinazione rispetto a un individuo, e che questa determinazione possa condurre ad un'azione (come avviene qualora si assegni un punteggio che esprime una valutazione sull'interessato).

Il Regolamento non distingue tra decisioni di natura pubblica o privata. Nel silenzio del testo dobbiamo dunque ritenere che esso si rivolga alle determinazioni adottate sia nella sfera di autonomia dei privati, sia nell'esercizio di poteri pubblici.

La seconda condizione – che la decisione sia basata esclusivamente sul trattamento automatizzato – richiede che esseri umani non esercitino una reale influenza sull'esito del processo decisionale. Questa condizione si realizza anche quando la decisione finale sia attribuita solo formalmente ad una persona, ma sia di fatto affidata al sistema. Si pensi al caso il cui l'esame di una richiesta di mutuo sia formalmente affidato al funzionario bancario competente, il quale però si uniformi acriticamente alle valutazioni dell'IA. Analoga è l'ipotesi in cui al funzionario sia consentito discostarsi dalla valutazione automatica solo a patto di un'assunzione di responsabilità (civile, penale o amministrativa), capace di avere conseguenze particolarmente gravose. Va inoltre considerato che, in questi casi è la struttura stessa dei processi decisionali che spesso “potenzia” – attraverso meccanismi di influenza non coercitiva (il cosiddetto nudging) – l'indicazione del sistema, rendendola di fatto una decisione automatica. Si pensi al caso in cui la determinazione automatizzata sia posta come scelta predefinita (di “default”) e invece la possibilità di discostarsi comporti un onere motivazionale o un'assunzione di responsabilità specifica.

La stessa condizione, invece, non è soddisfatta – la decisione non è basata esclusivamente sul trattamento automatizzato – qualora il sistema sia utilizzato solo come supporto decisionale ed esseri umani siano responsabili della deci-

sione, e deliberino nel merito di ogni singolo caso, decidendo autonomamente se accogliere o rifiutare i suggerimenti del sistema.

La terza condizione – che la decisione abbia effetti significativi – richiede che quest'ultima produca effetti giuridici o influisca in modo rilevante sull'interessato.

Il Considerando 71 menziona due esempi di decisioni di tale tipo: il rifiuto automatico di una domanda di credito online e le pratiche di assunzione elettronica. È stato affermato che per essere significativi gli effetti non possano riguardare esclusivamente la sfera emotiva. Si è altresì rilevato che la pubblicità mirata di regola non possa generare effetti di sufficiente rilevanza, «salvo che l'invio di messaggi pubblicitari comporti una discriminazione palesemente iniqua, nella forma di pratiche di trattamento sfavorevole nelle transazioni online (*weblining*), e tale discriminazione abbia conseguenze economiche non banali». Ciò si verificherebbe, per esempio, qualora l'interessato dovesse pagare un prezzo significativamente più elevato per taluni beni o servizi rispetto al prezzo proposto ad altri individui.

Come accennato in precedenza, è dubbio se sia altresì necessaria una quarta condizione, vale a dire che il processo decisionale automatizzato includa la profilazione dell'interessato, cioè un'inferenza che, sulla base dei suoi dati personali, gli attribuisca ulteriori caratteristiche e attitudini. Più esattamente, secondo il Considerando 71, la profilazione «consiste in una forma di trattamento automatizzato dei dati personali che valuta aspetti personali concernenti una persona fisica, in particolare al fine di analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato».

L'interpretazione secondo cui la profilazione è condizione necessaria è suggerita dal Considerando 71, secondo il quale il trattamento automatizzato di cui all'Art. 22(1) include la profilazione. È peraltro possibile una diversa interpretazione, secondo cui l'articolo 22 comprende, accanto alle decisioni basate sulla profilazione, anche le decisioni non basate su di essa. Tale ipotesi è suggerita dalla formulazione del comma (1) dell'articolo 22, dove una virgola separa i termini «trattamento automatizzato» dalle parole «compresa la profilazione». Ciò potrebbe far ritenere che, contrariamente a quanto appena affermato, la profilazione sia solo una componente opzionale delle decisioni automatizzate proibite dall'Art.22(1). La differenza tra le due interpretazioni è raramente rilevante, poiché la profilazione è un elemento caratteristico della maggior parte delle decisioni automatizzate. Un caso limite (nel quale si ha decisione automatica senza profilazione) potrebbe consistere nell'irrogazione automatica di san-

zioni a seguito della rilevazione di un eccesso di velocità di veicolo mediante sensore. Oggi, molte decisioni adottate dai sistemi di intelligenza artificiale ricadono nell'ambito applicativo dell'articolo 22(1).

4. Art. 22 GDPR: eccezioni e misure di salvaguardia

Il divieto di decisioni automatiche incontra eccezioni, cui debbono però accompagnarsi misure di salvaguardia.

4.1. Le eccezioni al divieto

Secondo il par. 2 dell'articolo 22 il divieto di decisioni automatizzate non si applica quando: «la decisione (a) sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento; (b) sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato; o (c) si basi sul consenso esplicito dell'interessato». L'eccezione di cui alla lettera (a) fa sì che processi decisionali automatizzati siano consentiti anche in settori chiave quali, per esempio, il reclutamento di personale e la concessione di prestiti. Tuttavia, affinché l'eccezione sia applicabile, le decisioni automatizzate devono essere “necessarie”. Il carattere di necessità potrebbe dipendere, dal numero estremamente elevato di casi da esaminare. Si consideri, ad esempio, l'ipotesi in cui si debba valutare un numero molto elevato di candidature per una posizione lavorativa. La necessità potrebbe anche dipendere dall'abilità di tali tecnologie di superare le capacità cognitive e di giudizio degli esseri umani. In alcuni casi, infatti, il coinvolgimento umano potrebbe non garantire un livello più elevato di protezione degli interessati, e sarebbe quindi superfluo o addirittura disfunzionale rispetto ai valori sociali, politici e giuridici in gioco. Per esempio, decisioni automatizzate potrebbero meglio promuovere e garantire «la parità di opportunità» per tutti i candidati ad una certa posizione.

L'eccezione di cui alla lettera (b) consente agli Stati membri di ricorrere a decisioni automatizzate, a condizione che siano adottate adeguate misure di tutela. Il Considerando 71 indica quali esempi il monitoraggio e la prevenzione delle frodi e dell'evasione fiscale.

L'eccezione di cui alla lettera (c) fa riferimento al “consenso esplicito” dell'interessato. Il consenso è definito in generale dall'Art. 4 n. 11 del Regolamento che lo caratterizza come «qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manife-

sta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento».

L'Art. 22 parla di consenso "esplicito" quale qualificazione ulteriore rispetto agli elementi già inclusi nella definizione dell'Art- 4, n. 11. Tale formulazione ricorre in varie ipotesi nelle quali, come osserva l'Articolo 29WP «emergono seri rischi per la protezione dei dati» e quindi «un livello alto di controllo individuale sui dati personali si ritiene appropriato». Sempre secondo l'Articolo 29WP, il termine "esplicito" si riferisce al modo in cui il consenso è espresso dall'interessato. In particolare, tale termine indica che «l'interessato deve esprimere una dichiarazione esplicita di consenso», ad esempio mediante forma scritta. Il fatto che il consenso sia esplicito non fa venir meno il generale requisito della libertà dello stesso. Si consideri, ad esempio, il caso in cui una NGO utilizzi un metodo automatizzato per classificare (profilare) taluni richiedenti e determinarne lo stato di bisogno, così da poter decidere se assegnare loro dei benefici. In tal caso, è dubbio che il consenso di un richiedente possa essere considerato libero, poiché non acconsentire comporterebbe l'esclusione certa dal beneficio.

4.2. Le misure di salvaguardia

Nei casi di cui all'articolo 22(2), lettere (a) e (c) – quando la decisione basata unicamente sul trattamento automatizzato sia necessaria per la conclusione o l'esecuzione di un contratto o si basi sul consenso dell'interessato – il paragrafo 3, richiede l'adozione di misure di salvaguardia adeguate.

Nei casi di cui al paragrafo 2, lettere a) e c), il titolare del trattamento attua misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione.

Le misure di salvaguardia sono previste anche nel caso dell'eccezione di cui alla lettera b), cioè per i trattamenti automatizzati autorizzati dal diritto europeo o nazionale.

Secondo il gruppo di lavoro dell'Articolo 29WP, alcune di queste misure, volte a ridurre i rischi delle decisioni automatizzate, includono ad esempio i controlli di garanzia e qualità, le procedure di audit degli algoritmi, la minimizzazione, pseudonimizzazione e anonimizzazione dei dati e i meccanismi di certificazione. Tali misure dovrebbero garantire che i requisiti stabiliti dal Considerando (71) – rispetto a correttezza, accuratezza e affidabilità delle decisioni algoritmiche – siano rispettati. Secondo il Considerando «è opportuno che il titolare del trattamento utilizzi procedure matematiche o statistiche appropriate per la profilazione, metta in atto misure tecniche e organizzative adeguate al fine di

garantire, in particolare, che siano rettificati i fattori che comportano inesattezze dei dati e sia minimizzato il rischio di errori e al fine di garantire la sicurezza dei dati personali secondo una modalità che tenga conto dei potenziali rischi esistenti per gli interessi e i diritti dell'interessato e che impedisca tra l'altro effetti discriminatori nei confronti di persone fisiche sulla base della razza o dell'origine etnica, delle opinioni politiche, della religione o delle convinzioni personali, dell'appartenenza sindacale, dello status genetico, dello stato di salute o dell'orientamento sessuale, ovvero che comportano misure aventi tali effetti». Questa parte del Considerando (71), sebbene non sia stata inserita nel testo dell'articolo 22, mantiene una valenza interpretativa estremamente rilevante, al fine di evitare decisioni algoritmiche arbitrarie, basate su pregiudizi o discriminazioni. Secondo il gruppo di lavoro dell'Art. 29WP, il titolare ha l'obbligo di dimostrare che i dati di input non siano «inesatti o irrilevanti o estrapolati dal contesto». È inoltre necessario dimostrare che tali dati non violino «le ragionevoli aspettative degli interessati», in relazione allo scopo per cui sono stati raccolti. Nei sistemi basati sull'apprendimento automatico, ciò dovrebbe applicarsi non solo ai dati riguardanti l'interessato coinvolto in una particolare decisione, ma anche ai dati degli insiemi di addestramento, dove la presenza di eventuali pregiudizi e bias può influenzare il modello algoritmico, e ripercuotersi quindi sull'accuratezza delle inferenze automatizzate.

Altre misure derivano da ulteriori disposizioni del GDPR, in particolare gli Art. 13, 14 e 15, e riguardano l'interazione con gli interessati, come il diritto di avere accesso ai sistemi di decisione, di ottenere l'intervento del titolare, di esprimere la propria opinione, di ottenere «informazioni significative sulla logica utilizzata» per la decisione e su tale base di contestare la decisione stessa. Per esempio, quando una decisione automatizzata sia comunicata all'interessato, si potrebbero fornire sia un link che consenta l'accesso a un processo di revisione della decisione, secondo tempistiche predefinite, sia l'indicazione di un punto di contatto per eventuali chiarimenti.

La previsione di una procedura di ricorso è particolarmente importante rispetto alle decisioni adottate da sistemi ad elevata opacità, incapaci di fornire spiegazioni e giustificazioni che siano comprensibili e significative per un essere umano.

4.3. Decisioni basate su dati sensibili

L'articolo 22, par. 4 introduce il divieto di basare le decisioni automatizzate su “dati sensibili”, vale a dire sulle categorie speciali di dati di cui all'articolo 9, par. 1 GDPR: «Le decisioni di cui al paragrafo 2 non si basano sulle categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, a meno che non sia

d'applicazione l'articolo 9, paragrafo 2, lettere a) o g), e non siano in vigore misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato" A tale divieto fanno eccezione i casi in cui l'interessato abbia dato il proprio consenso esplicito (articolo 9(2) lettera (a)) o il trattamento sia necessario per ragioni di pubblico interesse (articolo 9, par. 2, lettera g). Si noti che anche quando l'interessato abbia dato il proprio consenso, la decisione automatica può essere illecita, per esempio in quanto discriminatoria.

Le tecnologie dell'IA mettono in discussione l'applicabilità del divieto di trattamento di dati sensibili. In primo luogo, i dati sensibili possono essere inferiti probabilisticamente a partire da dati non sensibili. Per esempio, l'orientamento sessuale di un individuo può essere desunto sulla base delle sue attività online, come le ricerche su Internet, i like sui profili dei social network. In tal caso, l'inferenza di tali dati dovrebbe essere considerata come trattamento di dati sensibili, e quindi illecita, a meno che non siano soddisfatte le condizioni di cui all'Art. 9.

In secondo luogo, i dati non sensibili possono fungere da proxy per i dati sensibili a essi correlati, anche se questi ultimi non sono inferiti dal sistema. Per esempio, il luogo di residenza può comportarsi da sostituto (proxy) per l'etnia. Decisioni basate su dati sensibili potrebbero, dare luogo a casi di discriminazione.

5. Art. 22 GDPR: un diritto alla spiegazione?

Una delle questioni maggiormente dibattute rispetto al GDPR concerne l'esistenza di un diritto alla spiegazione.

5.1. Un conflitto tra considerandi e articolato?

Per comprendere se il GDPR conferisce il diritto degli interessati di ottenere una spiegazione è necessario confrontare l'articolo 22 e il Considerando (71).

Secondo il Considerando (71), le decisioni basate unicamente sul trattamento automatizzato debbono essere accompagnate da garanzie adeguate, tra cui: (a) informazioni specifiche all'interessato, (b) il diritto di ottenere l'intervento umano, (c) il diritto di esprimere la propria opinione, (d) il diritto di ottenere una spiegazione della decisione conseguita dopo tale valutazione, e infine (e) il diritto di contestare la decisione.

Diversamente, secondo l'Art. 22 GDPR, misure appropriate per tutelare i diritti, le libertà e i legittimi interessi degli interessati includono "almeno": (a) il diritto di ottenere l'intervento umano da parte del titolare, (b) di esprimere la propria opinione, e (c) di contestare la decisione. Dall'analisi comparativa dei

due testi appare evidente come nell'Art. 22 GDPR siano stati omessi due elementi, presenti invece nel considerando (71), vale a dire (1) l'obbligo del titolare di fornire «informazioni specifiche all'interessato» e (2) il diritto di quest'ultimo di «ottenere una spiegazione della decisione conseguita dopo tale valutazione».

La prima omissione non è particolarmente significativa dal momento che, come precedentemente osservato, l'obbligo del titolare di fornire informazioni è già stabilito dagli articoli 13, 14 e 15 GDPR, anche se il requisito della specificità delle informazioni è enunciato unicamente nel Considerando (71).

La seconda omissione è più problematica e solleva la questione di determinare se i titolari del trattamento abbiano o meno l'obbligo giuridico di fornire una spiegazione individualizzata. A tale riguardo, due sono le interpretazioni possibili. Secondo una prima interpretazione, il legislatore europeo, inserendo il diritto alla spiegazione nel solo Considerando (71), e omettendolo negli articoli del GDPR, intendeva veicolare un duplice messaggio: da un lato, escludere un obbligo giuridico coercibile di fornire spiegazioni individualizzate, e dall'altro, raccomandare ai responsabili del trattamento di fornire tali spiegazioni quando possibile, secondo le proprie determinazioni discrezionali.

Quindi, secondo questa interpretazione, fornire una spiegazione individualizzata costituirebbe semplicemente una buona prassi e non un requisito giuridicamente vincolante.

Un'altra possibile interpretazione è che il legislatore europeo intendesse, al contrario, stabilire un obbligo giuridico coercibile di fornire spiegazioni individualizzate, senza tuttavia gravare indebitamente sui titolari. Questa interpretazione sembra essere supportata dall'uso dell'avverbio “almeno”, che precede il riferimento al «diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione, e di contestare la decisione». Tale avverbio sembra suggerire che alcuni titolari del trattamento siano giuridicamente tenuti ad adottare misure di garanzia ulteriori, compresa, possibilmente, la prestazione di spiegazioni individualizzate, come indicato nel considerando (71). Quindi, secondo tale interpretazione, una spiegazione sarebbe giuridicamente necessaria ogniqualvolta sia possibile alla luce degli sviluppi tecnologici, dei costi e delle pratiche aziendali. Entrambe le interpretazioni – relative alla lettura combinata degli articoli 13, 14, 15 e 22 GDPR – appaiono possibili. È probabile che la ragione di tale ambiguità derivi da un'incertezza del legislatore rispetto all'opportunità di introdurre un obbligo giuridico di fornire spiegazioni individualizzate.

Come osservato da alcuni, l'opinione secondo cui gli interessati sarebbero titolari di un diritto ad ottenere spiegazioni personalizzate ai sensi del GDPR potrebbe, in futuro, essere avallata in via interpretativa dalle autorità per la protezione dei dati e dalle autorità giudiziarie. Tali autorità potrebbero ritenere che la

possibilità di ottenere una spiegazione individualizzata sia una precondizione per l'esercizio effettivo del diritto di contestare le decisioni automatizzate. Il diritto alla spiegazione è infatti connesso ai diritti a un equo processo e a un ricorso effettivo, rispettivamente sanciti dagli articoli 6 e 13 della Convenzione europea dei Diritti dell'Uomo.

Nonostante sia indubbia l'importanza della spiegazione individualizzata, essa non si configura quale rimedio generale rispetto a possibili pregiudizi, malfunzionamenti e applicazioni inappropriate delle tecnologie dell'IA.

L'efficacia della spiegazione incontra infatti limiti analoghi a quelli relativi al consenso, poiché tali strumenti di tutela si basano entrambi sull'iniziativa informata dell'interessato. È stato spesso osservato che il consenso non fornisce una protezione efficace, dato che gli interessati si trovano in una posizione di inferiorità rispetto alle conoscenze tecnologiche e giuridiche e al potere di fatto dei titolari. Inoltre, essi dispongono di tempo e energie limitate, e non sono in grado di perseguire in modo coordinato i propri interessi. Tale valutazione è applicabile anche al diritto alla spiegazione che rischia di essere scarsamente utilizzato. Inoltre, anche qualora le spiegazioni evidenziassero potenziali difetti delle decisioni automatizzate, gli interessati potrebbero non essere in grado di ottenere nuove decisioni più soddisfacenti.

5.2. Contenuto e significato del diritto alla spiegazione

Come osservato nelle sezioni precedenti, restano aperti numerosi interrogativi circa l'esistenza e il contenuto del diritto all'informazione/spiegazione.

Per chiarire innanzitutto il quadro normativo riassumiamo di seguito i principali riferimenti nel GDPR.

– Secondo gli articoli 13 e 14 (sul diritto all'informazione) e 15 (sul diritto di accesso), il titolare deve dare informazioni circa l'esistenza di un processo decisionale automatizzato, compresa la profilazione, di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato»;

– Secondo l'articolo 22, l'interessato ha «il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione»;

– Secondo il Considerando 71 l'interessato dovrebbe avere anche il diritto di ottenere specifiche informazioni e «una spiegazione della decisione [...] e di contestare la decisione». A tale riguardo, l'Articolo 29 WP/251 (p. 25) afferma che i titolari dovrebbero fornire agli interessati, in modo semplice, le ragioni o i criteri su cui si basa la decisione. Tali informazioni dovrebbero essere esaustive così da consentire agli interessati di comprendere i motivi della decisione.

Infine, l'articolo 7, par. 4 (a) della Direttiva sui diritti dei consumatori disciplina l'informazione che deve essere fornita ai consumatori rispetto alle offerte online, spesso basate sulla profilazione. Tale articolo, nella versione emendata dalla Direttiva (UE) 2019/2161, stabilisce che il professionista deve indicare i «parametri principali che determinano la classificazione dei prodotti presentati al consumatore come risultato della sua ricerca» e «l'importanza relativa di tali parametri rispetto ad altri parametri».

In base a questo insieme di norme, l'obbligo informazione può assumere contenuti molto diversi e riguardare:

1. informazioni sull'esistenza della profilazione e della conseguente decisione automatizzata, vale a dire sul fatto che l'interessato sarà profilato o è già soggetto a profilazione, e che ciò potrà condurre ad una decisione nei suoi riguardi;
2. informazioni generali sulle finalità della profilazione e del processo decisionale;
3. informazioni generali sul tipo di approccio e di tecnologia adottati;
4. informazioni generali su quali dati di input (predittori) e risultati (obiettivi/previsioni), e quali categorie di dati vengono prese in considerazione;
5. informazioni generali sull'importanza relativa di tali dati di input nella determinazione dei risultati;
6. informazioni specifiche su quali dati sono stati raccolti sull'interessato e quali utilizzati per la sua profilazione;
7. indicazioni specifiche su quali caratteristiche dell'interessato, e quali valori delle stesse, hanno determinato la decisione nei suoi riguardi;
8. informazioni specifiche sui dati dell'interessato ottenuti mediante processi di inferenza;
9. informazioni specifiche sul processo di inferenza mediante il quale certi valori attribuiti alle caratteristiche dell'interessato hanno determinato una specifica decisione nei suoi riguardi.

In questo elenco, le informazioni enunciate nei punti da (1) a (5) riguardano informazioni generaliste *ex ante*, che dovrebbero essere date all'interessato prima che i suoi dati siano raccolti, o in ogni caso, elaborati.

Diversamente, le informazioni contenute nei punti da (6) a (9) riguardano obblighi informativi individualizzati *ex post*, vale a dire successivi alla raccolta, all'analisi e all'utilizzo dei dati.

Ex ante, il titolare del trattamento è senza dubbio tenuto a comunicare all'interessato le informazioni di cui ai punti (1) e (2). Le informazioni di cui al punto (3) dovrebbero essere fornite qualora la metodologia e la tecnologia adottate comportino una differenza significativa nel risultato della decisione (ad esempio, quando siano inappropriate o possano condurre a errori e pregiudizi).

Anche le informazioni di cui al punto (4) dovrebbero essere comunicate all'interessato, poiché queste costituiscono una sorta di minimo resoconto della "logica" alla base del trattamento, almeno relativamente ai tipi di dati utilizzati quali input per le decisioni del sistema.

Questa prospettiva è stata esplicitamente adottata dal California Consumer Privacy Act, che alla Sezione 1798.100 (b) richiede ai titolari del trattamento di «informare i consumatori sulle categorie di informazioni personali raccolte».

Ci si può domandare se vi sia anche un obbligo di comunicazione delle informazioni di cui al punto (5), poiché rilevanti rispetto alla "logica" del trattamento, sebbene possa risultare difficile determinare in astratto (senza cioè fare riferimento a un caso specifico) l'importanza di un certo fattore.

Ex post, dovrebbero essere comunicati all'interessato tutti i dati di cui al punto (6), in quanto oggetto del diritto di accesso. Se assumiamo, inoltre, l'esistenza del diritto di ottenere una spiegazione personalizzata, anche le informazioni di cui al punto (7) diventerebbero necessarie. Una spiegazione individualizzata potrebbe anche richiedere la comunicazione delle informazioni di cui al punto (8), vale a dire informazioni specifiche sui dati dell'interessato ottenuti mediante processi di inferenza, quando le conclusioni intermedie del sistema assumano un ruolo decisivo per la decisione. Infine, potrebbero essere comunicate anche le informazioni di cui al punto (9), sebbene, in via generale, le informazioni relative ai punti (7) e (8) dovrebbero essere sufficienti a fornire spiegazioni personalizzate adeguate. Le informazioni di cui sopra devono essere integrate con ulteriori informazioni nel caso di decisioni da parte di autorità pubbliche.

In tale contesto, l'obbligo di motivazione degli atti e dei provvedimenti amministrativi impone un riferimento alle norme applicate e ai poteri esercitati.

5.3. Questioni aperte sul diritto alla spiegazione nel GDPR

Data la varietà dei processi decisionali automatizzati, è difficile specificare in termini generali e al tempo stesso precisi quali informazioni debbano essere obbligatoriamente comunicate all'interessato. Le informazioni che il titolare del trattamento può essere ragionevolmente tenuto a fornire dipendono dall'importanza della decisione, dall'ampiezza della discrezionalità della stessa e dalla fattibilità tecnologica di fornire una spiegazione adeguata, senza costi eccessivi. Tuttavia, agli interessati che abbiano ottenuto una decisione diversa rispetto a quanto sperato, dovrebbero essere comunque date informazioni specifiche e rilevanti, così da metterli in condizione di capire quali dati personali abbiano determinato l'esito sfavorevole. I fattori causalmente rilevanti potrebbero essere identificati osservando quali valori non comuni possano spiegare l'esito della decisione.

Si consideri per esempio il caso di un individuo con un reddito di ammontare medio e un'ipoteca in corso, la cui richiesta di un nuovo mutuo ipotecario venga respinta. Si esaminino le seguenti ipotesi: (a) se l'individuo avesse avuto un reddito molto più elevato, la sua domanda sarebbe stata accettata indipendentemente dall'ipoteca in corso e (b) l'assenza di tale ipoteca avrebbe determinato l'accettazione della nuova domanda a fronte del reddito di ammontare medio dell'individuo. In tali circostanze, diremmo che era l'ipoteca in corso, piuttosto che il reddito di ammontare medio, il motivo principale o la causa che spiega perché la domanda di mutuo è stata respinta. Tale fattore giustifica, infatti, lo scostamento dal risultato standard in un caso di questo tipo.

Nonostante le importanti indicazioni contenute nel Regolamento, le decisioni automatizzate sollevano un insieme di questioni di fondo, a cui il sistema giuridico non ha ancora dato una risposta adeguata.

Sul tema della spiegazione è intervenuto il Gruppo di Lavoro dell'Articolo 29 (WP/251, p. 25), affermando che in ogni caso i titolari dovrebbero fornire agli interessati, in modo semplice, le ragioni o i criteri su cui si basa la decisione. Tali informazioni dovrebbero essere esaustive, così da consentire agli interessati di comprendere i motivi della decisione. Resta da stabilire se una spiegazione generalista possa rispondere alle esigenze avanzate dal Gruppo di Lavoro.

La Corte di Giustizia si è occupata recentemente del tema della decisione automatica nel caso Schufa, una società privata di diritto tedesco che fornisce ai propri clienti (spesso istituti bancari) informazioni sul merito creditizio di terzi, in particolare di consumatori. A tal fine, Schufa effettua un pronostico sulla probabilità che il terzo sia in grado di restituire un credito a partire da talune informazioni che lo riguardano (in particolare, ma non solo, la sua situazione finanziaria) secondo procedure automatizzate.

Nel caso di specie, una persona non aveva ottenuto, da una banca, il credito richiesto in ragione del punteggio di affidabilità creditizia attribuitogli da Schufa.

Tale persona aveva chiesto a Schufa di fornire le informazioni cui il destinatario di una decisione automatica ha diritto di avere in base all'Art. 22 GDPR.

Schufa negava di essere soggetta all'Art. 22, in quanto non aveva adottato alcuna decisione automatica sulla concessione del credito, ma si era limitata a fornire alla banca la propria valutazione di affidabilità.

La Corte risolveva la questione affermando che l'Art. 22, doveva essere interpretato nel senso che:

il calcolo automatizzato, da parte di una società che fornisce informazioni commerciali, di un tasso di probabilità basato su dati personali relativi a una persona e riguardanti la capacità di quest'ultima di onorare in futuro gli impegni di pagamento costituisce un «processo decisionale automatizzato relativo alle persone fisiche», ai

sensi di tale disposizione, qualora da tale tasso di probabilità dipenda in modo decisivo la stipula, l'esecuzione o la cessazione di un rapporto contrattuale con tale persona da parte di un terzo, al quale è comunicato tale tasso di probabilità.

Quindi le tutele stabilite dall'Art. 22 si applicano anche alle valutazioni automatiche preliminari, che abbiano un'influenza decisiva sulla determinazione finale, anche quando tale determinazione sia affidata ad una persona.

6. Art. 86 AIA: un diritto alla spiegazione?

L'AI Act non affronta in termini generali il tema della decisione automatica, ma dedica l'Art. 86 al tema della spiegazione.

6.1. Il diritto alla spiegazione nell'Art 86 AIA

Il primo comma stabilisce che ogni persona ha il diritto di ottenere dal deployer una spiegazione chiara e significativa di una decisione automatica qualora tale decisione: i) si basi sull'output di un sistema di intelligenza artificiale (IA) ad alto rischio di cui all'allegato III (esclusi quelli di cui al punto 2), e ii) produca effetti giuridici o abbia un impatto negativo sulla salute, sulla sicurezza o sui diritti fondamentali.

I successivi commi 2 e 3 restringono l'obbligo del deployer, escludendone i casi in cui i) il diritto nazionale o dell'Unione Europea prevedano eccezioni o limitazioni, ii) il diritto dell'Unione già preveda il diritto alla spiegazione.

L'Art. 86 non figurava nella proposta originaria della Commissione, che si limitava a prevedere obblighi informativi per il developer. È stato introdotto successivamente, a seguito di un emendamento del Parlamento europeo.

Nel garantire la trasparenza dell'IA, l'art. 86 opera in combinazione con altre disposizioni dell'AIA, in particolare con l'Articolo 13(1), secondo cui i sistemi ad alto rischio devono essere progettati e sviluppati in modo che «il loro funzionamento sia sufficientemente trasparente da consentire ai deployer di interpretare l'output del sistema e utilizzarlo adeguatamente» (articolo 13(1)). Inoltre, tali sistemi devono essere accompagnati da «informazioni concise, complete, corrette e chiare che siano pertinenti, accessibili e comprensibili per i deployer» (Art.13(2)).

L'Art. 86 assegna dunque al diritto alla spiegazione un ambito applicativo limitato. Esso spetta a qualunque persona sia oggetto di una decisione automatica, purché siano soddisfatte due condizioni: la prima relativa al tipo di sistema su cui si basa la decisione, la seconda relativa all'impatto della decisione stessa. La norma prevede, inoltre, specifiche eccezioni e limitazioni, come illustrato nelle sezioni seguenti. In particolare, esamineremo l'Art. 86 rispetto a: a) l'ambi-

to soggettivo, b) l'ambito applicativo, c) gli impatti della decisione, d) il contenuto della spiegazione, le eccezioni e le limitazioni del diritto. Infine, analizzeremo il rapporto tra l'Articolo 86 e altre normative, in particolare il GDPR.

6.2. *L'ambito soggettivo*

Per quanto riguarda il titolare dell'obbligo di fornire la spiegazione (soggetto passivo del rapporto giuridico), l'Art. 86 utilizza il termine "deployer", ossia «una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo che utilizza un sistema di IA sotto la propria autorità, tranne nel caso in cui il sistema [...] sia utilizzato nel corso di un'attività personale non professionale» (Art. 3 (4)). Quindi, chiunque usi, per fini professionali, un sistema di IA per adottare decisioni, è, in linea di principio, soggetto all'obbligo di spiegazione. Più problematica è l'identificazione del titolare del diritto alla spiegazione (soggetto attivo). Nella versione italiana, l'Articolo 86 parla di "persona interessata", locuzione che richiama quella di "interessato" nel GDPR, riferita a «una persona fisica identificata o identificabile». Da qui la questione se il diritto alla spiegazione spetti solo alle persone fisiche, o si estenda a quelle giuridiche. Altre versioni linguistiche della norma sembrano opporsi a questa interpretazione. In quella inglese si usa il termine "affected person", che rinvia a ogni persona su cui la decisione produca effetti, senza distinguere tra persone fisiche (denotate nel GDPR con il termine "data subject") e giuridiche.

L'estensione del diritto anche alle persone giuridiche è supportata da considerazioni teleologiche: molte decisioni automatizzate, per esempio in ambito creditizio, hanno effetti diretti sulle persone giuridiche e, indirettamente, sulle persone fisiche che ne fanno parte (titolari, soci, dipendenti). Tuttavia, l'esclusione delle persone giuridiche potrebbe avere fondamento alla luce degli impatti considerati. Come vedremo nella sezione 6.3, il diritto alla spiegazione riguarda, oltre alle decisioni con effetti giuridici, solo quelle suscettibili di incidere sulla salute, la sicurezza e i diritti fondamentali, interessi che tipicamente appartengono alle persone fisiche. Tale interpretazione sembra essere confermata dall'Articolo 6(3), che restringe il concetto di alto rischio (di cui all'allegato III) ai sistemi capaci di generare danni per la salute, la sicurezza o i diritti fondamentali delle persone fisiche.

6.3. *Ambito applicativo: tipologie di sistemi*

Il diritto alla spiegazione si applica alle decisioni dei sistemi ad alto rischio elencati nell'allegato III. Sono esclusi quelli impiegati in infrastrutture critiche, ossia componenti di sicurezza destinati alla gestione e al funzionamento delle infrastrut-

ture digitali essenziali, del traffico stradale o della fornitura di acqua, gas, riscaldamento o elettricità. Pertanto, il diritto riguarda solo i sistemi che operano nelle seguenti aree: (1) biometria; (3) istruzione e formazione professionale; (4) occupazione, gestione dei lavoratori, e accesso al lavoro autonomo; (5) accesso e fruizione di servizi privati essenziali e di servizi pubblici essenziali e prestazioni pubbliche essenziali; (6) attività di contrasto; (7) migrazione e asilo, gestione e controllo delle frontiere; (8) amministrazione della giustizia e processi democratici.

L'inclusione nell'allegato III comporta solo una presunzione relativa di alto rischio, superabile a norma dell'Articolo 6(3) qualora il sistema non presenti «un rischio significativo di danno per la salute, la sicurezza o i diritti fondamentali delle persone fisiche, anche nel senso di non influenzare materialmente il risultato del processo decisionale».

Infine, sono esclusi dal diritto alla spiegazione tutti i sistemi di cui all'Art. 6(1), ossia quelli che costituiscono un prodotto regolato dalle normative di armonizzazione dell'Unione Europea secondo la «nuova cornice legislativa» (il c.d. «New Legislative Framework») o la componente di sicurezza di un siffatto prodotto. Queste normative sono elencate nell'Allegato I e tra queste figurano la Direttiva 2009/48/CE sulla sicurezza dei giocattoli e il Regolamento (UE) 2017/745 sui dispositivi medici. Tale esclusione suscita perplessità, escludendo dal diritto alla spiegazione settori cruciali (come le decisioni mediche), anche quando una spiegazione potrebbe essere fornita in modo efficace e a costi contenuti.

6.4. Ambito applicativo: quali decisioni

Il diritto alla spiegazione presuppone (Articolo 86 (1)) che la decisione soddisfi due condizioni: i) sia stata adottata dal deployer «sulla base dell'output» del sistema di IA e ii) abbia un «impatto significativo» sulla persona.

La prima condizione richiede che l'output del sistema abbia avuto un'influenza rilevante sulla decisione (così che questa possa considerarsi basata su tale output). La norma sembra quindi avere un ambito applicativo più ampio di quello dell'Articolo 22 GDPR, che riguarda solo le decisioni basate «unicamente sul trattamento automatizzato». Tale ampiezza può, tuttavia, generare incertezze. Si pensi a un motore di ricerca basato sull'IA che abbia dato informazioni utili a una decisione. Poiché la decisione si fonda, almeno in parte, sull'output del motore di ricerca, secondo la lettera della norma vi sarebbe un diritto alla spiegazione del suo funzionamento. Questa conclusione appare quanto meno discutibile, poiché il motore di ricerca si limita a produrre elementi di carattere informativo, la cui valutazione è affidata al decisore.

Quanto alla seconda condizione, la norma precisa che affinché l'impatto su una persona sia significativo è necessario che la decisione (1) produca effetti

giuridici o (2) «in modo analogo incida significativamente su tale persona in un modo che essa ritenga avere un impatto negativo sulla sua salute, sulla sua sicurezza o sui suoi diritti fondamentali».

Il secondo caso sembra riferirsi alla percezione soggettiva, piuttosto che alla reale dimensione dell'impatto negativo. Riteniamo che questa formulazione sia il risultato di un tentativo mal riuscito di tener conto di possibili stati di sofferenza psichica, causati dall'aspettativa (anche non realistica) di impatti negativi.

Si crea così una curiosa sovrapposizione con l'art. 22 del GDPR: quest'ultimo ha portata più ampia quanto agli impatti significativi, includendo quelli meramente economici, mentre l'art. 86 risulta più esteso del GDPR comprendendo anche stati di sofferenza relativi a impatti negativi solo immaginati.

Circa la significatività degli impatti, può essere opportuno richiamare alcune considerazioni relative al GDPR. Il Considerando 71 offre due esempi: il rifiuto automatico di una domanda di credito online e le pratiche di assunzione elettronica. Come osservato in precedenza, per essere significativi a norma dell'articolo 22 GDPR, gli effetti sulla sfera emotiva e la pubblicità mirata, di regola, non hanno sufficiente rilevanza. Resta da verificare se queste considerazioni siano valide anche rispetto all'Articolo 86 che, come osservato, fa riferimento alla percezione soggettiva del destinatario della decisione, mentre non comprende gli impatti meramente economici.

6.5. Il contenuto della spiegazione

Le spiegazioni devono essere chiare e significative (art 86 (1)) i) sul ruolo del sistema di IA nella procedura decisionale e ii) sui principali elementi della decisione adottata.

Il considerando 171 aggiunge che la spiegazione dovrebbe «fornire una base su cui le persone interessate possano esercitare i loro diritti».

Il requisito di chiarezza implica che la spiegazione sia comprensibile per il destinatario, escludendo il ricorso esclusivo a spiegazioni modellistiche o tecniche. Anche quando sia fornita una spiegazione tecnica, dovrebbe essere accompagnata da indicazioni accessibili a tutti i destinatari della decisione.

Il requisito di significatività postula informazioni adeguate (a) sul ruolo del sistema e (b) sugli elementi della decisione. Quanto al ruolo del sistema, gli aspetti più rilevanti sono: (i) il tipo di approccio e di tecnologia adottati; (ii) le finalità del processo decisionale; (iii) la fase o le fasi in cui si utilizza un sistema di IA; e (iv) il modo in cui gli output del sistema influenzano la decisione finale.

Quanto agli elementi della decisione, gli aspetti rilevanti sono: (i) quali categorie di dati di input (predittori) vengono considerate per ottenere quali risultati (obiettivi/previsioni); (ii) l'importanza relativa di tali categorie nella determina-

zione dei risultati; (iii) quali processi di inferenza hanno determinato la specifica decisione; e (iv) quali nuove conclusioni sono state ottenute mediante processi di inferenza.

In concreto, il tipo di informazioni richieste dipende dal contenuto della decisione e dalla tecnologia adottata, che può facilitare o ostacolare certe forme di spiegazione.

In ogni caso, possiamo identificare una serie di elementi costitutivi minimi di una spiegazione individualizzata “significativa”. Dovrebbe indicare quale output del sistema (e.g., quale punteggio di affidabilità creditizia) abbia condotto all’esito decisorio (e.g., il diniego del prestito). Dovrebbe specificare quali valori dei dati di input (e.g., livello di reddito, posizione lavorativa o età) siano stati decisivi, ossia tali che valori diversi avrebbero condotto ad esiti diversi (spiegazione contrastiva). La spiegazione dovrebbe includere i dati inferiti che abbiano avuto un ruolo rilevante nel determinare l’esito finale, almeno quando abbiano significato autonomo (per esempio, non sarà necessario fornire il valore numerico calcolato dal nodo di una rete neurale, mentre la classificazione secondo una scala del livello di istruzione o reddito è certamente significativa).

Nella spiegazione generalizzata, il deployer potrà riferirsi alle indicazioni ottenute dal fornitore ai sensi dell’Articolo 13, presentandole in modo comprensibile al destinatario della decisione e adeguate al contesto d’uso.

Come per il GDPR, in mancanza di una formulazione univoca, permane l’incertezza sull’obbligo giuridico di una spiegazione individualizzata. A nostro parere, se l’Articolo 86 deve avere una valenza giuridica ulteriore rispetto a quella del GDPR, è necessario assumere che l’AIA introduca tale obbligo. Lo stesso Articolo limita la propria applicazione ai casi in cui «il diritto di cui al paragrafo 1 non sia altrimenti previsto dal diritto dell’Unione». Ne deriva che, poiché l’obbligo di informazione generalista (per tutte le decisioni basate su dati personali) già discende dal GDPR, l’Art. 86, se limitato a tale informazione, avrebbe applicazione estremamente limitata (per esempio, solo a dati non personali, a dati di persone giuridiche qualora il diritto ex articolo 86 sia a esse applicabile, e a decisioni non completamente automatizzate a norma dell’articolo 22 del GDPR).

In vero, se si ritenesse che dal GDPR discenda già implicitamente un obbligo di spiegazione individualizzata, l’ambito applicativo dell’Articolo 86 risulterebbe ugualmente limitato.

Tuttavia, finché nella pratica del diritto non vi sarà convergenza sull’obbligo di spiegazione individualizzata in base al GDPR, l’affermazione di tale obbligo secondo l’Art. 86 continuerà ad avere rilevanza autonoma.

7. Art. 86 AIA. Il coordinamento con altre normative

Il diritto alla spiegazione dell'Art. 86 si affianca ad altre norme che affrontano, da prospettive diverse e in differenti contesti, il tema della decisione automatica.

7.1. La disciplina della spiegazione in altre normative

I paragrafi 2 e 3 dell'Art. 86 si occupano del coordinamento con altre normative europee e nazionali. Il paragrafo 2 fa salve le eccezioni o limitazioni al diritto alla spiegazione già previste dalla normativa dell'Unione o dal diritto nazionale (in linea con il diritto dell'Unione). Tali limitazioni o esclusioni prevalgono dunque sull'Art. 86. Il paragrafo 3 stabilisce inoltre che la disposizione non introduce un nuovo diritto alla spiegazione qualora esso sia già previsto nel quadro giuridico europeo.

La principale normativa di riferimento resta il GDPR e, in particolare, gli articoli 13, 14 e 22. Rilevano però anche le normative sulla protezione dei consumatori e sulla responsabilità contrattuale o extracontrattuale, nella misura in cui spiegazioni adeguate contribuiscano a ridurre i rischi e, quindi, a soddisfare gli obblighi di diligenza e protezione gravanti sul professionista.

La spiegazione può, infatti, contribuire a evitare o limitare il danno, quando generalizzata e comunicata prima della decisione, o quando individualizzata e suscettibile di condurre ad una revisione della decisione stessa. Per esempio, la spiegazione delle ragioni per cui il consumatore è stato oggetto di un'offerta (residenza, nazionalità, genere, profili comportamentali come la propensione al gioco) può condurlo a riflettere sui rischi connessi a tale offerta, e quindi prevenire il danno che ne potrebbe derivare.

Il Digital Services Act (DSA), a propria volta, tratta il tema della spiegazione negli Articoli 26 e 27. Il primo dedicato alla pubblicità online impone alle piattaforme di fornire, per ogni messaggio pubblicitario mirato, informazioni pertinenti circa i «parametri utilizzati per determinare il destinatario al quale viene presentata la pubblicità e, laddove applicabile, alle modalità di modifica di detti parametri» (Articolo 26(d)DSA). Il testo dell'Articolo 26 non chiarisce se si richieda solamente l'indicazione dei criteri adottati in generale per l'invio della pubblicità (spiegazione generalista), o anche i valori per quei criteri nel caso concreto (spiegazione individualizzata). Per esempio, nell'invio di un'offerta di lavoro, resta da stabilire se sia sufficiente indicare che le competenze professionali sono state un criterio rilevante, o sia necessario anche specificare quale tipo e livello di competenze sono stati attribuiti al destinatario dell'offerta.

Similmente, ci si potrebbe chiedere se, quando viene proposto un prezzo, sia sufficiente specificare che le propensioni all'acquisto sono state considerate, o sia necessario indicare in quale classe di consumatori l'utente è stato inserito.

L'Art. 27 disciplina i sistemi di raccomandazione e richiede che le piattaforme che se ne avvalgano specifichino, nelle condizioni generali, i principali parametri utilizzati e qualunque opzione che consenta ai destinatari di modificare o influenzare tali parametri (Articolo 27(2) DSA). In quest'ultimo caso, diversamente da quanto rilevato sopra, è evidente che si richiede solamente una spiegazione generalista.

Possono essere, inoltre, rilevanti alcune norme di settore, in particolare nel campo dei mercati finanziari. Per esempio, tra gli obblighi di informazione connessi alla concessione di un credito, vi è quello di comunicare i risultati ottenuti tramite la consultazione di database, al fine di valutare l'affidabilità del consumatore (Art. 6 (1) (k) della Direttiva 2008/48 relativa ai contratti di credito ai consumatori).

Infine, speciali esigenze di spiegazione caratterizzano gli atti di autorità pubbliche, cui si applica un obbligo di motivazione. In questo caso, la spiegazione deve illustrare come la decisione sia basata su norme e principi giuridici e sia stata, quindi, adottata nell'adempimento di obblighi di legge, o nel perseguimento di un interesse pubblico discrezionale.

Rispetto alle normative elencate, l'Articolo 86 può svolgere una funzione integrativa o suppletiva, qualora se ne tragga la necessità di una spiegazione individualizzata (rispetto alle norme del DSA e a quelle sul credito) e che presenti le ragioni della decisione, al di là della specificazione delle norme e dei principi giuridici applicati (rispetto alle decisioni pubbliche).

7.2. Sovrapposizioni e differenze tra AI Act e GDPR

Abbiamo osservato come il tema delle decisioni automatiche è affrontato dal GDPR, a cui si sovrappone parzialmente l'IA Act. Esamineremo ora la correlazione tra le due normative. In particolare, considereremo se entrambe stabiliscano un obbligo giuridico di spiegazione e come differiscano rispetto al contenuto e all'ambito applicativo.

Dall'esame svolto fin qui, vi è una chiara, ma parziale, sovrapposizione tra gli obblighi di informazione/spiegazione contenuti nel GDPR e l'obbligo di spiegazione di cui all'Articolo 86 AIA. Entrambi non distinguono tra decisioni di natura pubblica o privata, e dunque, nel silenzio dei testi dobbiamo ritenere che si rivolgano alle determinazioni adottate sia nella sfera di autonomia dei privati, sia nell'esercizio di poteri pubblici.

Diversamente, emergono le seguenti differenze:

- i) Il GDPR si applica solo alle persone fisiche, mentre l'Art. 86 potrebbe riferirsi anche alle persone giuridiche;
- ii) Il GDPR postula che la decisione si basi sul trattamento di dati personali e in particolare sulla profilazione, mentre l'Articolo 86 prescinde da tali requisiti;
- iii) Il GDPR richiede che la decisione sia basata esclusivamente sul trattamento automatizzato, condizione non prevista dall'Articolo 86;
- iv) L'Articolo 86 include solo i sistemi ad alto rischio, categoria non rilevante per il GDPR;
- v) L'Articolo 86 sembra postulare che la persona oggetto della decisione ritenga di aver subito un impatto negativo, mentre il GDPR richiede che tale impatto si sia realizzato.
- vi) L'Articolo 86 considera, oltre agli effetti giuridici, solo gli impatti negativi su salute, sicurezza e diritti fondamentali, limitazione assente nel GDPR.

Riteniamo che la parziale sovrapposizione tra l'Articolo 86 e l'Articolo 22 del GDPR potrà generare incertezze nell'interpretazione e applicazione delle due disposizioni. Comunanze e differenze tra le due previsioni non sembrano essere il frutto di una scelta ragionata e consapevole dell'esigenza di coordinare AIA e GDPR.

7.3. La spiegazione: una questione aperta?

Come emerge dall'analisi nelle sezioni precedenti, l'Articolo 86 tende a generare più dubbi che risposte, sul controverso tema della spiegabilità delle decisioni basate sull'IA. Se l'intento del legislatore europeo era chiarire le incertezze interpretative già sorte in relazione all'Articolo 22 del GDPR, ci sembra che questo obiettivo non sia stato raggiunto.

L'emendamento del Parlamento Europeo, che ha introdotto l'Articolo 86, ha comunque il merito di aver richiamato l'attenzione sulla fondamentale necessità della spiegabilità, ancora insoddisfatta dai sistemi attuali e non adeguatamente promossa dalle normative vigenti. Ci auguriamo che alcuni dei dubbi sollevati trovino soluzione nel futuro contesto di attuazione dell'AIA, anche grazie al contributo coordinato delle autorità competenti, specialmente in tema di IA e protezione dei dati¹.

¹ Per i riferimenti e per ulteriori approfondimenti, F. LAGIOIA, G. SARTOR, A. SIMONCINI, *Art. 22. processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione*, in R. D'ORAZIO ET AL. (a cura di), *Codice della privacy e Data Protection*, Milano: Giuffrè, 2021, pp. 378 – 390; G. SARTOR, F. LAGIOIA, *Le decisioni algoritmiche tra etica e diritto*, in U. RUFFOLO (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Milano: Giuffrè, 2020; F. LAGIOIA, G. SARTOR, *ALA-articolo 86*, in A. MANTELERO ET AL. (a cura di), *Commentario all'AI Act*, Milano: Kluwer, 2025, pp. 760–770.

RESPONSABILITÀ E INTELLIGENZA ARTIFICIALE

Chantal Bompreszzi

Sommario: 1. Responsabilità e software. 2. L'imputazione di responsabilità e la qualificazione giuridica del software. 3. Etica dell'IA e *accountability*. 4. Le principali problematiche sollevate dalla dottrina. 5. L'approccio adottato con l'*AI ACT*. 6. Gli interventi legislativi delle istituzioni europee. 7. Il ritiro dell'AILD e il cambio di approccio del legislatore europeo.

1. Responsabilità e software

La responsabilità per danni cagionati da software è oggetto di indagine sin dagli Anni '80¹. Al pari di oggi, si indagava chi dovesse rispondere dei danni cagionati da un software. Il dibattito giuridico si è acceso particolarmente negli Anni '90, quando è diventato comune nei mercati finanziari di tutto il mondo concludere automaticamente contratti per conto delle parti ad opera dei cd "*electronic agents*" o "agenti software", programmi informatici in grado di spostarsi nella rete verso le raccolte di dati sui quali devono operare e che recano al loro interno istruzioni circa le priorità da rispettare². Questi sistemi informatici abbinavano proposte di acquisto e di vendita in base a parametri predefiniti relativi a prezzo, data e ora. In particolare, ci si è concentrati sull'imputazione delle dichiarazioni contrattuali e sulla responsabilità conseguente in caso di inadempimento, dato il maggiore grado di autonomia di questi strumenti. Il problema che si è posto con maggior forza è stato quello dell'allocazione del rischio riconducibile a un malfunzionamento dell'agente. La posizione prevalente è stata quella di considerare gli agenti come meri mezzi di trasmissione di volontà, e

¹ G. ALPA, *Responsabilità extracontrattuale ed elaboratore elettronico*, in *Dir. dell'Informazione e dell'Informatica* 1986 (II), pp. 387-393; C. ROSSELLO, *La responsabilità da inadeguato funzionamento di programmi per elaboratore elettronico: aspetti e problemi dell'esperienza nordamericana*, in G. ALPA (a cura di), *Computers e responsabilità civile*, Milano: Giuffrè 1985, pp. 87-142.

² Una definizione di "*electronic agent*" è contenuta nell'*Uniform Electronic Transactions Act*, per cui esso è «*a computer program or an electronic or other automated means used independently to initiate an action or respond to electronic records or performances in whole or in part, without review or action by an individual*» (sect. 2 (6)).

non come entità dotate di una soggettività giuridica³, per cui il rischio deve considerarsi accettato e sopportato dal soggetto che utilizza l'agente, sulla base dei principi di autoresponsabilità e affidamento. Questo approccio è stato adottato a livello internazionale dall'UNCITRAL, affermando che il principio di imputazione della responsabilità in capo al soggetto che si serve di un determinato software sia responsabile del medesimo anche nel caso in cui l'agente non agisca in maniera automatica ma autonoma⁴. La posizione dell'UNCITRAL ha costituito un opportuno chiarimento in materia, privilegiando l'interpretazione normativa e negando la necessità di un intervento normativo nuovo e *ad hoc*.

Questioni nuove sul tema della responsabilità si pongono, invece, laddove il software abbia una certa autonomia decisionale, ovvero quando gli output del programma siano imprevedibili per il loro carattere non deterministico e opaco, quali sono i sistemi di intelligenza artificiale.

2. L'imputazione di responsabilità e la qualificazione giuridica del software

In merito al rapporto tra intelligenza artificiale e responsabilità, il primo interrogativo posto ha riguardato la qualificazione del software come mero strumento di trasmissione di volontà piuttosto che come soggetto giuridico su cui addossare direttamente le conseguenze negative del proprio operare. Rispetto al dibattito verificatosi sul punto negli Anni '90, l'elemento di novità è rappresentato dal fatto che si è innanzi a sistemi dotati di autonomia decisionale e imprevedibilità dei risultati.

Il Parlamento europeo, con una Risoluzione del 16 febbraio 2017⁵, ha invitato la Commissione europea a valutare «l'istituzione di uno status giuridico specifico per i robot nel lungo termine, di modo che almeno i robot autonomi più sofisticati possano essere considerati come persone elettroniche responsabili di risarcire qualsiasi danno da loro causato, nonché eventualmente il ricono-

³ Vedi il confronto tra G. FINOCCHIARO, *La conclusione del contratto telematico mediante i «software agents»: un falso problema giuridico?*, in *Contratto e Impresa*, 2002 (XVIII-II), pp. 500-509 e G. SARTOR, *Gli agenti software: nuovi soggetti del ciberdiritto?*, in *Contratto e Impresa*, 2002 (XVIII-II), pp. 465-499.

⁴ United Nations, General Assembly, *Legal aspects of electronic commerce*, A/CN.9/WG.IV/WP.95, par. 71-73. «[...] while the expression "electronic agent" has been used for purpose of convenience, the analogy between an automated system and a sales agent was not appropriate. This, general principle of agency law (for example, principle involving limitation of liability as a result of the faulty behaviour of the agent) could not be used in connection with the operation of such systems» «[...] as a general principle, the person on whose behalf a computer was programmed should ultimately be responsible for any message generated by the machine».

⁵ Risoluzione del Parlamento europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica (2015/2103(INL)), https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_IT.html.

scimento della personalità elettronica dei robot che prendono decisioni autonome o che interagiscono in modo indipendente con terzi» (punto 59, lett. f).

Questa posizione del Parlamento europeo, volta a riconoscere specifica soggettività giuridica e personalità elettronica ai robot, è stata fortemente criticata, in quanto ritenuta una soluzione apparente⁶. Anche ammettendo, infatti, di poter conferire soggettività a una cosa (un programma informatico), è stato sollevato il problema del risarcimento del danno, poiché il robot non avrebbe un patrimonio di cui poter disporre con il quale risarcire il danno. Peraltro, anche laddove venisse costituito un patrimonio dedicato (così come da taluno suggerito), si è osservato che un patrimonio riservato al risarcimento di queste tipologie di danni si potrebbe comunque ipotizzare senza dover costruire tutta l'impalcatura della soggettività. L'attribuzione di soggettività si sostanzierebbe, cioè, in un'inutile complicazione di rapporti.

Più recentemente, la Risoluzione del Parlamento europeo del 20 ottobre 2020 recante raccomandazioni alla Commissione su un regime di responsabilità civile per l'intelligenza artificiale⁷ ha escluso il conferimento di personalità giuridica⁸, ponendosi in antitesi rispetto alla precedente Risoluzione del 16 febbraio 2017. Sulla stessa lunghezza d'onda, l'UNCITRAL *Model Law on Automated Contracting* del 2025⁹ ha chiarito che i sistemi automatizzati sono strumenti privi di volontà propria o di personalità giuridica, e i risultati prodotti da tali sistemi devono essere attribuiti alle persone e non al sistema stesso (art. 7)¹⁰.

3. Etica dell'IA e accountability

Nel giugno 2018, la Commissione europea ha nominato cinquantadue esperti indipendenti nel *High-Level Expert Group on Artificial Intelligence (AI HLEG)*¹¹, con il compito di formulare linee guida per un'IA affidabile (*Ethics Guidelines for Trustworthy AI* dell'8 aprile 2019), basate su tre pilastri fondamentali: legalità (garantire il rispetto delle leggi e dei diritti fondamentali), etica (difendere la dignità

⁶ Vedi U. RUFFOLO, *La personalità elettronica tra "doveri" e "diritti" della macchina*, in ID. (a cura di), *XXVI Lezioni di diritto dell'intelligenza artificiale*, Torino: Giappichelli 2021, pp. 115-127; G. FINOCCHIARO, *Intelligenza artificiale e responsabilità*, in *Contratto e Impresa*, 2020 (II), pp. 713-731.

⁷ Risoluzione del Parlamento europeo del 20 ottobre 2020 recante raccomandazioni alla Commissione su un regime di responsabilità civile per l'intelligenza artificiale (2020/2014(INL)), https://www.europarl.europa.eu/doceo/document/TA-9-2020-027_6_IT.html.

⁸ Vedi il punto 7 della Risoluzione.

⁹ <https://uncitral.un.org/en/mlac>.

¹⁰ Vedi in particolare il par. 2 dell'art. 7, secondo cui «an action carried out by an automated system is attributed to the person who uses the system for that purpose».

¹¹ <https://digital-strategy.ec.europa.eu/en/news/commission-appoints-expert-group-ai-and-launches-european-ai-alliance>.

e prevenire la discriminazione) e robustezza tecnica (assicurare sicurezza e resilienza).

Per rendere operativi questi pilastri, le Linee guida hanno definito sette requisiti: agenzia e supervisione umana; robustezza tecnica e sicurezza; privacy e governance dei dati; trasparenza; diversità, non discriminazione e equità; benessere sociale e ambientale; e responsabilità (*accountability*). Dopo un ampio periodo di sperimentazione con vari stakeholder, l'8 luglio 2020 l'AI HLEG ha pubblicato la *Assessment List for Trustworthy AI* (ALTAI)¹², uno strumento di autovalutazione che permette alle organizzazioni di confrontare i propri sistemi con i sette requisiti attraverso un questionario strutturato e una metodologia di valutazione. Entrambi i documenti sono volontari, pensati per promuovere standard etici condivisi pur senza pregiudicare il regime di responsabilità vincolante previsto dalle proposte legislative precedenti.

In particolare, per quanto qui interessa, il requisito dell'*accountability* sottolinea l'importanza di stabilire meccanismi chiari e trasparenti per garantire la responsabilità di chi sviluppa, distribuisce e utilizza i sistemi di IA. Esso richiede di mettere in atto strumenti che permettano di gestire i rischi, di monitorare e valutare le decisioni prese dall'IA, e di intervenire in caso di impatti ingiusti o dannosi. È fondamentale che i sistemi di IA siano soggetti a meccanismi di *audit*, interni ed esterni. La possibilità di condurre valutazioni e di accedere ai registri di tali valutazioni può contribuire a un'IA affidabile. In applicazioni che riguardano diritti fondamentali, inclusi sistemi critici per la sicurezza, i sistemi di IA dovrebbero poter essere sottoposti a *audit* indipendenti. Ciò non implica necessariamente che le informazioni sui modelli di business e sulla proprietà intellettuale legati al sistema di IA debbano essere sempre pubblicamente disponibili.

Inoltre, bisogna prevedere procedure di gestione del rischio, che consentano di riferire sulle azioni o decisioni che contribuiscono all'esito del sistema di IA, sia di rispondere alle conseguenze di tale esito. È fondamentale identificare, valutare, documentare e minimizzare i potenziali impatti negativi dei sistemi di IA, specialmente per coloro che sono (direttamente o indirettamente) coinvolti o colpiti. Deve essere garantita una protezione adeguata per *whistleblower*, ONG, sindacati o altri soggetti che segnalano legittimamente preoccupazioni riguardo a un sistema di IA.

Infine, in caso di eventi avversi, devono essere previsti a monte meccanismi accessibili che garantiscano un risarcimento adeguato.

¹² HIGH-LEVEL EXPERT GROUP ON AI (2020), *The Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self Assessment*, <https://digital-strategy.ec.europa.eu/en/library/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment>.

4. Le principali problematiche sollevate dalla dottrina

Come prima anticipato¹³, il principale elemento di novità è rappresentato dal fatto che i sistemi di intelligenza artificiale sono dotati di autonomia decisionale e imprevedibilità dei risultati. In dottrina è stato dunque posto il tema del soggetto a cui attribuire la responsabilità giuridica in caso di danni cagionati dall'intelligenza artificiale. Si è in proposito indagata l'applicabilità delle norme sulla responsabilità civile e sulla responsabilità da prodotto difettoso.

Superata l'idea di attribuire una specifica soggettività giuridica ai robot, in secondo luogo, sono state evidenziate le difficoltà probatorie per il danneggiato. Da un lato, molteplici sono gli attori coinvolti (dal produttore, al fornitore, all'ideatore del programma, all'utilizzatore, etc.), per cui non è agevole identificare la causa del danno; dall'altro, la prova è ostacolata dalla maggiore autonomia di elaborazione dell'algoritmo, che sfugge al controllo del soggetto astrattamente responsabile. In generale, è stato ritenuto poco efficace tentare di applicare categorie e criteri di natura soggettiva, quali il dolo o la colpa, o la ricerca dell'errore *ex post*. Piuttosto, si è ritenuto più utile un modello fondato sulla responsabilità oggettiva e sull'allocazione *ex ante* del rischio. Principio cardine di quest'ultimo modello sarebbe l'*accountability*, che implicherebbe la preventiva responsabilizzazione del soggetto che trae vantaggio dall'uso del sistema di intelligenza artificiale e che sarebbe tenuto ad evitare il rischio adottando le misure più idonee a tale scopo, anche dandone la prova¹⁴.

Sulla disciplina in materia di responsabilità da prodotto difettoso, gli aspetti più problematici sinora sollevati riguardo all'adequatezza della Direttiva vigente¹⁵ rispetto al digitale interessano¹⁶: l'accostabilità dei sistemi di IA alla nozione di "prodotto"¹⁷; le difficoltà probatorie, per il danneggiato, relative alla difettosità del prodotto e al nesso di causalità tra difetto e danno; l'esclusione di responsabilità del produttore per difetti sopravvenuti, di cui all'art. 120, 2° co., Cod. Cons., che mal si concilierebbe con il carattere dinamico dei *device* in questione, a discapito dei soggetti danneggiati¹⁸; il danno cagionato da dispositivi di

¹³ Vedi *supra* il par. 2.

¹⁴ G. FINOCCHIARO, *Intelligenza artificiale e responsabilità*, cit.

¹⁵ Direttiva 85/374/CEE del Consiglio del 25 luglio 1985 relativa al ravvicinamento delle disposizioni legislative, regolamentari ed amministrative degli Stati Membri in materia di responsabilità per danno da prodotti difettosi, OJ L 210, 7.8.1985, pp. 29–33.

¹⁶ Sul rapporto tra IA e disciplina in materia di responsabilità da prodotti difettosi, si veda, *ex multis*, A. AMIDEI, *Responsabilità da prodotto e intelligenza artificiale*, in U. RUFFOLO (a cura di), *XXVI Lezioni di diritto dell'intelligenza artificiale*, Torino: Giappichelli 2021, pp. 149–162.

¹⁷ La discussione trae origine dalle perplessità circa l'applicabilità della disciplina al software.

¹⁸ Il produttore potrebbe esimersi da responsabilità in tutti i casi in cui difetti si dovessero manifestare successivamente, per effetto dell'autoapprendimento del dispositivo.

per sé non difettosi ma potenzialmente lesivi per effetto dell'interazione con altri¹⁹.

5. L'approccio adottato con l'AI ACT

L'approccio *ex ante*, basato sulla preventiva valutazione del rischio e su relativi obblighi di conformità preventiva è quello adottato dal Regolamento (UE) 2024/1689 sull'Intelligenza artificiale (d'ora in avanti, *AI ACT*)²⁰. L'*AI ACT*, infatti, classifica i sistemi di IA in pratiche proibite, applicazioni ad alto rischio²¹, applicazioni a rischio limitato e minimo. I sistemi ad alto rischio sono soggetti a obblighi vincolanti *ex ante*, come valutazioni di conformità, analisi dell'impatto sui diritti fondamentali, documentazione tecnica e monitoraggio post-commercializzazione, mentre le applicazioni a rischio limitato devono rispettare solo requisiti di trasparenza.

L'approccio anzidetto risulta evidente in particolare dal considerando 79, il quale esplicita che «è opportuno che una specifica persona fisica o giuridica, definita come il fornitore, si assuma la responsabilità dell'immissione sul mercato o della messa in servizio di un sistema di IA ad alto rischio, a prescindere dal fatto che tale persona fisica o giuridica sia la persona che ha progettato o sviluppato il sistema». In altri termini, il soggetto che trae maggiore vantaggio dal sistema di IA deve essere anche quello che deve adottare tutte le misure necessarie per evitarlo o almeno attenuarlo, le quali nel Regolamento si sostanziano nell'assoggettamento a specifici obblighi²².

D'altro canto, tranne la previsione di sanzioni amministrative, l'*AI Act* non contiene disposizioni armonizzate sulla responsabilità civile, demandando la riforma della responsabilità a un'iniziativa legislativa separata²³.

¹⁹ Si pensi all'*Internet of Things*. Qui la nozione di prodotto è sfumata, essendo l'attività di questi strumenti accostabile anche a quella di servizio.

²⁰ Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale) GU L 1689 del 12.7.2024, pp. 1-144. La recente Proposta di Omnibus Digitale sull'IA (COM(2025) 836 final del 19 novembre 2025) prevede di intervenire sull'*AI Act* con misure di semplificazione mirate.

²¹ Sul rapporto tra sistemi ad alto rischio e responsabilità, vedi C. BOMPRESZI, S. SAPIENZA, *Algorithmic Justice e la classificazione di rischio nella Proposta AI Act*, in M. PALMIRANI, S. SAPIENZA (a cura di), *La trasformazione digitale della giustizia nel dialogo tra discipline*, Milano: Giuffrè 2022, pp. 65-114.

²² D. CHIAPPINI, *Intelligenza Artificiale e responsabilità civile: nuovi orizzonti di regolamentazione alla luce dell'Artificial Intelligence Act dell'Unione europea*, in *Rivista Italiana di Informatica e Diritto*, 2022 (II), pp. 95-108.

²³ European Parliament, *Artificial Intelligence and Civil Liability – A European perspective*, Luglio 2025, p. 20, [https://www.europarl.europa.eu/thinktank/en/document/IUST_STU\(2025\)77642](https://www.europarl.europa.eu/thinktank/en/document/IUST_STU(2025)77642).

6. Gli interventi legislativi delle istituzioni europee

Il primo intervento in tal senso delle istituzioni europee si rinviene nella succitata Risoluzione del 20 ottobre 2020²⁴, la quale, nel delineare una Proposta di Regolamento, ha optato per un modello di allocazione del rischio sul soggetto più vicino allo stesso (l'operatore) e che trae il maggior vantaggio dal sistema di IA. Secondo un approccio basato sull'*accountability*, questi è tenuto ad adottare le misure idonee ad evitarlo e a fornire la prova liberatoria. Nella Proposta di Regolamento allegata alla Risoluzione si distingue, poi, tra sistemi ad alto rischio, per cui si configura una responsabilità di tipo oggettivo, e altri sistemi di IA, assoggettati ad un regime di responsabilità per colpa (presunta, con onere della prova sull'operatore).

Più di recente, questa Proposta è stata superata dalla Commissione europea, la quale nel 2022 ha adottato una Proposta di Direttiva relativa all'adeguamento delle norme in materia di responsabilità civile extracontrattuale all'intelligenza artificiale (d'ora in avanti, AILD), avente l'obiettivo di contribuire a ridurre gli ostacoli giuridici che le vittime debbono affrontare per poter ottenere il risarcimento di danni subiti per opera di sistemi di IA, in parte succitati²⁵. La Proposta ha introdotto infatti, limitatamente a regimi di responsabilità per colpa, una presunzione di causalità da far valere, a certe condizioni, circa il rapporto tra la colpa del convenuto e il comportamento del sistema di IA; inoltre, è stato previsto in favore del danneggiato un diritto di accesso alle prove da parte di aziende e fornitori nei casi di coinvolgimento di sistemi ad alto rischio.

Nel medesimo anno, la Commissione europea, contestualmente all'AILD, ha adottato altresì una Proposta di revisione della Direttiva sulla responsabilità per danno da prodotti difettosi²⁶ (d'ora in avanti, PLD); anche in tale contesto, viene alleggerito l'onere della prova per il danneggiato in ipotesi nuove, come quella di danni prodotti da sistemi di IA, con estensione di responsabilità per prodotti divenuti difettosi a causa di aggiornamenti (o mancati dovuti adeguamenti) dei software necessari a preservarne la sicurezza, e vengono imposte *disclosure of evidence* ai fabbricanti²⁷. La Proposta è stata approvata dando luogo al-

²⁴ Vedi *supra* par. 2.

²⁵ European Commission, Proposal for a Directive on adapting non contractual civil liability rules to artificial intelligence, https://ec.europa.eu/info/files/proposal-directive-adapting-non-contractual-civil-liability-rules-artificial-intelligence_en.

²⁶ European Commission, Proposal for a Directive of the European Parliament and of the Council on liability for defective products, https://single-market-economy.ec.europa.eu/document/3193da9a-cecb-44ad-9a9c-7b6b23220bcd_en

²⁷ https://ec.europa.eu/commission/presscorner/detail/it/ip_22_5807.

la Direttiva (UE) 2024/2853 (d'ora in avanti, *PLD Revised*, o *PLDr*)²⁸, la quale amplia la definizione di “prodotto” includendo anche prodotti digitali e software, e allarga il campo dei danni risarcibili, come quelli psicologici e ai dati (ad esempio, distruzione o danneggiamento). Inoltre, la *PLDr* chiarisce come valutare se un prodotto è difettoso, considerando anche aspetti come la capacità di apprendere o evolversi dopo l'acquisto (molto rilevante per l'intelligenza artificiale), l'interazione con altri dispositivi connessi e la conformità agli standard di cybersecurity. Un'altra novità importante è che i tribunali possono presumere che un prodotto sia difettoso o che il danno sia causato da un difetto, soprattutto se la prova risulta difficile a causa della complessità tecnica o scientifica. I produttori, inoltre, sono ora responsabili anche per i danni causati da vulnerabilità di cybersecurity, aumentando così i rischi di responsabilità in caso di attacchi informatici. La direttiva impone anche regole più stringenti per le piattaforme online. Gli Stati membri dell'UE hanno tempo fino al 9 dicembre 2026 per recepirla nelle leggi nazionali, e le nuove regole si applicheranno ai prodotti immessi sul mercato o messi in servizio dopo quella data. In sostanza, questa direttiva mira a rafforzare la protezione dei consumatori, adattando le norme alle nuove tecnologie e all'economia digitale, anche se questo comporterà sfide per le aziende, che dovranno aggiornare le proprie pratiche e affrontare maggiori rischi di responsabilità, specialmente in settori come quello farmaceutico e dei dispositivi medici, dove le tecnologie IA sono sempre più presenti.

7. Il ritiro dell'AILD e il cambio di approccio del legislatore europeo

La AILD, proposta nel 2022, avrebbe dovuto integrare i regimi nazionali con strumenti procedurali armonizzati, ma si è rivelata tecnicamente complessa, scarsamente efficiente e con applicabilità incerta. L'eccessivo affidamento sulle presunzioni e la difficoltà di coordinamento con i diversi sistemi nazionali ne hanno minato l'efficacia. La Commissione, nel 2025, ha annunciato l'intenzione di ritirare la proposta²⁹.

Quest'ultimo atto della Commissione europea ha di fatto confermato un cambio di approccio³⁰. Nel 2017, infatti, il Parlamento europeo individuava nella responsabilità civile il fulcro della governance giuridica dell'IA, proponendo

²⁸ Direttiva (UE) 2024/2853 del Parlamento europeo e del Consiglio del 23 ottobre 2024 sulla responsabilità per danno da prodotti difettosi, che abroga la Direttiva 85/374/CEE del Consiglio, GU L 2853 del 18.11.2024, pp. 1-22.

²⁹ https://commission.europa.eu/strategy-and-policy/strategy-documents/commission-work-programme/com-missionwork-programme-2025_en. Vedi Annex IV (List of intended withdrawals).

³⁰ Chiamato “*the great reversal*”. Vedi European Parliament, *Artificial Intelligence and Civil Liability*, cit.

un regime di responsabilità oggettiva per gli operatori di sistemi autonomi, affiancato da obblighi assicurativi e da un fondo di compensazione. Dal 2021, con l'avvento della Commissione von der Leyen, l'attenzione si è spostata su un approccio "*ex ante*", incentrato sull'*AI Act*, basato su valutazioni di rischio e obblighi di conformità preventiva, relegando la responsabilità civile a strumento secondario. La gerarchia per cui il principio di legge vincolante (*hard-law*) prevale sulla governance basata su norme non vincolanti (*soft-law*), è stata di fatto invertita, posponendo a data da destinarsi una riforma della responsabilità civile specifica per l'IA.

Indipendentemente dall'approccio scelto, e dalle diversità di opinioni circa la strategia migliore da intraprendere, occorre un'azione unitaria e uniforme dell'UE, che scongiuri i rischi derivanti dalla frammentazione normativa dei singoli Stati membri. In proposito, l'Italia ha già approvato la Legge 23 settembre 2025, n. 132, recante "Disposizioni e deleghe al Governo in materia di intelligenza artificiale", in cui si affida al Governo la delega a adottare, entro dodici mesi dall'entrata in vigore della norma, uno o più decreti legislativi con riferimento anche ai casi di responsabilità civile (art. 24, co. 1)). In quest'ultimo caso, è prescritto che il Governo debba prevedere strumenti di tutela del danneggiato, anche attraverso una specifica regolamentazione dei criteri di ripartizione dell'onere della prova, tenuto conto della classificazione dei sistemi di intelligenza artificiale e dei relativi obblighi come individuati dall'*AI ACT* (art. 24, co. 5, lett. d)).

PARTE IV – MERCATI E SERVIZI

LA REGOLAZIONE DEI MERCATI DIGITALI: IL DIGITAL MARKETS ACT

Federico Galli

SOMMARIO: 1. Aspetti economici degli intermediari di Internet. 2. L'ascesa dei "mercati digitali". 3. Diritto della concorrenza e mercati digitali. 4. Il Regolamento Platform-to-Business. 5. Il Digital Markets Act. 5.1. Ambito di applicazione e relazione con il diritto generale della concorrenza e con il Regolamento Platform-to-Business. 5.2. I gatekeeper e la loro designazione. 5.3. Obblighi e divieti ad applicazione diretta. 5.4. Obblighi e divieti ad applicazione coordinata. 5.5. La conformità e gli altri obblighi dei gatekeeper. 5.6. Applicazione e sanzioni.

1. Aspetti economici degli intermediari di Internet

Gli intermediari di Internet sono caratterizzati da alcuni effetti economici rilevanti che ne spiegano il ruolo centrale nell'attuale società dell'informazione.

Un primo elemento distintivo riguarda i costi marginali molto bassi e le economie di scala e di scopo: il costo di servire un nuovo utente è spesso trascurabile, mentre lo stesso asset tecnologico – come un'infrastruttura cloud, un motore di ricerca, un sistema operativo o un database di utenti – può essere riutilizzato in mercati differenti, abbattendo drasticamente i costi medi.

Questi intermediari operano poi come piattaforme multi-versante (*multi-sided platforms*) che mettono in contatto due o più gruppi di utenti (ad esempio, consumatori e inserzionisti, oppure venditori e acquirenti), facilitandone interazioni e scambi commerciali¹. Il modello di business si fonda sugli effetti di rete diretti e indiretti: il beneficio per gli utenti di un lato della piattaforma aumenta all'aumentare del numero di utenti sull'altro lato, generando un circolo virtuoso che tende a far crescere rapidamente la base utenti della piattaforma dominante e a creare fenomeni di "*winner-take-all*" con alte barriere all'entrata per nuovi operatori².

¹ L'analisi economica dei mercati multi-versante si deve in particolare al contributo pionieristico di J.C. ROCHET, J. TIROLE, *Platform Competition in Two-Sided Markets*, in *Journal of the European Economic Association*, 2003 (4), pp. 990-1029.

² Si parla di effetto di rete "indiretto" per contrapporlo all'effetto di rete "diretto", cioè il fe-

Un'altra caratteristica economica cruciale dei mercati digitali è il ruolo dei dati³. Molte piattaforme offrono servizi apparentemente gratuiti agli utenti finali, ma monetizzano raccogliendo ingenti quantità di informazioni personali. Questi dati, una volta aggregati ed elaborati, diventano una risorsa strategica per lo sviluppo di nuovi prodotti e servizi, per la pubblicità mirata e per altre forme di intermediazione rivolte a inserzionisti e imprese. La loro accumulazione progressiva e la crescente qualità connessa all'ampliarsi della base utenti conferiscono alle principali piattaforme un vantaggio competitivo difficilmente replicabile⁴.

A ciò si aggiunge il ruolo degli algoritmi e dei sistemi di intelligenza artificiale, che permettono di trasformare i dati grezzi in previsioni e raccomandazioni sempre più accurate. L'uso di tali strumenti rafforza il potere di mercato delle piattaforme, poiché la capacità predittiva e la qualità dei servizi migliorano proporzionalmente alla quantità di dati disponibili.

La concorrenza stessa tende a svilupparsi sempre più “attraverso gli algoritmi”⁵: le imprese non competono soltanto in termini di prezzo o qualità del servizio, ma anche nella capacità di progettare e addestrare algoritmi in grado di offrire esperienze personalizzate, di ottimizzare l'allocazione pubblicitaria o di anticipare i bisogni degli utenti.

2. L'ascesa dei “mercati digitali”

L'effetto cumulativo dei fattori sopra delineati spiega perché nell'ultimo ventennio un numero molto ristretto di intermediari globali sia riuscito a dominare interi ecosistemi digitali, spesso integrando tra loro più segmenti (pubblicità, e-commerce, social network, sistemi operativi, servizi cloud). Si tratta di posizioni di controllo quasi monopolistico, che non derivano necessariamente da pratiche anticoncorrenziali isolate, ma dal funzionamento intrinseco dei mercati stessi.

nomeno per cui l'utilità di un servizio aumenta con il crescere del numero di utenti che appartengono al medesimo lato della rete.

³ V. MAYER-SCHÖNBERGER, K. CUKIER, *Big data: A revolution that will transform how we live, work, and think*, Boston: Houghton Mifflin Harcourt, 2013.

⁴ V. MAYER-SCHÖNBERGER, T. RAMGE, *Access rules: Freeing data from big tech for a better future*, Berkeley: Univ of California Press, 2022.

⁵ Cfr. A. EZRACHI, M.E. STUCKE, *Virtual Competition: The Promise and Perils of the Algorithm-Driven Economy*, Cambridge, Mass.: Harvard University Press, 2016, che analizzano come la diffusione degli algoritmi di *pricing*, *matching* e raccomandazione trasformi la natura stessa della competizione, favorendo in alcuni casi fenomeni di coordinamento tacito o di rafforzamento del potere di mercato.

Oggi si parla ormai di veri e propri “mercati digitali” che contraddistinguono il panorama economico globale e le dinamiche competitive. Giganti tecnologici come Google, Amazon, Facebook/Meta, Apple e Microsoft (spesso indicati come Big Tech o con l’acronimo GAFAM) si sono imposti come attori dominanti, grazie a piattaforme digitali divenute infrastrutture fondamentali del commercio e della comunicazione contemporanea. Il valore di mercato di queste imprese è cresciuto fino a collocarle ai primi posti al mondo⁶, e le loro piattaforme online hanno acquisito un ruolo centrale nelle attività economiche e nelle interazioni sociali: costituiscono punti di passaggio obbligati tra imprese e utenti finali in numerosi settori digitali. Di conseguenza, controllando l’accesso a mercati e servizi chiave, tali piattaforme esercitano un’influenza enorme sulle opportunità commerciali di terzi e sulle scelte dei consumatori.

Questa crescita ha portato a una concentrazione di potere di mercato senza precedenti in pochi soggetti. Il dibattito odierno riconosce il rischio derivante da un’eccessiva concentrazione nelle mani di pochi gatekeeper globali. In molti mercati digitali, l’impresa leader gode di quote di mercato schiaccianti – spesso superiori al 90% – lasciando ai concorrenti solo nicchie marginali. Ad esempio, Google detiene la stragrande maggioranza degli utenti di motori di ricerca in Europa⁷, Amazon domina l’e-commerce in vari paesi⁸, Facebook controlla i principali social media e la messaggistica istantanea (insieme al suo servizio WhatsApp)⁹, Apple e Google gestiscono i sistemi operativi mobili e i relativi app store senza rivali¹⁰, etc.

⁶ Si vedano, ad esempio, le classifiche annuali di Forbes dedicate alle aziende con la maggiore capitalizzazione di mercato, nonché articoli di stampa come quelli del New York Times e del Wall Street Journal, che mettono in evidenza come Apple, Microsoft, Alphabet, Amazon e Meta dominino stabilmente la parte alta della graduatoria negli ultimi anni.

⁷ Secondo StatCounter, nel periodo agosto 2024–agosto 2025 Google ha detenuto circa il 90,28% delle ricerche online in Europa: <https://gs.statcounter.com/search-engine-market-share/all/europe>.

⁸ In Germania la penetrazione di Amazon nel mercato online è pari al 64%, in Spagna al 50%, secondo NielsenIQ: <https://nielseniq.com/global/en/insights/analysis/2023/amazon-in-europe-insights-and-key-figures/>. Inoltre, in Italia e Francia Amazon genera almeno il doppio delle vendite rispetto al concorrente numero 2: <https://ecommercenews.eu/ecommerce-market-concentration-highest-in-italy-and-spain/>.

⁹ In Europa Facebook ha una quota dell’81,04% del mercato dei social media (StatCounter, agosto 2024–agosto 2025): <https://gs.statcounter.com/social-media-stats/all/europe>. WhatsApp ha oltre il 90% di penetrazione in diversi paesi europei, ad esempio 95,5% in Germania e 92,2% in Spagna: <https://adamconnell.me/whatsapp-statistics/>.

¹⁰ Nel mercato europeo dei sistemi operativi mobili, Android copre circa il 65–66% e iOS circa il 34–35% (StatCounter, agosto 2024–agosto 2025): <https://gs.statcounter.com/os-market-share/mobile/europe>.

Questo dominio multi-settore dei grandi intermediari digitali solleva preoccupazioni economiche: se da un lato esso è certamente causa di efficienze innovative e di benefici apprezzati dai consumatori (quali la riduzione dei costi di ricerca, l'accesso a servizi personalizzati, la maggiore rapidità delle transazioni e, in molti casi, la gratuità apparente del servizio), dall'altro lato il potere di mercato così concentrato può condurre ad abusi, riduzione della concorrenza, minore innovazione e svantaggi per utenti e imprese più piccoli.

Va notato, peraltro, che l'ascesa dei mercati digitali non ha solo conseguenze economiche, ma anche sociali e politiche di rilievo¹¹. Le grandi piattaforme svolgono un ruolo centrale nell'accesso all'informazione, nel funzionamento della sfera pubblica e nella formazione dell'opinione collettiva, influenzando in modo diretto la qualità del dibattito democratico. Esse incidono, inoltre, sulla tutela dei diritti fondamentali (privacy, libertà di espressione, diritto alla non discriminazione) e pongono questioni nuove in termini di responsabilità e impatti sociali.

Tale evoluzione ha messo in discussione l'adeguatezza dei paradigmi regolatori tradizionali. Le piattaforme digitali hanno la capacità di "ridefinire le regole del gioco"¹² e pongono un'urgente necessità di ripensare gli approcci normativi, in particolare nel campo della regolazione economica. Il potere crescente di colossi come Amazon o Google ha catalizzato un ampio dibattito – dalla comunità accademica ai decisori pubblici – su come aggiornare le politiche per garantire mercati equi, promuovere l'innovazione e tutelare imprese e consumatori in un contesto sempre più dominato dalle piattaforme online.

In risposta a queste sfide, le autorità di varie giurisdizioni hanno iniziato a valutare nuovi strumenti normativi per contenere gli eccessi di potere delle *big tech* e preservare la contestabilità dei mercati digitali.

¹¹ Si veda, per esempio, S. ZUBOFF, *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*, Roma: Luiss University Press, 2019, che descrive come le grandi piattaforme digitali abbiano trasformato i dati personali degli utenti in materia prima per un nuovo modello economico, fondato sull'estrazione, la previsione e la modifica dei comportamenti. Secondo l'autrice, ciò non produce solo effetti economici, ma incide profondamente sulla sfera sociale e politica, minacciando la privacy, l'autonomia individuale e persino il funzionamento della democrazia.

¹² Così Margrethe Vestager, Vicepresidente esecutiva della Commissione europea responsabile per la politica di concorrenza, nelle dichiarazioni rese in seguito al compromesso politico sul DMA, del 31 marzo 2022, disponibile al link: https://ec.europa.eu/commission/presscorner/detail/en/speech_22_2042. In quell'occasione, Vestager ha sottolineato come le grandi piattaforme non siano semplicemente attori del mercato, ma vere e proprie "regole del gioco" (*rule-makers*) capaci di condizionare la concorrenza e l'innovazione nei mercati digitali.

3. Diritto della concorrenza e mercati digitali

Il diritto della concorrenza (o diritto antitrust) tradizionale fornisce gli strumenti giuridici per tutelare l'assetto competitivo nei mercati.

Ad esempio, nell'Unione europea, l'abuso di posizione dominante è vietato dall'art. 102 TFUE, e analoghe norme esistono nelle legislazioni nazionali (in Italia, art. 3 L. 287/90)¹³. Una posizione dominante in sé non è illecita – può risultare da meritato successo competitivo – ma diventa sanzionabile quando viene abusata per escludere concorrenti o sfruttare i clienti, con effetti dannosi sul benessere dei consumatori.

Negli anni recenti, le autorità antitrust hanno più volte affrontato comportamenti anticoncorrenziali da parte dei colossi digitali. Ad esempio, alla società Google è stato contestato un comportamento di *self-preferencing* nei risultati del motore di ricerca, ovvero la sistematica preferenza accordata ai propri servizi di comparazione prezzi a scapito dei concorrenti¹⁴.

Si ricordano anche il procedimento relativo alle restrizioni imposte ai produttori di dispositivi Android, accusati di essere vincolati a pre-installare le applicazioni di Google (Search e Chrome) e ad adottare esclusivamente la versione autorizzata del sistema operativo, condotte ritenute atte a rafforzare la posizione dominante del motore di ricerca¹⁵; quello nei confronti di Apple per aver imposto condizioni contrattuali gravose agli sviluppatori dell'App Store, in particolare l'obbligo di utilizzare il sistema di pagamento in-app della società e il divieto di informare i consumatori circa modalità alternative di acquisto più convenienti¹⁶; infine, il procedimento contro Amazon per l'uso di dati dei venditori terzi presenti sul proprio *marketplace* per orientare le proprie strategie di vendita e sviluppare prodotti a marchio proprio in concorrenza diretta con gli stessi¹⁷.

¹³ Ricordiamo le altre fattispecie tradizionalmente ricondotte al diritto antitrust: gli accordi restrittivi della concorrenza, vietati dall'art. 101 TFUE e dall'art. 2 L. 287/90; il controllo preventivo delle concentrazioni, disciplinato dal Regolamento (CE) n. 139/2004 e dall'art. 16 ss. L. 287/90.

¹⁴ Caso *Google Search (Shopping)*, Commissione europea, Decisione C(2017) 4444 final, 27 giugno 2017, che ha inflitto a Google una sanzione pari a 2,42 miliardi di euro per abuso di posizione dominante ai sensi dell'art. 102 TFUE.

¹⁵ Caso *Google Android*, Commissione europea, Decisione C(2018) 4761 final, 18 luglio 2018, con cui è stata comminata a Google una sanzione di 4,34 miliardi di euro.

¹⁶ Caso *Apple App Store (Spotify)*, Commissione europea, procedimento AT.40437, concluso con decisione del 4 marzo 2024 che ha irrogato una sanzione di circa 1,8 miliardi di euro.

¹⁷ Caso *Amazon Marketplace e uso dei dati dei venditori terzi*, Commissione europea, procedimento AT.40462 e AT.40703, chiuso con impegni vincolanti il 20 dicembre 2022.

Questi interventi hanno portato a ingenti sanzioni (per esempio, l'Ue ha comminato multe record a Google per oltre 8 miliardi di euro complessivi) e in alcuni casi a obblighi correttivi imposti alle imprese.

Tuttavia, l'azione *ex post* – cioè una volta che la pratica anticoncorrenziale si è già materializzata – del diritto antitrust presenta limiti strutturali nei mercati digitali: le indagini e i procedimenti sono complessi e lenti, spesso giungendo a decisione quando ormai il mercato digitale è già “consolidato” (*tipped market*)¹⁸ a favore del monopolista; inoltre, molte condotte tipiche delle piattaforme (come la preferenza data ai propri servizi, l'uso incrociato dei dati, le clausole di esclusiva o di parità, ecc.) mettono in discussione l'applicazione dei criteri antitrust tradizionali, che sono stati pensati per i mercati analogici, in cui gli effetti anticoncorrenziali sono tendenzialmente più evidenti.

In effetti, si è fatta sempre più largo l'idea che le norme antitrust generali, da sole, siano insufficienti ad affrontare le peculiari sfide poste dai mercati digitali a più versanti¹⁹. Questa consapevolezza ha stimolato, a livello internazionale, una “concorrenza regolamentare” tra diverse giurisdizioni, tutte alla ricerca di soluzioni innovative per governare il potere dei grandi intermediari online.

Ad esempio, già all'inizio del 2021 la Germania ha modificato la propria legge antitrust (*Gesetz gegen Wettbewerbsbeschränkungen*) introducendo il paragrafo §19a. Questo consente al *Bundeskartellamt* (l'Autorità federale tedesca della concorrenza) di designare alcune imprese digitali come aventi “importanza preminente per la concorrenza intersettoriale” e di vietare in via preventiva una serie di condotte ritenute anticoncorrenziali (come forme di auto-preferenza, bundling forzato, ostacoli all'interoperabilità, ecc.). Contestualmente, il legislatore tedesco ha esteso ai rapporti tra piattaforme e utenti business il concetto di abuso di dipendenza economica, tradizionalmente riferito ai fornitori che dipendono da un unico distributore dominante²⁰.

In Italia, oltre all'applicazione delle norme generali in materia di abuso di posizione dominante da parte dell'Autorità Garante della Concorrenza e del Mercato (AGCM), il legislatore è intervenuto direttamente per affrontare alcune pratiche ritenute particolarmente dannose nel contesto delle piattaforme digitali. Un esempio significativo è rappresentato dalla nullità delle clausole di pa-

¹⁸ Il concetto di *tipped market*, ovvero di mercato già consolidatosi a favore di un unico operatore in virtù di effetti di rete e dinamiche cumulative, è stato sviluppato da diversi autori: si veda, ad esempio, N. PETIT, *Big tech and the digital economy: The monopolopoly scenario*, Oxford: Oxford University Press, 2020.

¹⁹ Si veda, su tutti, R. PODSZUN, S. KREIFELS, *Digital platforms and competition law*, in *J. Eur. Consumer & Mkt. L.*, 2016 (5), p. 33.

²⁰ Cfr. Riforma della legge antitrust tedesca (10. GWB-Novelle, nota anche come *GWB-Digitalisierungsgesetz*), entrata in vigore il 19 gennaio 2021.

rità tariffaria (cosiddette *most favoured nation clauses*) introdotto con la legge di bilancio del 2019²¹. Tali clausole, molto diffuse (non solo) nel settore delle piattaforme di prenotazione alberghiera online, obbligavano le strutture alberghiere a non offrire sui propri siti o su altre piattaforme condizioni più vantaggiose rispetto a quelle praticate sul portale dominante (come Booking.com o Expedia). L'AGCM aveva già avviato procedimenti nei confronti di queste pratiche, ritenute idonee a ridurre la libertà commerciale delle strutture ricettive e a mantenere elevate le commissioni applicate dalle piattaforme. Con l'intervento legislativo, l'uso di tali clausole è stato sanzionato con la nullità contrattuale, segnando un passo importante nel contrasto a forme di abuso contrattuale tipiche dei mercati digitali e nel rafforzamento del principio di concorrenza effettiva. Questa scelta normativa riflette l'esigenza di affiancare agli strumenti antitrust tradizionali misure mirate, capaci di riequilibrare rapporti contrattuali caratterizzati da forti asimmetrie di potere tra le grandi piattaforme e gli operatori di dimensioni minori.

Così, in modo analogo, altri paesi e autorità (Regno Unito, Stati Uniti, Australia, Cina) hanno avviato riforme o studi per dotarsi di strumenti ex ante mirati alle piattaforme digitali. Ad esempio, nel Regno Unito la Competition and Markets Authority (CMA) ha proposto l'istituzione della *Digital Markets Unit* (2021), che ha il compito di sorvegliare le imprese con uno *strategic market status* e di imporre regole comportamentali ex ante per garantire condizioni di concorrenza leale²².

L'Unione Europea ha progressivamente costruito un proprio quadro di intervento sui mercati digitali: un percorso iniziato con misure settoriali di trasparenza nel Regolamento Platform to Business e culminato con l'adozione nel 2022 di uno strumento organico di regolazione ex ante, il Digital Markets Act, destinato a operare in parallelo al diritto antitrust generale.

4. Il Regolamento Platform-to-Business

Il primo passo dell'Ue per affrontare gli squilibri nei mercati digitali è stato il Regolamento (UE) 2019/1150, noto come Regolamento "Platform-to-Business" (P2B)²³. Esso trova applicazione dal 12 luglio 2020 e mira a pro-

²¹ F. GALLI, *La nullità della clausola 'MFN' nei contratti tra agenzie di intermediazione telematiche e imprese alberghiere*, in *Le nuove leggi civili commentate*, 2018 (41), pp. 1387-1425.

²² CMA, *A new pro-competition regime for digital markets*, aprile 2021: <https://www.gov.uk/government/publications/a-new-pro-competition-regime-for-digital-markets>.

²³ Regolamento (UE) 2019/1150 del Parlamento europeo e del Consiglio, del 20 giugno 2019, che promuove equità e trasparenza per gli utenti commerciali dei servizi di intermediazione online, GU L 186 dell'11.7.2019, pagg. 57-79.

muovere equità e trasparenza nei rapporti contrattuali tra le piattaforme online e i loro utenti commerciali (ossia le imprese che utilizzano tali piattaforme per raggiungere i consumatori)²⁴.

In realtà, il Regolamento P2B non è uno strumento di concorrenza in senso stretto: esso piuttosto mira a riequilibrare i rapporti contrattuali tra piattaforme e utenti commerciali (es. venditori, sviluppatori, inserzionisti, etc.), ponendo rimedio a situazioni di asimmetria di potere negoziale che rischiano di tradursi in pratiche commerciali scorrette e opache. L'intervento del legislatore europeo si colloca, infatti, in una logica di regolazione pro-concorrenziale e di tutela procedurale, volta a garantire maggiore prevedibilità e correttezza nei rapporti B2B (dove uno dei due professionisti sia appunto una piattaforma), piuttosto che a reprimere direttamente condotte abusive ai sensi del diritto antitrust.

In quanto ad ambito di applicazione, il Regolamento copre i servizi di intermediazione online (quali mercati digitali, marketplace, app store, piattaforme di prenotazione, siti di comparazione dei prezzi, etc.) e i motori di ricerca online, purché offrano servizi a imprese stabilite nell'UE.

Dal punto di vista del contenuto, il Regolamento P2B introduce una serie di obblighi a carico dei gestori di piattaforme orientati su due assi principali: obblighi di trasparenza e obblighi di correttezza, che includono anche l'accesso a strumenti di ricorso.

Nel primo gruppo, i fornitori di servizi di intermediazione online devono rendere chiare e accessibili le condizioni contrattuali verso gli utenti commerciali. Ad esempio, i termini di servizio devono essere scritti in linguaggio semplice, devono essere disponibili anche in fase precontrattuale e facilmente reperibili (art. 3).

Devono inoltre indicare in modo esplicito le motivazioni che possono portare a sospensione o cessazione dell'account dell'utente commerciale (art. 4) nonché fornire informazioni sui criteri di *ranking* che influenzano la visibilità dei prodotti e servizi sulla piattaforma (art. 5). Vanno dichiarati eventuali beni o servizi accessori offerti dalla piattaforma assieme a quelli dell'utente commerciale, e l'eventuale utilizzo da parte della piattaforma di canali di distribuzione aggiuntivi (ad esempio, programmi di affiliazione) per commercializzare i prodotti degli utenti business (art. 6).

Infine, se la piattaforma applica un trattamento differenziato ai propri prodotti e servizi rispetto a quelli di terzi (ad esempio un proprio prodotto messo in evidenza), tale differenza di trattamento va dichiarata e descritta (art. 7). In-

²⁴ In realtà, come chiarisce l'art. 1, il Regolamento tutela "gli utenti commerciali di servizi di intermediazione online e gli utenti titolari di siti web aziendali che siano in relazione con motori di ricerca online".

fine, sono richiesti preavvisi minimi per modifiche unilaterali dei termini contrattuali (in genere 30 giorni di preavviso) e il divieto di modifiche retroattive delle condizioni, salvo consenso delle parti o obbligo legislativo (art. 8).

Nel secondo gruppo (ossia gli obblighi di correttezza che includono l'accesso a strumenti di ricorso), il Regolamento P2B vieta una serie di pratiche considerate scorrette nei confronti degli utenti commerciali e richiede l'adozione di procedure di risoluzione delle dispute.

Ad esempio, sono vietate sospensioni o cancellazioni di account degli utenti commerciali senza adeguata motivazione o preavviso (art. 4). I gestori di piattaforme devono implementare sistemi interni di gestione dei reclami, gratuiti e tempestivi, per affrontare le contestazioni sollevate dagli utenti commerciali sul servizio (art. 11). Devono indicare nei termini almeno due mediatori indipendenti con cui sono disposti a cooperare per risolvere in via extragiudiziale eventuali controversie (art. 12).

Una disposizione è dedicata infine all'accesso ai dati (art. 9). Il Regolamento impone ai gestori di piattaforme online di chiarire nei propri termini e condizioni le modalità con cui i dati generati dalle interazioni tra utenti finali e utenti commerciali vengono raccolti, utilizzati e messi a disposizione delle parti. In particolare, essi devono specificare se e in che misura l'utente commerciale può accedere ai dati prodotti nell'ambito della propria attività sulla piattaforma, e a quali condizioni tali dati possano essere condivisi con terzi. L'obiettivo è ridurre l'asimmetria informativa tra piattaforma e impresa utente, favorendo una maggiore trasparenza e prevedibilità nell'utilizzo delle informazioni, che costituiscono una risorsa economica cruciale nei mercati digitali.

Sebbene il regolamento P2B preveda queste tutele, va notato che molte sue disposizioni non sono accompagnate da sanzioni immediate. L'art. 15, infatti, rimette l'attuazione e l'applicazione concreta del regolamento alle autorità nazionali competenti, lasciando così un certo margine di discrezionalità agli Stati membri nella scelta degli organi responsabili e delle procedure di enforcement.

In Italia, il monitoraggio del rispetto del regolamento P2B e l'irrogazione delle eventuali sanzioni sono stati attribuiti all'AGCOM (Autorità per le Garanzie nelle Comunicazioni). In virtù di quanto previsto dall'art. 1, comma 515, della legge n. 178/2020 (legge di bilancio 2021)²⁵, AGCOM svolge attività di vigilanza sull'applicazione del regolamento, sia su segnalazione di soggetti inte-

²⁵ La legge n. 178/2020 (legge di bilancio 2021), all'art. 1, comma 515, ha introdotto la misura di adeguamento necessaria per dare attuazione al Regolamento (UE) 2019/1150. In particolare, essa ha modificato la legge istitutiva dell'AGCOM (l. n. 249/1997), ampliandone le competenze e attribuendole espressamente il potere di vigilanza e sanzione in materia di applicazione del Regolamento P2B.

ressati sia d'ufficio. Qualora accerti violazioni delle disposizioni del P2B da parte di piattaforme online o motori di ricerca, l'Autorità è tenuta ad avviare i relativi procedimenti sanzionatori.

5. Il Digital Markets Act

Un secondo passo più decisivo verso la regolazione dei mercati digitali è stato compiuto con il Digital Markets Act (DMA)²⁶, alla cui analisi dedicheremo il resto di questo capitolo.

Questo regolamento è stato proposto nel 2020, insieme al Digital Services Act²⁷, contribuendo ad un “pacchetto” di riforme per l'economia digitale europea. Il testo finale del DMA è stato pubblicato nella Gazzetta ufficiale dell'Ue il 12 ottobre 2022 ed è entrato in vigore il 1° novembre 2022.

5.1. Ambito di applicazione e relazione con il diritto generale della concorrenza e con il Regolamento P2B

Secondo l'articolo 1, il DMA mira a contribuire al corretto funzionamento del mercato interno stabilendo norme armonizzate che garantiscano mercati “equi e contendibili” nel settore digitale in tutta l'Unione, a vantaggio degli utenti commerciali e dei consumatori.

Dunque, a differenza del tradizionale diritto antitrust, basato su principi generali come il divieto di abuso di posizione dominante applicati dopo che il comportamento illecito ha prodotto effetti, il DMA impone regole specifiche *ex ante* ai grandi operatori digitali prima che certi comportamenti possano nuocere alla concorrenza²⁸. In altre parole, non sostituisce il diritto antitrust ma lo affianca: costituisce un insieme di obblighi e divieti preventivi rivolti a soggetti designati come gatekeeper, per integrare e rendere più tempestiva la tutela della concorrenza nel contesto digitale.

Resta perciò ferma la possibilità per le autorità antitrust di intervenire con gli strumenti ordinari in fattispecie non coperte dal DMA o per sanzionare condotte abusive ulteriori; il DMA prevede infatti espressamente che le sue disposizioni si applicano fatte salve le norme generali antitrust (ad es. l'art. 102

²⁶ Regolamento (UE) 2022/1925 del Parlamento europeo e del Consiglio del 14 settembre 2022 sui mercati equi e contendibili nel settore digitale e che modifica le direttive (UE) 2019/1937 e (UE) 2020/1828, pubblicato in G.U.U.E. L 265 del 12 ottobre 2022, p. 1 ss.

²⁷ Regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio del 19 ottobre 2022 relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (Digital Services Act), pubblicato in G.U.U.E. L 277 del 27 ottobre 2022, p. 1 ss.

²⁸ R. PODSZUN, P. BONGARTZ, S. LANGENSTEIN, *The digital markets act: Moving from competition law to regulation for large gatekeepers*, in J. Eur. Consumer & Mkt. L., 2021 (10), p. 60.

TFUE) e altre normative settoriali. È fondamentale però che vi sia coordinamento tra le nuove regole e le normative esistenti (a livello sia Ue che nazionale) per evitare sovrapposizioni o conflitti – ad esempio in materia di antitrust nazionale o di tutela dei dati personali.

Il DMA si applica solo a un numero ristretto di attori: i fornitori di “servizi di piattaforma di base” (*core platform services*) che vengano formalmente designati come “gatekeeper” (vedi *infra*). I servizi di piattaforma di base coperti dal Regolamento comprendono dieci categorie principali di servizi digitali, i servizi di intermediazione online (ad es. marketplace di *e-commerce*, app store), i motori di ricerca online, i servizi di *social network*, le piattaforme di condivisione video, i servizi di comunicazione interpersonale non basati su numeri (come le applicazioni di messaggistica), i sistemi operativi, i *browser web*, gli assistenti virtuali, i servizi di *cloud computing*, e i servizi pubblicitari online collegati a uno degli altri servizi elencati²⁹. Si tratta di una lista chiusa: servizi digitali non rientranti in tali categorie restano esclusi dal campo di applicazione del DMA, anche se forniti da imprese di grandi dimensioni.

Rispetto al Regolamento P2B visto nel precedente paragrafo, dunque, il DMA ha un ambito di applicazione più ampio perché coinvolge anche altri intermediari digitali, come i sistemi operativi, i browser, i servizi di cloud computing o gli assistenti virtuali, che non rientravano nell’orizzonte applicativo del P2B, limitato invece ai soli servizi di intermediazione online e ai motori di ricerca.

D’altra parte, a differenza del P2B, il DMA richiede che gli intermediari soddisfino specifici criteri di dimensione ed influenza sistemica per poter essere formalmente designati come “gatekeeper”. Non tutte le piattaforme, dunque, sono soggette al nuovo regime: soltanto quelle che, per fatturato, base di utenti e diffusione territoriale, svolgono un ruolo di “porta d’accesso” imprescindibile tra imprese e consumatori (vd. *infra*).

In sostanza, il Regolamento ha nel mirino le piattaforme che fungono da infrastrutture essenziali dell’economia digitale, attraverso cui altri operatori raggiungono utenti finali. L’introduzione del DMA è motivata proprio dall’esigenza di fronteggiare il crescente potere economico detenuto da alcuni gestori di piattaforme “sistemiche”, evitando che possano usare il loro ruolo per chiudere il mercato o ostacolare l’ingresso di nuovi concorrenti, a detrimento dell’innovazione³⁰.

²⁹ Articolo 2, paragrafo 2 del DMA

³⁰ M. CINI, P. CZULNO, *Digital Single Market and the EU Competition Regime: An Explanation of Policy Change*, in *Journal of European Integration*, 2022 (44), pp. 41-57.

Come affermato dalla Commissione, l'obiettivo è garantire condizioni eque (*fair*) per le imprese che dipendono da queste piattaforme e contestabilità (*contestable markets*), ossia la possibilità per nuovi entranti o operatori più piccoli di sfidare i "gatekeeper" sui meriti. In tal senso, il DMA si pone come un corpus di obblighi asimmetrici (applicati solo ai *player* dominanti) volti a correggere *ex ante* le distorsioni più rilevanti osservate nei mercati digitali recenti.

È importante sottolineare che il DMA, essendo un regolamento europeo, è direttamente applicabile e vincolante in tutti gli Stati membri senza bisogno di recepimento, assicurando così un quadro uniforme nell'intero mercato unico digitale.

5.2. I gatekeeper e la loro designazione

Il concetto di "gatekeeper" è al centro del DMA. In termini generali, un gatekeeper è un'impresa che soddisfa tre criteri qualitativi³¹:

- (a) ha un impatto significativo sul mercato interno dell'Ue,
- (b) fornisce un servizio di piattaforma di base che costituisce un importante punto di accesso (*gateway*) tra imprese e consumatori, e
- (c) detiene (o prevedibilmente deterrà nel prossimo futuro) una posizione solida e duratura.

Per rendere operativa questa definizione, il Regolamento stabilisce alcune soglie quantitative che fanno presumere il soddisfacimento dei criteri di gatekeeper.

In particolare, si presume che un'impresa abbia un impatto significativo sul mercato interno (criterio della lettera *a*) quando realizza un fatturato annuo nell'Unione di almeno 7,5 miliardi di euro negli ultimi tre esercizi, oppure ha una capitalizzazione di mercato (o valore di borsa) di almeno 75 miliardi di euro nell'ultimo esercizio, e allo stesso tempo fornisce un servizio di piattaforma di base in almeno tre Stati membri dell'UE.

Inoltre, si presume che un servizio di piattaforma di base sia un punto di accesso importante (criterio della lettera *b*) quando esso conta almeno 45 milioni di utenti finali attivi mensilmente nell'Unione e 10.000 utenti commerciali attivi annualmente nell'ultimo anno finanziario. Se queste soglie vengono raggiunte in tre esercizi finanziari precedenti, si presume anche che il gatekeeper abbia una posizione solida e duratura (criterio della lettera *c*).

Un'impresa che soddisfa tutti questi criteri è tenuta entro 2 mesi a notificare formalmente alla Commissione europea il fatto di aver raggiunto lo status di gatekeeper. Dopo la notifica, la Commissione valuta i dati e adotta una deci-

³¹ Art. 3 del DMA.

sione che designa ufficialmente l'impresa come gatekeeper, specificando a quali servizi di piattaforma di base forniti dalla stessa si applicano gli obblighi del DMA. La designazione deve avvenire senza indugio e al più tardi entro 45 giorni lavorativi dalla notifica completa.

Qualora un'impresa ritenga di non soddisfare le condizioni pur superando le soglie (o viceversa, cioè ritenga di soddisfare le condizioni non superando le soglie), può presentare argomentazioni alla Commissione, la quale ha facoltà di svolgere un'indagine di mercato più approfondita (entro massimo 5 mesi) per confermare o meno la designazione. Inoltre, la Commissione può designare come gatekeeper anche un fornitore di servizi di piattaforma di base che non supera tutte le soglie di cui sopra, se attraverso un'indagine di mercato accerta che esso soddisfa alcuni requisiti qualitativi, come ad esempio le dimensioni e le attività dell'impresa, il numero di utenti, gli effetti di rete e i vantaggi basati sui dati, gli effetti di scala, il lock-in degli utenti commerciali e dei consumatori.

A partire dalla data di designazione, il gatekeeper dispone in genere di sei mesi di tempo per conformarsi a tutti gli obblighi del DMA.

È importante notare che la designazione è legata ai singoli servizi di piattaforma di base. Così, ad esempio, il gruppo Alphabet è stato individuato come gatekeeper non solo per il motore di ricerca Google Search, ma anche per Android come sistema operativo, per l'app store Google Play, per YouTube quale piattaforma di condivisione video, per Chrome come browser, per Google Maps e per Google Shopping nell'ambito dell'intermediazione online, oltre che per i servizi di pubblicità digitale tramite Google Ads. Analogamente, ad Amazon lo status di gatekeeper è stato riconosciuto per il marketplace e per i servizi pubblicitari collegati, mentre ad Apple per l'App Store, il browser Safari e il sistema operativo iOS. Altri casi hanno riguardato Booking.com per l'intermediazione alberghiera, ByteDance per TikTok come social network, Meta per i propri social e servizi di comunicazione (Facebook, Instagram, WhatsApp e Messenger, oltre a Marketplace) e Microsoft per Windows e LinkedIn³².

³² European Commission, "Digital Markets Act: Commission designates six gatekeepers", 6 settembre 2023 — prima decisione di designazione che include Alphabet, Amazon, Apple, ByteDance, Meta, Microsoft, con l'elenco dei *core platform services* designati. https://ec.europa.eu/commission/presscorner/detail/en/ip_23_4328; European Commission, "DMA designated Gatekeepers – Digital Markets Act", aggiornamenti successivi includenti Booking.com (29 aprile 2024) per il servizio di intermediazione online; vedi la pagina istituzionale "Gatekeepers" con l'elenco completo aggiornato al 2025: https://digital-markets-act.ec.europa.eu/gatekeepers_en.

Questa elencazione, riferita al 2025, riflette l'approccio selettivo e mirato del Regolamento, che guarda alla natura di ciascun servizio e non alla sola dimensione del gruppo economico.

Proprio in questo contesto emerge il problema della corretta delimitazione dei servizi di piattaforma di base. In alcuni casi, infatti, la Commissione ha dovuto valutare se procedere a una designazione congiunta o separata: emblematici sono i casi di Messenger e Marketplace di Facebook, trattati come servizi distinti.

Un ulteriore elemento di complessità riguarda l'utilizzo degli indicatori quantitativi e qualitativi: non sempre i dati numerici bastano per stabilire la soglia di gatekeeper, come si è visto nella discussione sull'inclusione o meno di iPadOS come sistema operativo distinto rispetto a iOS³³. In altri casi, la Commissione ha accettato la cosiddetta "prova contraria": è accaduto, ad esempio, per Gmail³⁴ e per TikTok Ads³⁵, ritenuti non configurabili come servizi di piattaforma di base autonomi. Diversamente, i tentativi di Meta e ByteDance di contestare la designazione dei propri servizi principali come gatekeeper non hanno avuto esito favorevole: la Corte di giustizia dell'Unione europea ha confermato le decisioni della Commissione, respingendo i ricorsi e consolidando la legittimità dell'approccio adottato³⁶.

Restano invece ancora aperte alcune questioni relative a specifici servizi: la Commissione ha avviato indagini di mercato, ai sensi dell'art. 17, paragrafo 3, su Microsoft Edge, Bing e i servizi pubblicitari Microsoft Ads, così come su iMessage di Apple e sul social network X (già Twitter). In questi casi, all'esito delle indagini, la Commissione ha concluso di non designare tali servizi come gatekeeper, riconoscendo che non raggiungono in modo pieno i requisiti richiesti. Ciò conferma il carattere dinamico e basato su un approccio caso per caso del processo di designazione, che si articola non solo attraverso soglie

³³ Commissione europea, Decisione di designazione dei gatekeeper ai sensi dell'art. 3, par. 9 DMA, 6 settembre 2023, relativa ad Apple, in cui iPadOS non è stato ritenuto, allo stato, un sistema operativo "core" distinto da iOS.

³⁴ Commissione europea, Decisione di designazione dei gatekeeper ai sensi dell'art. 3, par. 9 DMA, 6 settembre 2023, relativa ad Alphabet, in cui Gmail è stato escluso dall'elenco dei servizi di piattaforma di base.

³⁵ Commissione europea, Decisione di designazione dei gatekeeper ai sensi dell'art. 3, par. 9 DMA, 6 settembre 2023, relativa a ByteDance, con la quale i servizi pubblicitari collegati a TikTok non sono stati qualificati come CPS autonomi.

³⁶ Tribunale dell'Unione europea, Ordinanza 9 febbraio 2024, causa T-107/24 R, ByteDance Ltd. c. Commissione europea, che ha respinto la richiesta di sospensione dell'esecuzione della decisione di designazione come gatekeeper. Analogo esito nel procedimento avviato da Meta Platforms Ireland Ltd.

economiche e di utenza, ma anche tramite un attento scrutinio qualitativo del ruolo effettivamente svolto da ciascun servizio nel mercato digitale europeo.

5.3. Obblighi e divieti ad applicazione diretta

Il cuore del DMA consiste in una lista di obblighi e divieti imposti ai gatekeeper, volti a prevenire a monte comportamenti sleali o restrittivi della concorrenza. In buona parte, tali regole si ispirano a problematiche emerse in casi antitrust o segnalazioni degli ultimi anni, andando a codificare in disposizioni regolamentari alcune “*best practices*” che i gatekeeper dovranno rispettare.

Il DMA distingue tra obblighi ad applicazione diretta e obblighi suscettibili di specificazione (si veda *infra*).

Gli obblighi ad applicazione diretta (contenuti principalmente nell’articolo 5 del DMA) sono quelli che non richiedono ulteriori atti attuativi o valutazioni caso per caso: il gatekeeper deve osservarli immediatamente e automaticamente una volta designato, senza bisogno di istruzioni aggiuntive da parte della Commissione europea. In pratica, si tratta di una sorta di “*black list*” di pratiche vietate (o di obblighi) la cui violazione costituisce di per sé un illecito. Di seguito evidenziamo i più importanti³⁷.

Un primo obbligo riguarda il divieto di combinare dati senza consenso dell’utente finale³⁸: il gatekeeper non può unire o incrociare dati personali degli utenti raccolti da diversi servizi, né utilizzare i dati raccolti presso terzi tramite il suo servizio, se non a seguito di esplicito consenso dell’utente³⁹. Ad esempio, una piattaforma non potrà combinare i dati di un utente del suo social network con quelli della sua app di messaggistica per finalità di profilazione o pubblicità, senza previa autorizzazione. Tale disposizione è volta a rafforzare la tutela della privacy e a impedire che il vantaggio competitivo dei gatekeeper derivi dall’uso incrociato dei dati su larga scala.

³⁷ L’elenco qui proposto non è esaustivo, ma copre le misure più rilevanti di applicazione diretta. In totale, il DMA include 13 obblighi e 9 divieti specifici rivolti ai gatekeeper. Alcuni si applicano trasversalmente a tutti i servizi di piattaforma di base, altri solo a determinati servizi (ad es. motori di ricerca, app store, social network).

³⁸ Articolo 5, paragrafo 2 del DMA

³⁹ Il consenso è definito con riferimento all’articolo 4, paragrafo 11, del GDPR, ossia come «qualsiasi indicazione libera, specifica, informata e inequivocabile della volontà dell’interessato con la quale egli, mediante una dichiarazione o una chiara azione affermativa, manifesta il proprio consenso al trattamento dei dati personali che lo riguardano». Sul rapporto tra il consenso come base giuridica del trattamento dei dati e il consenso dell’art. 5, paragrafo 2 del DMA, si veda A. D’AMICO, *The DMA’s Consent Moment and its Relationship with the GDPR*, in *European Journal of Risk Regulation*, 2024, pp. 1-14.

Un secondo divieto concerne le vendite abbinate e le iscrizioni obbligatorie⁴⁰. Il gatekeeper non può costringere gli utenti a servirsi di un servizio aggiuntivo come condizione per accedere al servizio principale. In altre parole, è vietato rendere obbligatoria l'iscrizione ad altri servizi dello stesso gruppo (o l'uso di un sistema di autenticazione proprietario) per poter accedere a un servizio di piattaforma di base. Allo stesso modo, è proibito vincolare l'utilizzo della piattaforma all'adozione di strumenti complementari del gatekeeper (ad esempio sistemi di pagamento, motori di ricerca o browser) se non strettamente necessari. Questo obbligo, noto come “*anti-tying*”, mira a preservare la libertà di scelta degli utenti rispetto a prodotti e servizi alternativi di terzi.

Il Regolamento vieta inoltre al gatekeeper di discriminare gli utenti commerciali imponendo clausole di parità⁴¹. È fatto divieto di impedire ai business users di offrire i loro beni o servizi su piattaforme concorrenti o a condizioni diverse (anche più vantaggiose). Sono quindi bandite le cosiddette *most-favoured-nation clauses* che, come abbiamo detto sopra, alcune piattaforme imponevano per mantenere condizioni uniformi. Ciò significa, ad esempio, che un app store non potrà vietare a uno sviluppatore di proporre la propria applicazione a un prezzo inferiore su uno store alternativo, così come un *marketplace* non potrà penalizzare un venditore che scelga di offrire i propri prodotti su altri siti a condizioni migliori. In questo modo si salvaguarda la libertà commerciale degli operatori e si promuove la concorrenza tra canali distributivi.

Un ulteriore obbligo riguarda la trasparenza nella pubblicità digitale⁴². Il gatekeeper che fornisce servizi pubblicitari online è tenuto a comunicare con chiarezza prezzi e performance del posizionamento degli annunci pubblicitari sia agli inserzionisti sia ai *publisher* (cioè gli operatori di siti web che pubblicano tali annunci). Deve quindi fornire quotidianamente informazioni dettagliate sui costi delle campagne e sulle metriche di misurazione (click, visualizzazioni, ecc.), oltre a consentire l'accesso a strumenti indipendenti per la verifica delle performance. Questa disposizione contribuisce a ridurre l'opacità del settore pubblicitario digitale, prevenendo possibili sfruttamenti delle asimmetrie informative da parte di gatekeeper che spesso svolgono contemporaneamente il ruolo di venditore e intermediario degli spazi pubblicitari.

Particolare attenzione è dedicata anche alla libertà di disinstallare applicazioni predefinite⁴³. Gli utenti devono poter rimuovere facilmente le app preinstallate sui dispositivi o sistemi operativi del gatekeeper, purché non siano es-

⁴⁰ Articolo 5, paragrafi 7 e 8 del DMA.

⁴¹ Articolo 5, paragrafo 3 e 4 del DMA.

⁴² Articolo 5, paragrafi 9 e 10 del DMA.

⁴³ Articolo 5, paragrafo 5 del DMA.

senziali al funzionamento del sistema. È inoltre vietata la pratica di pre-installare un numero ristretto di applicazioni del gatekeeper in posizioni privilegiate tali da compromettere la visibilità delle alternative di terzi. Ne consegue, ad esempio, che produttori di sistemi operativi mobili come Apple o Google non potranno rendere non rimuovibili le proprie app native (browser, mappe, posta elettronica, ecc.) al solo fine di difendere i propri servizi dalla concorrenza, né ostacolare tecnicamente l'installazione di applicazioni o app store di terzi.

Infine, va richiamato anche il divieto di auto-preferenza (*self-preferencing*) dei propri servizi⁴⁴, formalmente collocato tra gli obblighi ad applicazione coordinata, ma strettamente connesso alla logica degli obblighi diretti. Esso vieta al gatekeeper di sfruttare il controllo della piattaforma per favorire indebitamente i propri prodotti o servizi a scapito dei concorrenti. Rientrano in questa categoria le pratiche di posizionamento privilegiato, come la visualizzazione sistematica dei prodotti Amazon Basics sul marketplace Amazon o dei servizi di Google nei risultati del suo motore di ricerca.

5.4. Obblighi e divieti ad applicazione coordinata

Accanto alla “*black list*” sopra indicata, il DMA prevede un insieme aggiuntivo di obblighi e divieti il cui rispetto potrebbe richiedere una maggiore adattabilità o specificazione tecnica. Si tratta delle norme elencate all’Articolo 6, talvolta chiamate “*grey list*”, perché la loro implementazione pratica può variare a seconda del modello di business del gatekeeper e necessita di un “dialogo regolatorio” con la Commissione.

In altre parole, questi obblighi sono comunque vincolanti per i gatekeeper, ma il Regolamento riconosce che potrebbero servire linee guida o misure attuative specifiche per garantire un’efficace conformità.

La Commissione può infatti aprire procedimenti di valutazione sulle misure adottate dal gatekeeper per conformarsi agli obblighi dell’art. 6 e, entro sei mesi, può specificare formalmente le misure necessarie al rispetto della norma. Il gatekeeper stesso può chiedere tale procedura per avere certezza che la sua soluzione sia adeguata. Ciò consente un minimo di flessibilità e confronto tecnico, pur senza compromettere la cogenza delle regole (che restano obbligatorie).

Tra gli obblighi ad applicazione coordinata spicca innanzitutto il divieto di auto-preferenza (*self-preferencing*), previsto dall’art. 6, paragrafo 5 del DMA. Il gatekeeper non può classificare o trattare in modo privilegiato i propri prodotti o

⁴⁴ Articolo 6, paragrafo 5 del DMA.

servizi rispetto a quelli dei concorrenti all'interno della piattaforma che gestisce. Ciò riguarda, ad esempio, l'ordine dei risultati nei motori di ricerca o nei *marketplace*: un motore di ricerca con status di gatekeeper – come Google Search – non potrà posizionare sistematicamente i propri servizi verticali (shopping, mappe, viaggi, ecc.) prima dei risultati organici dei rivali; parimenti, una piattaforma di e-commerce non potrà avvalersi di algoritmi che, a parità di rilevanza, diano visibilità privilegiata alle proprie offerte rispetto a quelle dei venditori terzi. La finalità è prevenire condotte escludenti che sfruttano l'integrazione verticale del gatekeeper. Proprio perché richiede di distinguere tra miglioramenti legittimi dell'esperienza utente e favoritismi anticoncorrenziali, questo obbligo è soggetto a monitoraggio tecnico e a possibili specificazioni da parte della Commissione.

Un altro obbligo di rilievo riguarda l'interoperabilità dei servizi di messaggistica, disciplinata dall'art. 7 DMA ma collocata sistematicamente tra gli obblighi dell'art. 6, paragrafo 7. I gatekeeper che forniscono servizi di comunicazione interpersonale indipendenti dal numero⁴⁵ (come WhatsApp, Messenger o iMessage) devono consentire, su richiesta, l'interconnessione con applicazioni rivali. In termini pratici, un utente di un'app esterna deve poter inviare e ricevere messaggi (testo, voce, video) con un utente del servizio del gatekeeper. L'obbligo verrà attuato gradualmente, partendo dalle funzioni base fino ai gruppi e alle chiamate vocali/video, ed è accompagnato da requisiti tecnici per salvaguardare sicurezza e crittografia *end-to-end*. La misura mira a ridurre l'effetto "giardino recintato"⁴⁶.

Il DMA disciplina, inoltre, l'accesso equo ai dati e la portabilità⁴⁷, ponendosi sul solco sia del Regolamento P2B che, per quanto riguarda gli utenti finali, su quello del GDPR e del diritto alla portabilità riconosciuto al soggetto interessato⁴⁸.

⁴⁵ Si tratta del servizio di comunicazione interpersonale indipendente dal numero come definiti all'articolo 2, punto 7), della direttiva (UE) 2018/1972, cioè di «un servizio di comunicazione interpersonale che non connette in maniera diretta o indiretta con i numeri nazionali o internazionali di un piano di numerazione».

⁴⁶ L'effetto "giardino recintato" (*walled garden*) fa riferimento a un modello di piattaforma digitale chiusa, in cui l'operatore controlla in modo pervasivo l'accesso ai contenuti, ai servizi e ai dati, limitando la possibilità per gli utenti di interagire con sistemi esterni dei grandi servizi di messaggistica, rendendo più contestabile un settore fortemente influenzato dagli effetti di rete.

⁴⁷ Articolo 6, paragrafi 2 e 9 del DMA.

⁴⁸ Ricordiamo che il GDPR ha introdotto, all'art. 20, il diritto dell'interessato alla portabilità dei dati, ossia la facoltà di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano, forniti a un titolare del trattamento, e di trasmetterli a un altro titolare senza impedimenti. Tale diritto include, ove tecnicamente possibile, anche la trasmissione diretta da un titolare all'altro.

In primo luogo, il gatekeeper non può utilizzare i dati generati dagli utenti commerciali sulla propria piattaforma per competere direttamente contro di essi: è la risposta alle pratiche contestate ad Amazon, accusata di sfruttare i dati dei venditori indipendenti per sviluppare prodotti a marchio proprio.

In secondo luogo, il gatekeeper è tenuto a garantire agli utenti commerciali l'accesso ai dati generati o forniti dagli utenti finali nelle loro interazioni, nel rispetto del GDPR. Ciò consente, ad esempio, a un venditore su un marketplace di scaricare i dati relativi alle transazioni e utilizzarli su altri canali. Parallelamente, gli utenti finali devono poter beneficiare di strumenti efficaci di portabilità dei propri dati – in tempo reale e in formato interoperabile – verso altri servizi concorrenti, ampliando il diritto alla portabilità già previsto dall'art. 20 GDPR.

Infine, per i motori di ricerca, l'art. 6, paragrafo 11 introduce un obbligo specifico: fornire ai concorrenti, su richiesta, accesso ai dati anonimi e aggregati delle ricerche e dei click, così da evitare che il vantaggio dei gatekeeper, derivante dal riutilizzo di queste informazioni per migliorare i propri sistemi di ricerca, possa costituire una barriera all'ingresso insormontabile per i concorrenti stessi.

Infine, un obbligo riguarda la libertà di scelta e di installazione per gli utenti finali, sancita dall'art. 6, paragrafo 3. Il gatekeeper deve permettere l'installazione e l'utilizzo di applicazioni o app store di terze parti senza restrizioni ingiustificate, e garantire agli utenti la possibilità di modificare agevolmente le impostazioni predefinite che li vincolano ai suoi servizi. In concreto, un sistema operativo dovrà consentire di impostare un browser o un'app di posta alternativi rispetto a quelli del gatekeeper, mentre uno smartphone dovrà permettere il cosiddetto "*sideloading*" di app store concorrenti. L'obiettivo è aumentare la contestabilità "a portata di click", riducendo i *lock-in* creati da pre-selezioni e blocchi tecnici, pur bilanciando tale apertura con esigenze di sicurezza e protezione degli utenti.

Gli obblighi previsti agli articoli 5-7 (dunque sia quelli ad applicazione diretta che quelli ad applicazione coordinata) possono essere aggiornati dinamicamente. L'art. 12 attribuisce infatti alla Commissione europea il potere di adottare atti delegati per integrare il regolamento, sulla base di quanto emerso dalle indagini di mercato disciplinate dall'art. 19. In questo modo, se dovessero manifestarsi nuove pratiche commerciali sleali o restrittive che, pur non essendo espressamente contemplate nel testo originario, risultino analoghe a quelle già vietate, la Commissione potrà estendere l'applicazione di determinati obblighi a ulteriori servizi di piattaforma di base o a nuove categorie di utenti commerciali.

Si tratta, tuttavia, di un potere limitato: l'aggiornamento non può introdurre *ex nihilo* nuovi obblighi, ma solo ampliare l'ambito soggettivo e oggettivo di quelli già esistenti. In tal senso, l'art. 12 rappresenta uno strumento di flessibilità che consente al DMA di adattarsi all'evoluzione rapida dei mercati digitali, senza dover ricorrere ogni volta a una revisione legislativa completa.

5.5. La conformità e gli altri obblighi dei gatekeeper

Accanto agli obblighi specifici di cui agli articoli 5 e 6, il Digital Markets Act prevede un insieme di disposizioni generali volte ad assicurare la conformità dei gatekeeper al nuovo quadro regolatorio.

In primo luogo, l'art. 8 introduce un generale obbligo di conformità, imponendo alle imprese designate di adottare tutte le misure necessarie per rispettare in modo effettivo e continuativo le prescrizioni del regolamento. Questo dovere generale è poi rafforzato dall'art. 28, che prevede l'istituzione, presso ciascun gatekeeper, di una funzione di conformità interna, dotata di risorse adeguate e di sufficiente indipendenza, incaricata di monitorare l'osservanza delle regole e di riferire regolarmente al management e alla Commissione.

Un ruolo importante è svolto anche dalle relazioni di trasparenza, disciplinate dall'art. 11, che i gatekeeper sono tenuti a presentare periodicamente alla Commissione. Tali relazioni devono descrivere in modo dettagliato le misure adottate per conformarsi agli obblighi del DMA e consentono così all'autorità europea e al pubblico di valutare lo stato di attuazione del regolamento.

Le prime relazioni, rese disponibili da Alphabet, Amazon, Apple, ByteDance, Meta e Microsoft, hanno mostrato approcci differenti⁴⁹: alcuni operatori (in particolare Microsoft, Alphabet, Meta e ByteDance) hanno presentato documenti dettagliati, mentre altri (Apple e Amazon) si sono limitati a rapporti piuttosto brevi e generici. In generale, i gatekeeper tendono ad adottare una strategia difensiva: per gli obblighi che impongono divieti, dichiarano semplicemente di non porre in essere determinate condotte, senza fornire ulteriori evidenze; per gli obblighi che richiedono modifiche positive, spesso si limitano a misure minimali o ad interpretazioni funzionali al proprio modello di business. In alcuni casi, tuttavia, sono stati osservati cambiamenti tangibili, con effetti percepibili sia dal lato degli utenti finali sia da quello degli utenti commerciali. Non manca, d'altra parte, una tendenza ad adattare la portata degli obblighi al pro-

⁴⁹ Le relazioni di conformità predisposte dai gatekeeper ai sensi dell'art. 11 DMA sono rese disponibili sul sito ufficiale della Commissione europea, nella sezione dedicata ai casi di applicazione del Digital Markets Act: <https://digital-markets-act-cases.ec.europa.eu/reports/compliance-reports>.

prio vantaggio competitivo, come nel caso di TikTok, che ha proposto un'interpretazione dei vincoli nel settore pubblicitario coerente con il proprio modello integrato di social e pubblicità mirata.

A queste misure si affiancano ulteriori obblighi di carattere generale. L'art. 13 introduce il requisito di antielusione, che vieta ai gatekeeper di aggirare le regole attraverso artifici strutturali o comportamentali. Ne consegue che un'impresa non può frammentare artificialmente i propri servizi di piattaforma principale al fine di eludere le soglie quantitative per la designazione, né può adottare condotte tecniche, commerciali o contrattuali tali da compromettere l'effettiva applicazione degli obblighi. È parimenti vietato degradare la qualità dei servizi o alterarne le condizioni per scoraggiare gli utenti dall'esercitare i diritti loro garantiti dal DMA, inclusi i casi di interfacce utente ingannevoli (dark patterns).

L'art. 14 introduce invece un obbligo di informativa preventiva sulle operazioni di concentrazione: ogni gatekeeper deve comunicare alla Commissione qualsiasi progetto di fusione o acquisizione che coinvolga un altro fornitore di servizi di piattaforma di base o, più in generale, un'impresa operante nel settore digitale. La notifica è obbligatoria a prescindere dalla sussistenza dei requisiti di notifica previsti dal diritto antitrust ordinario. Lo scopo è evitare che le grandi piattaforme possano rafforzare il proprio potere di mercato attraverso acquisizioni "sotto soglia", sottratte al controllo delle autorità, e garantire così un monitoraggio sistematico delle strategie di crescita dei gatekeeper.

Infine, l'art. 15 introduce un obbligo di audit sulle tecniche di profilazione che coinvolgono consumatori. Entro sei mesi dalla designazione, ciascun gatekeeper deve trasmettere alla Commissione e al Comitato europeo per la protezione dei dati una relazione, sottoposta a verifica indipendente, che descriva in modo analitico le modalità di raccolta e utilizzo dei dati personali attraverso i propri servizi di piattaforma principale. Una sintesi della relazione deve inoltre essere resa pubblica e aggiornata almeno annualmente, in modo da assicurare trasparenza nei confronti di utenti, concorrenti e autorità⁵⁰. L'obiettivo è duplice: da un lato, responsabilizzare i gatekeeper sulle loro pratiche di trattamento dei dati; dall'altro, consentire un controllo esterno volto a prevenire forme eccessivamente invasive di profilazione, che potrebbero falsare la concorrenza e ledere i diritti fondamentali degli utenti.

⁵⁰ La Commissione ha approvato il Regolamento di esecuzione (UE) 2023/814 del 17 aprile 2023, che specifica il contenuto e la forma delle relazioni di audit previste dall'art. 15 DMA, nonché i criteri per la loro verifica indipendente. Il regolamento chiarisce in particolare le modalità di descrizione delle tecniche di profilazione, i requisiti di trasparenza verso gli utenti e la periodicità degli aggiornamenti, rafforzando così la funzione di accountability del nuovo regime.

5.6. Applicazione e sanzioni

Il modello applicativo del Digital Markets Act prevede un ruolo centrale per la Commissione europea. È quest'ultima, infatti, a sorvegliare l'applicazione del regolamento, con poteri di indagine e sanzione potenziati rispetto a quelli anti-trust⁵¹.

Il DMA istituisce in seno alla Commissione una struttura dedicata (in coordinamento con la DG COMP e CNECT) e incoraggia la cooperazione con le autorità nazionali garanti della concorrenza e del digitale, anche attraverso un *High-Level Group*, per confrontarsi sull'attuazione pratica del Regolamento. Tuttavia, le decisioni chiave (designazione dei gatekeeper, accertamento delle infrazioni, comminatoria di sanzioni) spettano alla Commissione; ciò al fine di garantire un approccio unificato in tutta l'Ue ed evitare frammentazioni⁵².

Sul fronte delle sanzioni, il DMA adotta un approccio molto rigoroso, commisurato alla dimensione dei soggetti coinvolti. In caso di inosservanza agli obblighi, la Commissione può imporre al gatekeeper multe fino al 10% del fatturato mondiale totale dell'impresa interessata nell'esercizio precedente. Se l'inosservanza è ripetuta (violazione reiterata della stessa disposizione), la sanzione massima può salire fino al 20% del fatturato mondiale⁵³. In entrambi i casi può trattarsi di importi nell'ordine di miliardi di euro, idonei a dissuadere anche le imprese più grandi dal violare le regole.

Oltre alle sanzioni pecuniarie, la Commissione ha il potere di adottare misure correttive non pecuniarie: può ad esempio adottare decisioni che impongono rimedi comportamentali specifici, come la cessazione di una certa pratica, obbligo di offrire un'interoperabilità entro una scadenza, ecc.).

Infine, in situazioni di inosservanza sistematica del DMA da parte di un gatekeeper – definita come la violazione di obblighi imposta con tre o più decisioni di infrazione nell'arco di otto anni – la Commissione può aprire un'indagine di mercato mirata e proporre misure aggiuntive proporzionate. Tali misure possono includere, tra l'altro, l'imposizione al gatekeeper di cedere parti di attività se necessario per assicurare la conformità, oppure – novità significa-

⁵¹ Gli articoli 20–24 del DMA disciplinano i poteri di indagine della Commissione europea. Essa può richiedere informazioni dettagliate ai gatekeeper e a terzi (art. 21), condurre interviste e audizioni (art. 22), nonché effettuare ispezioni in loco (*dawn raids*) nei locali delle imprese (art. 23), analogamente a quanto avviene nelle indagini antitrust ex Reg. (CE) n. 1/2003.

⁵² Sul difficile coordinamento tra la Commissione europea e le autorità nazionali, si veda I. GRAEF, *Regulating Digital Platforms: Streamlining the Interaction between the Digital Markets Act and National Competition Regimes*, in I. GRAEF, B. VAN DER SLOOT (a cura di), *The Legal Consistency of Technology Regulation in Europe*, Londra: Hart, 2024.

⁵³ Art. 30 del DMA.

tiva introdotta su spinta del Parlamento – la limitazione delle acquisizioni: la Commissione può proibire al gatekeeper recidivo di effettuare acquisizioni di altre società attive nel settore digitale per un determinato periodo. Quest’ultima sanzione mira a evitare che un gatekeeper che sistematicamente aggira le regole possa ulteriormente espandere il suo potere attraverso e acquisizione (il riferimento implicito è alle cosiddette “*killer acquisitions*”). Si noti che queste misure eccezionali saranno considerate solo in ultima istanza, qualora le normali sanzioni pecuniarie non abbiano sortito effetto deterrente.

Nel momento in cui si scrive risultano pendenti sei procedure di non conformità avviate dalla Commissione europea nei confronti di tre gatekeeper. Per quanto riguarda Alphabet/Google, le contestazioni riguardano l’uso delle interfacce per l’ottenimento del consenso al trattamento dei dati a fini pubblicitari, la pratica di *self-preferencing* in Google Search e le pratiche di *steering* su Google Play⁵⁴. Nei confronti di Apple, le indagini si stanno concentrando sullo *steering* nell’App Store, sulle impostazioni predefinite del browser (Safari) e sulle restrizioni all’uso di app store alternativi nel sistema operativo iOS⁵⁵. A Meta viene, invece, contestato il cosiddetto modello “*pay or consent*”, che obbliga gli utenti a scegliere tra pagare o acconsentire al trattamento dei dati per continuare a usare i servizi gratuitamente⁵⁶.

Da questi casi emergono due tendenze significative. Da un lato, la Commissione sembra orientata a seguire percorsi interpretativi già consolidati del diritto della concorrenza dell’UE (vedi paragrafo 3): essa applica principi sviluppati nella prassi preesistente, come quella sul divieto di abuso di posizione dominante (art. 102 TFUE), combinandoli con le nuove norme *ex ante* del DMA, al fine di garantire un’applicazione più rapida ed efficace⁵⁷.

⁵⁴ Commissione europea, “Commission opens non-compliance investigations against Alphabet, Apple and Meta under Digital Markets Act”, 25 marzo 2024, disponibile su: https://digital-markets-act.ec.europa.eu/commission-opens-non-compliance-investigations-against-alphabet-apple-and-meta-under-digital-markets-2024-03-25_en.

⁵⁵ *Ibid.*

⁵⁶ *Ibid.* Su questo punto si ricorda anche la decisione del Comitato europeo per la protezione dei dati (EDPB), che il 27 ottobre 2023 ha adottato una posizione vincolante ai sensi dell’art. 65 GDPR, confermando la valutazione negativa delle autorità nazionali (in particolare l’autorità norvegese) sul modello “pay or consent” proposto da Meta. Il Comitato ha chiarito che il consenso prestato in un simile contesto non può considerarsi libero ai sensi dell’art. 6 e 7 GDPR, e che il ricorso ad un modello a pagamento come unica alternativa non soddisfa i requisiti di necessità e proporzionalità. Cfr. EDPB, «Binding Decision 2/2023 on the dispute arisen on the draft decision of the Norwegian Data Protection Authority regarding Meta Platforms Ireland Limited», disponibile su: https://edpb.europa.eu/our-work-tools/binding-decisions_en.

⁵⁷ Cfr. la vicenda Google Shopping, in cui la Commissione aveva sanzionato pratiche di auto-preferenza ai sensi dell’art. 102 TFUE, v. Commissione europea, Decisione C(2017) 4444 final, caso AT.39740 – Google Search (Shopping).

Dall'altro lato, risulta evidente l'influenza esercitata dal GDPR e dagli sviluppi giurisprudenziali in materia di consenso dell'interessato, in particolare alla luce della sentenza della Corte di giustizia nel caso *Meta Platforms Inc. v Bundeskartellamt* (causa C-252/21). La decisione del 4 luglio 2023 aveva stabilito che un'autorità antitrust nazionale può considerare il trattamento dei dati personali imposto nei termini generali d'uso di un social network come abuso di posizione dominante, anche alla luce del GDPR, qualora il consenso non sia libero, informato e specifico, e non vi siano basi giuridiche alternative. Inoltre, la Corte aveva precisato che, qualora l'utente rifiuti il consenso a trattamenti non necessari, l'impresa dominante deve offrire un'alternativa equivalente, eventualmente a pagamento, per evitare che l'accesso al servizio sia vincolato a un consenso non valido⁵⁸.

L'entrata in vigore del DMA ha segnato un punto di svolta rilevante: esso rappresenta il primo regime di regolazione *ex ante* delle *big tech*. Altri paesi stanno procedendo in parallelo (UK, Australia, Cina con approcci differenti). L'Ue mira a fare da apripista auspicando che principi simili vengano adottati altrove per evitare frizioni e distorsioni su scala globale⁵⁹.

Nei prossimi anni, l'efficacia del Digital Markets Act dipenderà sia dalla reazione dei gatekeeper, che potrebbero tentare di aggirare le regole o, al contrario, adattare i modelli di business in modo costruttivo, sia dal livello di cooperazione internazionale nel far rispettare standard analoghi ovunque operino queste piattaforme globali. In ogni caso, adesso l'Unione europea dispone di una nuova "cassetta degli attrezzi" per promuovere l'equità e la contendibilità nei mercati digitali, affiancando agli strumenti antitrust tradizionali nuove regole rivolte ai gatekeeper: un cambiamento di paradigma volto a preservare un ecosistema digitale più aperto, competitivo e innovativo.

⁵⁸ Corte di giustizia dell'Unione europea, causa C-252/21, *Meta Platforms Inc. v Bundeskartellamt*, sentenza del 4 luglio 2023.

⁵⁹ Si parla del cosiddetto "effetto Bruxelles" (Brussels Effect), espressione coniata da A. BRADFORD, *The Brussels effect: How the European Union rules the world*, Oxford: Oxford University Press, 2020, per descrivere la capacità regolatoria dell'Unione europea di proiettare i propri standard oltre i confini del mercato interno. Data la dimensione e l'attrattiva del mercato unico, le grandi imprese globali tendono ad adeguare i loro comportamenti alle regole UE non solo in Europa ma anche nei mercati extraeuropei, al fine di evitare la frammentazione dei propri modelli di business. In questo senso, il DMA potrebbe avere un impatto extraterritoriale analogo a quello già osservato per il GDPR. Si veda anche H. DREWES, A. KIRK, *Extraterritorial Effects of the Digital Markets Act: The 'elusive long arm' of European digital regulation*, in *World Competition*, 2024 (47), pp. 473-494 che discutono la misura in cui sia legittimo che l'UE imponga la propria visione del funzionamento dei mercati digitali ad altre giurisdizioni.

LA REGOLAZIONE DEGLI INTERMEDIARI DI INTERNET: IL DIGITAL SERVICE ACT

Giuseppe Contissa

SOMMARIO: 1. Intermediari di Internet. 2. Aspetti socio-tecnici. 3. Gli Intermediari di Internet e la legge. 4. La Direttiva sul Commercio Elettronico. 5. Verso una regolamentazione della moderazione dei contenuti. 6. Il Digital Services Act, 6.1. Ambito di applicazione materiale e territoriale. 6.2. Il “nuovo” regime di responsabilità per gli ISP. 6.3. Obblighi di diligenza nella moderazione dei contenuti. 6.4. Obblighi di due diligence relativi all’interfaccia online, alla pubblicità e ai sistemi di raccomandazione. 6.5. VLOP e VLOSE: valutazione dei rischi, audit e accesso ai dati. 6.6. Applicazione e sanzioni.

1. Intermediari di Internet

Internet ha contribuito alla disintermediazione, consentendo interazioni dirette tra individui, entità commerciali ed enti pubblici. Tuttavia, l’intermediazione non è scomparsa. Su Internet sono emersi nuovi intermediari (*Internet service provider* o ISP), la maggior parte dei quali sono attori privati, che hanno assunto un ruolo sempre più importante¹. Essi forniscono e mantengono le infrastrutture che consentono la comunicazione di informazioni e lo svolgimento di attività economiche e di altro tipo su Internet: la disposizione fisica di cavi e computer, la gestione delle trasmissioni sulle linee di connessione, l’archiviazione e l’elaborazione dei dati, i servizi che facilitano la creazione di contenuti e l’accesso agli stessi, ecc.

Gli intermediari di Internet possono essere classificati in diverse categorie a seconda delle loro funzioni:

- fornitori di accesso e servizi di Internet, che offrono accesso cablati e wireless a Internet;
- fornitori di servizi di elaborazione dati e *web hosting*, che offrono nomi di dominio, archiviazione di siti web e servizi cloud;

¹ C. YOO, *The Dynamic Internet: How Technology, Users, and Businesses Are Transforming the Network*, Washington, DC: AEI Press, 2012.

- motori di ricerca, che aiutano gli utenti a trovare informazioni su Internet;
- social network, che facilitano le interazioni sociali e la condivisione di contenuti tra gli utenti;
- piattaforme di e-commerce, che consentono l'acquisto e la vendita online di beni e servizi;
- sistemi di pagamento su Internet, che elaborano i pagamenti online;
- piattaforme di comunicazione, inclusi servizi di posta elettronica, app di messaggistica e strumenti di videoconferenza che facilitano la comunicazione digitale.

L'evoluzione degli intermediari di Internet può essere tracciata attraverso le diverse fasi del Web.

Il Web 1.0, noto anche come “web statico”, rappresenta la fase iniziale di Internet, caratterizzata da pagine web statiche e interazione limitata con gli utenti. Durante questo periodo, gli intermediari di Internet includevano principalmente i fornitori di accesso a Internet e i fornitori di servizi di *hosting*. Il ruolo principale di questi intermediari era quello di fornire accesso alle informazioni e connettività alla rete. I siti web erano per lo più di sola lettura e i contenuti generati dagli utenti erano minimi.

Il ruolo degli intermediari di Internet è cambiato drasticamente con il Web 2.0, spesso definito “web dinamico”. Questa fase ha introdotto contenuti interattivi e generati dagli utenti, piattaforme di social media e strumenti collaborativi. Gli intermediari di Internet si sono evoluti per adattarsi a questi cambiamenti fornendo servizi più avanzati e diversificati. Le caratteristiche chiave del Web 2.0 includevano contenuti dinamici e interattivi, contenuti generati dagli utenti e social media, piattaforme di e-commerce potenziate, lo sviluppo di motori di ricerca e servizi di hosting avanzati e l'ascesa del cloud computing.

Durante il Web 2.0, intermediari come le piattaforme di social media Facebook (ora Meta) e Twitter (ora X), i giganti dell'e-commerce come Amazon ed eBay e i motori di ricerca generalisti come Google sono diventati parte integrante dell'esperienza Internet. Queste piattaforme hanno permesso agli utenti di interagire, creare contenuti e partecipare al commercio online, ampliando così in modo significativo il ruolo e la complessità degli intermediari Internet.

2. Aspetti socio-tecnici

La diffusione dell'intermediazione Internet è stata resa possibile in gran parte grazie ai sistemi automatizzati di elaborazione dei dati. In questo contesto, nell'ultimo decennio si sono verificati progressi significativi. Gli intermediari Internet hanno oggi accesso a grandi quantità di dati relativi agli utenti, comu-

nemente qualificati come Big Data, e possiedono elevate capacità di connettività. Questi dati includono le interazioni degli utenti, le preferenze individuali, i modelli di comportamento e altro ancora, raccolti attraverso vari servizi e piattaforme. La disponibilità di questi enormi set di dati consente agli intermediari di acquisire una conoscenza approfondita del comportamento degli utenti e delle tendenze di mercato, fornendo le basi per analisi avanzate, servizi personalizzati, e per l'anticipazione degli sviluppi del mercato.

Sfruttando questi dati, gli intermediari Internet sviluppano sistemi di IA basati su algoritmi di apprendimento automatico. Questi sistemi sono in grado di apprendere dai dati per effettuare classificazioni, previsioni e decisioni. I modelli di apprendimento automatico vengono addestrati sui dati storici per identificare schemi ricorrenti e correlazioni, che possono poi essere applicati a nuovi dati per prevedere risultati futuri o classificare accuratamente le informazioni.

L'IA basata sui dati viene applicata nella fornitura di servizi di intermediazione in diversi settori chiave. Ad esempio, nei motori di ricerca, gli algoritmi di IA analizzano le query degli utenti e le interazioni passate per restituire i risultati di ricerca più pertinenti, migliorando la soddisfazione e il coinvolgimento degli utenti. L'algoritmo PageRank di Google, ad esempio, interpreta i link come "voti di fiducia", dove una pagina riceve più valore se è linkata da altre pagine autorevoli, mentre il sistema RankBrain impiega tecniche di apprendimento automatico per interpretare meglio le *query* di ricerca comprendendone il contesto e l'intento. Questi sistemi consentono un recupero efficiente e accurato delle informazioni, oltre che esperienze di ricerca personalizzate.

Anche la pubblicità online trae vantaggio dall'IA, che tramite l'analisi dei dati degli utenti permette di fornire annunci personalizzati, aumentando la pertinenza e l'efficacia delle strategie di marketing. In particolare, la pubblicità comportamentale utilizza i dati sugli interessi e le abitudini degli individui per selezionare e visualizzare gli annunci.

Negli ultimi anni è emerso un complesso ecosistema di pubblicità online che coinvolge editori, reti pubblicitarie, piattaforme, data broker, società di analisi dei dati e società di ricerche di mercato. I dati personali vengono ottenuti attraverso le interazioni degli utenti, attività di tracciamento e l'analisi dei dati, e possono essere ulteriormente venduti per un ulteriore utilizzo nella pubblicità. Le società di gestione dei dati creano profili degli utenti, consentendo l'abbinamento degli annunci sulla base delle loro preferenze, desideri ed esigenze individuali.

La pubblicità online si basa sul *real-time bidding* (RTB). In questo meccanismo, gli spazi pubblicitari vengono acquistati e venduti in tempo reale attraver-

so aste automatizzate e poi visualizzati istantaneamente sui siti web degli editori. Anche le piattaforme di social media, come Facebook, Instagram e TikTok, sono diventate attori significativi nell'ecosistema pubblicitario, poiché utilizzano l'ampia disponibilità di dati raccolti dagli utenti per offrire opzioni pubblicitarie altamente mirate (il cosiddetto "pubblico personalizzato").

Un altro ambito di applicazione dell'intelligenza artificiale nei servizi di intermediazione è rappresentato dai sistemi di raccomandazione, utilizzati da piattaforme come Amazon e YouTube per agevolare gli utenti alla scoperta di prodotti, servizi e contenuti digitali in base alle loro preferenze. A differenza dei motori di ricerca, le preferenze non vengono segnalate dagli utenti attraverso le query, ma vengono previste sulla base del comportamento passato e dei dati di utenti simili.

Tra le principali tecniche in quest'ambito figurano il filtraggio basato sui contenuti ed il filtraggio collaborativo. Nel primo, il sistema raccomanda articoli simili a quelli che un utente ha apprezzato in passato sulla base delle caratteristiche dei contenuti. Ad esempio, il sistema raccomanda altri film d'azione se un utente ama i film d'azione. Nel secondo, il sistema si basa sulle interazioni degli utenti con gli articoli, come le valutazioni o gli acquisti, per trovare somiglianze tra utenti o articoli. Ad esempio, se gli utenti A e B hanno gusti simili, il sistema consiglierà all'utente A ciò che piace all'utente B e viceversa.

I sistemi di raccomandazione possono inoltre utilizzare l'apprendimento rinforzato per ottimizzare determinati obiettivi, come il coinvolgimento degli utenti: un sistema di raccomandazione potrebbe ricevere una ricompensa quando un utente clicca su un articolo raccomandato o effettua un acquisto. Nel tempo, il sistema impara a massimizzare queste ricompense fornendo raccomandazioni migliori.

Infine, la moderazione dei contenuti utilizza l'IA per rilevare e filtrare automaticamente i contenuti dannosi o inappropriati, garantendo un ambiente online più sicuro e produttivo. Questi sofisticati sistemi analizzano grandi quantità di dati, inclusi testi, immagini e video, per identificare e rispondere ai contenuti che violano le linee guida della comunità o gli standard legali. Utilizzano algoritmi avanzati di apprendimento automatico e tecniche di elaborazione del linguaggio naturale per discernere con precisione il contesto e l'intento, consentendo il rilevamento di forme sottili di comportamento dannoso come incitamento all'odio, molestie e disinformazione. In questo modo, la moderazione dei contenuti basata sull'IA raggiunge un equilibrio tra la salvaguardia della libertà di espressione e la protezione degli utenti da materiali dannosi. Inoltre, questi sistemi vengono continuamente aggiornati e perfezionati per

adattarsi all'evoluzione dei contenuti inappropriati, mantenendo così la loro efficacia nel tempo.

Tuttavia, permangono alcune sfide, come garantire l'accuratezza e l'equità, poiché i sistemi automatizzati a volte possono interpretare erroneamente il contesto o mostrare pregiudizi, rendendo necessaria una supervisione e un intervento umano continui per ottenere i migliori risultati.

Questi aspetti socio-tecnici sottolineano il ruolo fondamentale che gli intermediari Internet svolgono nel plasmare l'economia digitale e l'esperienza degli utenti.

3. Gli Intermediari di Internet e la legge

Gli intermediari di Internet sono ampiamente considerati fondamentali per facilitare lo scambio di informazioni e servizi online. Ciò ha portato a una posizione piuttosto favorevole nei confronti delle loro operazioni, consentendo a questi intermediari di prosperare con un'interferenza minima dal legislatore.

L'eccezione principale a tale impostazione ha riguardato la questione della responsabilità per quanto riguarda i contenuti memorizzati o trasmessi via Internet. Più specificamente, se e quando gli intermediari di Internet possano essere ritenuti responsabili per attività illegali svolte dagli utenti dei loro servizi. Ci riferiamo generalmente al termine "responsabilità indiretta" o "responsabilità secondaria", utilizzato rispettivamente nel diritto civile e nel *common law*, che copre generalmente le responsabilità dal comportamento illegale di terzi, come la responsabilità vicaria dei datori di lavoro. In questi casi, l'intermediario non avvia l'attività illecita che determina la sanzione. Piuttosto, fornisce il contesto o l'infrastruttura che consente e facilita il comportamento illegale dell'utente o ne amplifica gli effetti. Senza la piattaforma che ospita le informazioni e ne consente la trasmissione, la comunicazione illecita non potrebbe avvenire; senza il motore di ricerca, la comunicazione illegale non avrebbe raggiunto molte persone, ecc.

Per affrontare questo problema, diversi ordinamenti giuridici hanno progressivamente adottato leggi che regolano la responsabilità dei fornitori di servizi di intermediazione. I due esempi più importanti sono il *Communications Decency Act* statunitense del 1996 e la Direttiva sul commercio elettronico dell'UE del 2000. Il primo prevede un ampio regime di immunità per gli intermediari online in relazione ai contenuti di terzi, noto come "Sezione 230". Questa disposizione ha avuto un ruolo fondamentale per consentire alle piattaforme di Internet di ospitare contenuti generati dagli utenti senza essere ritenute responsabili per la maggior parte dei tipi di contenuti illegali pubblicati dagli utenti. La Direttiva sul commercio elettronico, invece, ha introdotto un regime di re-

sponsabilità condizionata, che protegge gli intermediari dall'essere ritenuti responsabili per i contenuti di terzi, a condizione che rispettino determinati obblighi, come la rimozione tempestiva dei contenuti illegali una volta segnalati.

Negli ultimi anni, il sistema giuridico ha assunto una posizione meno liberale nei confronti degli intermediari di Internet a causa di una serie di questioni emergenti. I principali intermediari online, come Google e Facebook, non sono più piccole start-up, ma attori dominanti del mercato con un notevole potere economico e con impatti significativi sui valori promossi e protetti dal sistema giuridico.

L'impatto di questi intermediari sulla privacy e sulla protezione dei dati è profondo. Tali aziende raccolgono e trattano grandi quantità di dati personali, spesso senza che gli utenti siano consapevoli dell'entità di tali pratiche². Questa vasta raccolta di dati solleva notevoli preoccupazioni in merito alla sorveglianza da parte delle aziende e dei governi³. Il potenziale abuso dei dati personali, sia per scopi commerciali che per facilitare il monitoraggio da parte degli Stati, rappresenta una grave minaccia per i diritti alla privacy individuali e collettivi. Il recente rafforzamento delle normative sulla protezione dei dati, come il Regolamento generale sulla protezione dei dati (GDPR) nell'Unione Europea, riflette l'urgente necessità di proteggere le informazioni personali nell'era digitale.

L'impatto sull'accesso alle opportunità per le imprese, i consumatori e i cittadini è significativo, portando spesso a problemi di discriminazione⁴. Gli algoritmi utilizzati dagli intermediari possono inavvertitamente riprodurre o amplificare i pregiudizi esistenti, con conseguente disparità di opportunità per i gruppi emarginati. Ad esempio, le pratiche di *targeting* pubblicitario possono escludere determinati gruppi demografici dagli annunci di lavoro o di alloggio, aggravando le disuguaglianze sociali. Inoltre, le piccole imprese possono avere difficoltà a competere con le grandi società, le quali dominano i mercati dell'intermediazione online. Ciò crea condizioni di disparità, in cui l'accesso alle opportunità economiche è ineguale, sollevando preoccupazioni in materia di equità e giustizia sociale.

La scelta degli individui è un altro ambito fortemente influenzato dalla manipolazione e dallo sfruttamento dei consumatori⁵. La pubblicità personalizzata

² FORBRUKERRÅDET, *Out of Control. How consumers are exploited by the online advertising industry*, 2020, <https://storage02.forbrukerradet.no/media/2020/01/2020-01-14-out-of-control-final-version.pdf>.

³ S. ZUBOFF, *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*, Roma: Luiss University press, 2019.

⁴ C. O'NEIL, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*, New York: Crown, 2016.

⁵ R. CALO, *Digital Market Manipulation*, in *Geo. Wash. L. Rev.*, 2014 (82).

e i sistemi di raccomandazione, sebbene possano essere vantaggiosi, possono catturare eccessivamente l'attenzione degli utenti⁶ e limitare la gamma di informazioni e prodotti a cui i consumatori sono esposti. Tale dinamica può portare a un modello di consumo ristretto e omogeneo, riducendo la diversità delle scelte disponibili. Inoltre, facendo leva sui pregiudizi cognitivi e le vulnerabilità emotive⁷, può manipolare il comportamento dei consumatori in modo significativo, portandoli spesso a prendere decisioni che potrebbero non essere nel loro interesse. Ciò solleva rilevanti questioni giuridiche riguardo i limiti entro i quali le aziende dovrebbero essere autorizzate a influenzare le scelte dei consumatori.

Infine, ancora più profondo è stato l'impatto sulle elezioni politiche e sul dibattito civico. Gli intermediari possono contribuire, anche attraverso i loro sistemi di raccomandazione, alla creazione di "bolle di filtro"⁸ in cui gli utenti sono esposti solo a informazioni che rafforzano le loro convinzioni, portando a una maggiore polarizzazione politica. La manipolazione dei dati e la pubblicità politica mirata, come si è visto nello scandalo Cambridge Analytica⁹, hanno dimostrato come queste piattaforme possano essere utilizzate per influenzare il comportamento degli elettori e i risultati elettorali, minando il processo democratico. Ciò rappresenta una minaccia significativa per il dibattito civico, poiché l'integrità delle informazioni e la diversità dei punti di vista sono compromesse, rendendo più difficile per i cittadini partecipare a discussioni informate ed equilibrate. A questo si aggiunge la rapida diffusione di notizie false e incitamenti all'odio su Internet, che contribuisce a distorcere la percezione del pubblico e alimentare le tensioni sociali, minando ulteriormente la qualità dell'impegno democratico e contribuendo a un ambiente politico sempre più polarizzato e ostile.

Questi sviluppi hanno spinto gli ordinamenti giuridici a richiedere una maggiore responsabilità da parte degli intermediari di Internet rispetto alla tutela di una pluralità di valori pubblici e di interessi giuridicamente protetti. Un approccio basato sulla responsabilità non si concentra solo sulla determinazione di chi debba essere ritenuto responsabile quando si verifica un evento ingiusto (*ex post factum*), ma comporta l'adozione di misure proattive prima che si verifi-

⁶ T. WU, *The Attention Merchants: The Epic Scramble to Get Inside Our Heads*, New York: Vintage, 2017.

⁷ A. MCSTAY, *Emotional AI: The Rise of Empathic Media*, Los Angeles: Sage, 2018.

⁸ E. PARISER, *The Filter Bubble: What the Internet Is Hiding from You*, London: Penguin UK, 2011.

⁹ C. WYLIE, *Mind*Chk: Cambridge Analytica and the Plot to Break America*, New York: Random House, 2019.

chi un evento o un'azione (*ex ante factum*)¹⁰. Ciò richiede agli intermediari non solo di reagire ai problemi man mano che si presentano, ma anche di attuare sistemi e pratiche che mitigano preventivamente i rischi.

In tale prospettiva, l'UE ha introdotto nuove norme che impongono ai diversi intermediari Internet di astenersi da determinate attività o di adottare misure proattive per prevenire potenziali danni a individui, gruppi e al mercato digitale. Vediamo più nel dettaglio questa evoluzione.

4. La Direttiva sul commercio elettronico

Nel 2000 l'UE ha adottato la Direttiva sul commercio elettronico. La Direttiva è stata proposta alla fine degli anni '90, quando si è riconosciuta la necessità di promuovere la crescita dell'economia digitale in tutta Europa. Istituito un quadro armonizzato per i servizi online, la Direttiva aveva l'obiettivo di incoraggiare l'innovazione, gli investimenti e lo sviluppo del commercio elettronico all'interno del mercato unico. Al centro delle sue disposizioni vi era l'equilibrio tra la certezza giuridica per i fornitori di servizi e la garanzia di un'adeguata protezione per gli utenti di Internet.

Questi obiettivi politici generali hanno anche plasmato il regime di responsabilità previsto dalla Direttiva sul commercio elettronico. Essa ha introdotto un quadro di cosiddetta "immunità condizionata" che dipendeva dal grado di controllo e dalle azioni intraprese dai fornitori di servizi in relazione ai contenuti memorizzati o trasmessi. Questo approccio ha ampiamente mitigato i rischi associati alla fornitura di servizi di Internet, promuovendo così gli investimenti nel settore digitale e consentendo ai fornitori di concentrarsi sul miglioramento dei propri servizi senza il timore immediato di essere ritenuti responsabili delle azioni illegali degli utenti.

In particolare, la Direttiva stabiliva norme di esenzione che prendevano in considerazione tre tipi di fornitori di servizi intermediari:

- *mere conduit* (semplice trasporto), ovvero la trasmissione in una rete di comunicazione di informazioni fornite da un destinatario del servizio o la fornitura di accesso a una rete di comunicazione. Ad esempio, Fastweb, una società di telecomunicazioni italiana, fornisce servizi di comunicazione di rete che consentono di inviare e-mail, navigare su siti web o riprodurre video in streaming;
- *caching*, ovvero la memorizzazione automatica, intermedia e temporanea delle informazioni trasmesse. Si pensi, ad esempio, a un popolare sito web

¹⁰ M.A.P. BOVENS, *The Quest for Responsibility: Accountability and Citizenship in Complex Organisations*, Cambridge: Cambridge University Press, 1998.

di notizie che fornisce articoli e contenuti multimediali a utenti di tutto il mondo. Ogni volta che un utente richiede di visualizzare un articolo, il server del sito web recupera il contenuto dal proprio database e lo invia al dispositivo dell'utente. Senza il caching, questo processo richiederebbe al server di recuperare l'articolo dal database per ogni nuova richiesta, il che può richiedere molto tempo, soprattutto nei periodi di traffico intenso;

- *hosting*, ovvero la memorizzazione di informazioni da parte di terzi. È il caso, ad esempio, delle società che forniscono l'infrastruttura per la creazione di siti web (ma non il contenuto dei siti web, che è fornito dagli utenti) o dei servizi di piattaforma come YouTube (YouTube fornisce l'infrastruttura per caricare e visualizzare i video, ma non i video stessi, che sono forniti dagli utenti).

Le condizioni specifiche per l'esenzione dalla responsabilità erano contenute negli articoli da 12 a 14. Le limitazioni di responsabilità erano formulate in modo orizzontale, ovvero coprivano la responsabilità civile, amministrativa e penale per tutti i tipi di attività illegali avviate da terzi online (compresi i diritti d'autore e i marchi, la diffamazione, la pubblicità ingannevole, le pratiche commerciali sleali, ecc).

I semplici fornitori di servizi di *mere conduit* (articolo 12) non erano considerati responsabili delle informazioni trasmesse attraverso il loro servizio, purché non avessero avviato la trasmissione, selezionato il destinatario della trasmissione o modificato le informazioni contenute nella trasmissione.

Inoltre, i fornitori di servizi di *caching* (articolo 13) non erano responsabili per la memorizzazione automatica, intermedia e temporanea delle informazioni trasmesse, a condizione che soddisfacessero determinate condizioni: non modificare le informazioni, rispettare le condizioni di accesso, conformarsi alle norme del settore per l'aggiornamento delle informazioni, non interferire con la tecnologia utilizzata per la raccolta dei dati e rimuovere o disabilitare tempestivamente l'accesso alle informazioni memorizzate previa notifica della loro rimozione dalla rete o a seguito di un ordine da un autorità giudiziaria/amministrativa.

Infine, il fornitore di *hosting* (articolo 14) non poteva essere ritenuto responsabile per la memorizzazione delle informazioni fornite da un destinatario del servizio a condizione che (a) il fornitore non fosse effettivamente a conoscenza di attività o contenuti illegali o, (b) una volta venuto a conoscenza di tali attività o contenuti, avesse provveduto a rimuovere o disabilitare rapidamente l'accesso a tali informazioni. Tale esenzione non si applicava se il destinatario del servizio agiva sotto l'autorità o il controllo del fornitore.

Le norme sulle esenzioni di responsabilità erano accompagnate da una norma generale diretta agli Stati membri affinché non imponessero ai fornitori, nella prestazione dei servizi di cui agli articoli 12, 13 e 14, l'obbligo generale di sorvegliare le informazioni che trasmettono o memorizzano, né l'obbligo generale di ricercare attivamente fatti o circostanze che indicassero attività illecite (articolo 15, paragrafo 1). Tuttavia, gli Stati membri potevano imporre ai fornitori di servizi della società dell'informazione l'obbligo di informare tempestivamente le autorità pubbliche competenti di presunte attività illegali o di fornire informazioni che consentissero l'identificazione dei destinatari dei loro servizi su richiesta delle autorità (articolo 15, paragrafo 2).

5. Verso una regolamentazione della moderazione dei contenuti

L'approccio dell'immunità condizionata alla responsabilità degli ISP ha presto iniziato a essere oggetto di critiche. Sono state messe in discussione le premesse stesse di questo approccio¹¹. È ancora vero che le società Internet non dispongono delle risorse finanziarie necessarie per risarcire i danni causati alle parti lese dalle attività degli utenti rese possibili da tali società? Perché non dovrebbero essere chiamate a pagare per le esternalità negative del loro modello di business? Date le loro capacità finanziarie e tecnologiche, possono ancora affermare di non essere in grado di esercitare un controllo efficace sui contenuti e sulle attività online? Lo sviluppo tecnologico, in particolare nel campo dell'intelligenza artificiale, può consentire controlli efficienti ed economici?

Questo cambiamento di prospettiva ha portato a una crescente richiesta agli ISP di assumersi una responsabilità più proattiva nel garantire che i contenuti e le attività forniti attraverso i loro servizi di intermediazione non portino a risultati dannosi. Pertanto, i quadri giuridici hanno iniziato ad evolversi per affrontare la maggiore capacità degli intermediari di moderare i contenuti.

Ad esempio, la legge tedesca sull'applicazione dei social network (*NetzDG*)¹² ha imposto alle piattaforme di social media di rimuovere i contenuti illegali entro 24 ore dalla notifica, pena l'applicazione di sanzioni pecuniarie sostanziali. Questa legge mira a garantire che le piattaforme agiscano rapidamente contro l'incitamento all'odio e altri contenuti illegali.

Inoltre, alcuni atti giuridici dell'UE hanno imposto agli intermediari obblighi di gestione proattiva dei contenuti. Ad esempio, la Direttiva del 2011 sugli

¹¹ M.R. TADDEO, L. FLORIDI (eds.), *The Responsibilities of Online Service Providers*, Cham: Springer, 2017.

¹² *Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken* del 1° settembre 2017, (BGBl. I S. 3352).

abusi sui minori¹³ introduce l'obbligo di rimuovere e bloccare l'accesso ai siti web che contengono o diffondono abusi sessuali su minori e pornografia infantile. Analogamente, la Direttiva del 2017 sul terrorismo¹⁴ prevede obblighi simili contro l'incitamento pubblico online ad atti di terrorismo. Questi sviluppi giuridici riflettono una tendenza più ampia verso il rafforzamento del ruolo delle piattaforme online nella prevenzione dei danni e nella tutela della sicurezza pubblica, richiedendo loro un coinvolgimento più attivo nel monitoraggio e nel controllo dei contenuti generati dagli utenti.

Gli strumenti legislativi più recenti sono passati dal considerare la moderazione come un'attività facoltativa a renderla una responsabilità obbligatoria per le piattaforme online in determinati contesti.

Ad esempio, la Direttiva sui servizi di media audiovisivi¹⁵ impone ai fornitori di contenuti di adottare misure per proteggere i minori e il pubblico in generale da contenuti dannosi, compresi quelli che promuovono il terrorismo, la pornografia infantile, il razzismo e la xenofobia. La direttiva impone alle piattaforme di introdurre sistemi efficaci per individuare e rimuovere tempestivamente tali contenuti.

Allo stesso modo, la Direttiva sul diritto d'autore del 2019¹⁶ impone obblighi specifici ai fornitori di servizi di condivisione di contenuti per garantire che i contenuti protetti da copyright non autorizzati non siano disponibili sulle loro piattaforme. I fornitori devono inoltre agire rapidamente per rimuovere le opere segnalate come contraffatte. La conformità a queste direttive richiede spesso l'uso di strumenti automatizzati avanzati e filtri sul caricamento, aumentando il livello delle pratiche di moderazione dei contenuti in tutto il settore.

Obbligare le piattaforme a impegnarsi in una moderazione attiva introduce diverse sfide complesse¹⁷.

¹³ Direttiva (UE) 2011/93/UE del Parlamento europeo e del Consiglio, del 13 dicembre 2011, relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile, e che sostituisce la decisione quadro 2004/68/GAI del Consiglio.

¹⁴ Direttiva (UE) 2017/541 del Parlamento europeo e del Consiglio, del 15 marzo 2017, sulla lotta contro il terrorismo e che sostituisce la decisione quadro 2002/475/GAI del Consiglio e modifica la decisione 2005/671/GAI del Consiglio.

¹⁵ Direttiva (UE) 2018/1808 del Parlamento europeo e del Consiglio, del 14 novembre 2018, recante modifica della direttiva 2010/13/UE relativa al coordinamento di determinate disposizioni legislative, regolamentari e amministrative degli Stati membri concernenti la fornitura di servizi di media audiovisivi (direttiva sui servizi di media audiovisivi), in considerazione dell'evoluzione delle realtà del mercato.

¹⁶ Direttiva (UE) 2019/790 del Parlamento europeo e del Consiglio, del 17 aprile 2019, sul diritto d'autore e sui diritti connessi nel mercato unico digitale e che modifica le direttive 96/9/CE e 2001/29/CE.

¹⁷ G. SARTOR, A. LOREGGIA, *L'impatto degli algoritmi per il filtraggio o la moderazione dei contenuti online*, Sintesi. Studio per la commissione JURI, Parlamento Europeo, 2020.

Le aziende più piccole, in particolare, potrebbero avere difficoltà a sostenere gli oneri finanziari e tecnologici necessari per conformarsi a queste direttive. I sistemi di filtraggio efficaci, sebbene necessari, possono portare a un blocco eccessivo, in cui contenuti legali e utili vengono inavvertitamente rimossi, compromettendo così la libertà di espressione. È fondamentale trovare un equilibrio tra la prevenzione dei danni e la protezione delle libertà civili, poiché gli sforzi di moderazione comportano una raccolta e una sorveglianza estese dei dati, che possono violare i diritti alla privacy. La sfida consiste nell'attuare misure che riducano al minimo i danni, garantendo al contempo che le piattaforme non limitino eccessivamente la comunicazione lecita. Ciò richiede un approccio attento e sfumato alla regolamentazione, che tenga conto dei diversi interessi delle parti coinvolte, inclusi gli utenti, gli operatori delle piattaforme e la società in generale.

6. Il Digital Services Act

Nel dicembre 2020, la Commissione europea ha pubblicato una proposta di legge sui servizi digitali. Il Regolamento UE 2022/2065¹⁸ è stato adottato nel novembre 2022 ed è entrato in vigore gradualmente, con piena applicazione a partire da febbraio 2024.

Il DSA modifica e sostituisce gli articoli 12-15 della Direttiva sul commercio elettronico relativi alla responsabilità degli ISP e introduce un nuovo quadro di obblighi stratificati rivolti a diversi tipi di prestatori di servizi di intermediazione online di diverse dimensioni.

6.1. *Ambito di applicazione materiale e territoriale*

Le norme del DSA si applicano a diverse categorie di servizi di intermediazione online in base al loro ruolo, alle loro dimensioni e al loro impatto nell'ecosistema online:

- servizi di intermediazione, che coprono le tre categorie originariamente incluse nella Direttiva sul commercio elettronico, ovvero “servizi di semplice trasporto”, “servizi di acquisizione” e “servizi di *hosting*”;

¹⁸ Regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio, del 19 ottobre 2022, relativo al mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali), GU L 277 del 27.10.2022.

- piattaforme online, definite come servizi di *hosting* che non solo memorizzano informazioni su richiesta del destinatario, ma le diffondono anche al pubblico¹⁹.
- piattaforme online di dimensioni molto grandi (VLOP) e motori di ricerca online di dimensioni molto grandi (VLOSE), che raggiungono almeno 45 milioni di destinatari attivi nell'UE su base mensile (10 % della popolazione dell'UE) e sono designati come tali dalla Commissione europea secondo la procedura di cui all'articolo 33²⁰.

Per quanto riguarda l'ambito di applicazione territoriale, tutti i servizi di intermediazione online offerti a destinatari il cui luogo di stabilimento si trova nell'Unione o che sono ubicati nell'Unione dovrebbero conformarsi alle nuove norme, compresi quelli stabiliti al di fuori dell'UE (articolo 2). Questo ampio ambito di applicazione territoriale del DSA è in linea con l'approccio adottato in altri regolamenti (ad esempio il GDPR), in cui il criterio principale è la misura in cui l'attività regolamentata riguarda le persone residenti nell'UE e non lo stabilimento del fornitore.

6.2. Il “nuovo” regime di responsabilità per gli ISP

Il DSA modifica gli articoli 12-15 della Direttiva sul commercio europeo relativi al regime di responsabilità degli ISP. Tuttavia, il DSA non ha modificato in modo significativo l'approccio esistente. Al contrario, ha preservato le norme di base in materia di responsabilità contenute nella Direttiva.

Questa scelta ha un significato politico: la conferma delle esenzioni di responsabilità da parte del DSA significa che esse ricevono un rinnovato sostegno attraverso il processo democratico come norme che hanno superato la prova del tempo e rimangono adeguate allo scopo.

Il DSA continua a individuare le tre attività tecniche più comuni per le esenzioni di responsabilità, vale a dire i fornitori di servizi di semplice trasporto (articolo 4), di memorizzazione temporanea (*caching*) (articolo 5) e di memorizzazione di informazioni (*hosting*) (articolo 6).

¹⁹ Articolo 3, lettera i). La definizione esclude il caso in cui la diffusione «è solo una caratteristica minore o meramente accessoria connessa intrinsecamente a un altro servizio o una funzionalità minore del servizio principale».

²⁰ A gennaio 2026, questi sono i servizi designati come VLOP: AliExpress, Amazon Store, Apple, Booking.com, Google (comprende Maps, Play, Shopping), LinkedIn, Meta (comprende Facebook e Instagram), Pinterest, Pornhub, Shein, Snapchat, Temu, TikTok, Wikipedia, X, XXXX, XVideos, YouTube, Zalando. I VLOSE designati sono Google Search e Bing di Microsoft.

È stato inoltre mantenuto il divieto per gli Stati membri di imporre agli ISP che trasmettono o memorizzano dati di accertare attivamente fatti o circostanze che indichino attività illegali (articolo 8).

L'unico aggiornamento degno di nota è stata l'introduzione della cosiddetta "clausola del buon samaritano". Questa clausola era stata introdotta per la prima volta nel *Communications Decency Act* degli Stati Uniti come modo per proteggere dalla responsabilità gli ISP che, in buona fede, agiscono per limitare l'accesso a materiale discutibile. Questa disposizione, non prevista nella Direttiva sul commercio elettronico, è stata introdotta nell'articolo 7 del DSA. Di conseguenza, «i prestatori di servizi intermediari non sono considerati inammissibili all'esenzione dalla responsabilità prevista agli articoli 4, 5 e 6 per il solo fatto di svolgere, in buona fede e in modo diligente, indagini volontarie di propria iniziativa o di adottare altre misure volte a individuare, identificare e rimuovere contenuti illegali o a disabilitare l'accesso agli stessi, o di adottare le misure necessarie per conformarsi alle prescrizioni del diritto dell'Unione e del diritto nazionale conforme al diritto dell'Unione, comprese le prescrizioni stabilite nel presente regolamento»²¹.

Questa disposizione è molto significativa in quanto fornisce un incentivo al rispetto degli obblighi di diligenza per un ambiente trasparente e sicuro nei successivi articoli del DSA, compresa la moderazione dei contenuti. Se gli ISP applicano diligentemente le procedure di moderazione dei contenuti, in conformità con le disposizioni del DSA, non saranno soggetti a responsabilità per la gestione attiva dei contenuti generati dagli utenti. Al contrario, se gli ISP non rispettano gli obblighi di diligenza nell'ambito della moderazione dei contenuti, potrebbero perdere il diritto all'immunità ed essere ritenuti responsabili.

6.3. Obblighi di diligenza nella moderazione dei contenuti

La caratteristica distintiva del DSA, rispetto alla Direttiva sul commercio elettronico, è l'attenzione alla moderazione dei contenuti e l'istituzione di obblighi di diligenza adeguati al tipo e alle dimensioni degli ISP.

La moderazione dei contenuti è definita come: «le attività, automatizzate o meno, svolte dai prestatori di servizi intermediari con il fine, in particolare, di individuare, identificare e contrastare contenuti illegali e informazioni incompatibili con le condizioni generali, forniti dai destinatari del servizio, comprese le misure adottate che incidono sulla disponibilità, sulla visibilità e sull'accessibilità di tali contenuti illegali o informazioni, quali la loro retrocessione, demonetizzazione o rimozione o la disabilitazione dell'accesso agli stessi, o che

²¹ Articolo 7 del DSA.

incidono sulla capacità dei destinatari del servizio di fornire tali informazioni, quali la cessazione o la sospensione dell'account di un destinatario del servizio»²².

Va notato che la moderazione dei contenuti non si limita ai contenuti illegali²³, ma anche alle «informazioni incompatibili con le condizioni generali». Ciò si riferisce alla possibilità di moderare i contenuti sulla base delle linee guida che delineano i comportamenti e gli usi accettabili all'interno del servizio, inclusi, ma non limitati a, contenuti che possono essere dannosi, fuorvianti o comunque contrari alle politiche del fornitore di servizi.

Il DSA introduce diversi obblighi di *due diligence* in materia di moderazione dei contenuti, differenziati in base al tipo di ISP.

Tutti gli ISP (semplice trasporto, *caching*, *hosting*) devono:

- designare un unico punto di contatto per facilitare la comunicazione diretta con le Autorità degli Stati membri, la Commissione e il Comitato europeo per i servizi digitali. Le informazioni di contatto devono essere pubbliche, facilmente accessibili e aggiornate (articolo 11);
- designare un unico punto di contatto per i destinatari del servizio, consentendo loro di comunicare direttamente e rapidamente, anche attraverso mezzi non automatizzati. Le informazioni di contatto necessarie devono essere rese pubbliche e mantenute aggiornate (articolo 12);
- designare un rappresentante legale all'interno dell'Unione se non hanno uno stabilimento nell'Unione ma offrono servizi nell'Unione. A tale rappresentante saranno rivolte le richieste relative alla conformità e all'applicazione (articolo 13);
- includere nelle condizioni generali informazioni chiare su eventuali restrizioni imposte all'uso del proprio servizio, comprese le politiche e le procedure di moderazione dei contenuti. Le modifiche significative devono essere comunicate ai destinatari del servizio (articolo 14);
- rendere disponibili relazioni annuali sulla trasparenza, che descrivano in dettaglio le attività di moderazione dei contenuti, compresi il numero di ordini delle autorità degli Stati membri ricevuti e le azioni intraprese in seguito a segnalazioni di contenuti illegali (articolo 15).

Oltre a ciò, i fornitori di servizi di *hosting* devono anche:

²² Articolo 3, lettera f) del DSA.

²³ Il concetto di "contenuto illegale" è definito all'articolo 3, lettera h) come «qualsiasi informazione che, di per sé o in relazione a un'attività, tra cui la vendita di prodotti o la prestazione di servizi, non è conforme al diritto dell'Unione o di qualunque Stato membro conforme con il diritto dell'Unione, indipendentemente dalla natura o dall'oggetto specifico di tale diritto».

- attuare meccanismi che consentano alle persone fisiche o giuridiche di segnalare loro contenuti illegali (il cosiddetto «meccanismo di segnalazione e azione»). Tali meccanismi devono essere di facile utilizzo, esclusivamente elettronici e in grado di trattare segnalazioni sufficientemente precise e motivate (articolo 16);

- fornire ai destinatari interessati una chiara dichiarazione dei motivi (SoR – “*Statement of Reasons*”) di qualsiasi restrizione imposta alle loro informazioni, specificando i fatti e le circostanze alla base della decisione e fornendo informazioni sulle possibilità di ricorso (articolo 17)²⁴;

- notificare alle autorità di polizia o giudiziarie qualsiasi informazione che fa sospettare che sia stato commesso, si stia commettendo o probabilmente sarà commesso reato che comporti una minaccia alla vita o alla sicurezza (articolo 18).

Infine, se i fornitori di servizi di *hosting* sono qualificabili come piattaforme online, ovvero se diffondono anche informazioni generate dagli utenti, devono, oltre a quanto previsto per i servizi di *hosting*:

- offrire un sistema interno di gestione dei reclami, che consenta ai destinatari di presentare reclami per via elettronica e gratuitamente in merito alle decisioni prese in relazione a contenuti illegali o violazioni dei termini e delle condizioni (articolo 20);

- facilitare la risoluzione extragiudiziale delle controversie per i destinatari, garantendo l'accesso a organismi certificati di risoluzione extragiudiziale delle controversie e rispettando le decisioni prese da tali organismi (articolo 21);

- dare priorità e trattare senza indebito ritardo le segnalazioni provenienti dai cosiddetti “segnalatori attendibili” (articolo 22). I segnalatori attendibili sono destinatari del servizio che segnalano attivamente contenuti illeciti e sono riconosciuti come tali da una decisione del coordinatore dei servizi digitali sulla base di criteri specifici²⁵;

- sospendere i servizi ai destinatari che forniscono frequentemente contenuti manifestamente illegali o presentano segnalazioni o reclami manifestamente infondati. I fornitori devono delineare la loro politica in materia di abuso nelle loro condizioni generali (articolo 23);

²⁴ A questo proposito, la Commissione europea ha lanciato la «banca dati sulla trasparenza del DSA» (<https://transparency.dsa.ec.europa.eu>), che consente di seguire quasi in tempo reale le decisioni di moderazione dei contenuti prese dai fornitori di piattaforme online.

²⁵ I criteri per l'assegnazione dello status di “segnalatori attendibili” sono: (a) dispone di capacità e competenze particolari ai fini dell'individuazione, dell'identificazione e della notifica di contenuti illegali; (b) indipendenza da qualsiasi fornitore di piattaforme online; (c) scopo di presentare segnalazioni in modo diligente, accurato e obiettivo.

- includere informazioni aggiuntive nelle loro relazioni sulla trasparenza, come il numero di controversie sottoposte a organismi di risoluzione extragiudiziale delle controversie e i relativi esiti (articolo 24).

Le microimprese e le piccole imprese che offrono servizi di piattaforma online sono generalmente escluse dagli obblighi aggiuntivi, a meno che non siano qualificate come piattaforme online di grandi dimensioni (articolo 19).

6.4. Obblighi di due diligence relativi all'interfaccia online, alla pubblicità e ai sistemi di raccomandazione

Oltre alla moderazione dei contenuti, il DSA stabilisce ulteriori obblighi di diligenza per le piattaforme online per quanto riguarda le modalità di progettazione dell'interfaccia online, la pubblicità e i sistemi di raccomandazione.

Alle piattaforme online è vietato progettare, organizzare e gestire le loro interfacce online in modo tale da ingannare o manipolare i destinatari dei loro servizi o da materialmente falsare o compromettere altrimenti la capacità dei destinatari dei loro servizi di prendere decisioni libere e informate (articolo 25). La Commissione europea può emanare linee guida su come ciò si applica a pratiche specifiche, come dare maggiore risalto a determinate scelte, richiedere ripetutamente decisioni già prese o rendere la cessazione del servizio più difficile rispetto alla sottoscrizione dello stesso.

I fornitori di piattaforme online che presentano pubblicità devono garantire che i destinatari possano chiaramente identificare, in tempo reale, che si tratta di pubblicità (articolo 26). Le informazioni dovrebbero includere anche la persona per conto della quale viene presentato l'annuncio pubblicitario, la persona che ha pagato per l'annuncio pubblicitario, se diversa, e informazioni significative sui parametri utilizzati per determinare il destinatario dell'annuncio pubblicitario. Inoltre, quando la pubblicità online viene visualizzata su VLOP e VLOSE, i fornitori di tali piattaforme devono compilare e rendere pubblico un archivio contenente informazioni dettagliate sugli annunci pubblicitari presentati sulle loro piattaforme (articolo 39)²⁶.

²⁶ Nella prima decisione relativa al DSA, la Corte di giustizia europea ha respinto la richiesta di Amazon di sospendere l'applicazione dell'articolo 39, che impone la pubblicazione di informazioni sui servizi pubblicitari (Amazon Services contro Commissione europea, causa C-638/23). Questa decisione sottolinea il sostegno della Corte agli obiettivi di trasparenza del DSA, enfatizzando l'interesse pubblico rispetto alle affermazioni di Amazon relative al danno competitivo derivante dalla divulgazione di informazioni potenzialmente riservate. Sebbene la decisione non sia definitiva e siano possibili future limitazioni alle disposizioni in materia di trasparenza, essa segnala un forte sostegno iniziale al quadro normativo del DSA.

La visualizzazione di pubblicità online è invece vietata quando (1) si basa sulla profilazione²⁷ utilizzando categorie speciali di dati personali (articolo 26, paragrafo 3); (2) quando il fornitore è ragionevolmente certo che il destinatario sia un minore (articolo 28, paragrafo 2).

Infine, il DSA stabilisce alcuni obblighi di diligenza in relazione ai sistemi di raccomandazione. I fornitori devono indicare chiaramente nelle loro condizioni generali i principali parametri utilizzati e le opzioni a disposizione dei destinatari per modificare o influenzare tali parametri (articolo 27). I fornitori, qualora siano disponibili più opzioni di funzionamento dei sistemi di raccomandazione, devono rendere accessibile una funzionalità che consenta agli utenti di selezionare e modificare in qualsiasi momento l'opzione preferita per l'ordinamento dei contenuti. Quando i sistemi di raccomandazione sono utilizzati da VLOP e VLOSE, i fornitori devono inoltre offrire la possibilità di rinunciare alle raccomandazioni basate sulla profilazione (articolo 38).

6.5. VLOP e VLOSE: valutazione dei rischi, audit e accesso ai dati

I fornitori di piattaforme online di dimensioni molto grandi (*Very Large Online Platform* - VLOP) e di motori di ricerca online di dimensioni molto grandi (*Very Large Online Search Engine* - VLOSE) sono soggetti a obblighi aggiuntivi che dovrebbero contribuire a garantire un ambiente online più sicuro e trasparente.

Un obbligo fondamentale riguarda la valutazione dei rischi. I VLOP e i VLOSE devono identificare, analizzare e valutare i rischi sistemici connessi ai loro servizi e adottare misure di mitigazione adeguate ed efficaci. La valutazione e la mitigazione dei rischi devono avvenire entro una data specificata e, successivamente, almeno una volta all'anno, in particolare prima di implementare funzionalità che possono avere un impatto critico.

La valutazione dovrebbe riguardare i cosiddetti “rischi sistemici”, ovvero la diffusione di contenuti illegali, gli effetti negativi sui diritti fondamentali, il dibattito civico, la sicurezza pubblica e le questioni relative alla violenza di genere e alla salute pubblica. La valutazione del rischio sistemico dovrebbe, in particolare, tenere conto di fattori quali la progettazione dei sistemi di raccomandazione, la moderazione dei contenuti, le condizioni generali applicabili, la selezione e presentazione della pubblicità e le pratiche del fornitore relative ai dati.

²⁷ Il riferimento è alla definizione di “profilazione” contenuta nell'articolo 4 del GDPR, ovvero «qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica».

Deve inoltre tenere conto dei rischi sistemici che potrebbero essere influenzati dalla manipolazione intenzionale del loro servizio, compreso l'uso non autentico o lo sfruttamento automatizzato del servizio.

Le possibili misure di mitigazione includono l'adattamento della progettazione del servizio, dei termini e delle condizioni, dei processi di moderazione dei contenuti, dei sistemi algoritmici e dei sistemi pubblicitari. Inoltre, è importante rafforzare i processi interni, cooperare con segnalatori affidabili e altri fornitori, sensibilizzare l'opinione pubblica e proteggere i diritti dei minori.

Inoltre, i VLOP e i VLOSE devono:

- sottoporsi a una revisione (audit) indipendente annuale a proprie spese per garantire il rispetto degli obblighi e degli impegni (articolo 37);
- fornire al Coordinatore dei servizi digitali, cioè l'Autorità nazionale deputata all'applicazione del Regolamento, alla Commissione europea e, in alcuni casi, a ricercatori autorizzati l'accesso ai dati necessari per monitorare e valutare la conformità (articolo 40);
- istituire una funzione di controllo della conformità indipendente con "responsabili della conformità" per monitorare il rispetto del regolamento (articolo 41);
- pubblicare, almeno ogni sei mesi, la relazione che descrive in dettaglio la moderazione dei contenuti (come previsto dall'articolo 15) e una relazione che fornisce informazioni sulle valutazioni dei rischi, sulle misure di mitigazione, sui risultati degli audit e sulle consultazioni (articolo 42).

6.6. Applicazione e sanzioni

Il DSA delinea un sistema di applicazione complesso. Quest'ultimo è condiviso tra le autorità nazionali, incaricate di vigilare sugli ISP e sulle piattaforme online di minori dimensioni, e la Commissione, che ha competenza esclusiva per i VLOP e i VLOSE.

L'autorità nazionale, denominata "Coordinatore dei servizi digitali", è un'autorità indipendente responsabile della supervisione dei servizi di intermediazione stabiliti nel proprio Stato membro e/o del coordinamento con le autorità settoriali specializzate.

Il DSA istituisce inoltre il Comitato europeo per i servizi digitali (EBDS) come gruppo consultivo dei DSC e della Commissione sull'applicazione del regolamento.

In caso di inadempienza, gli Stati membri (o la Commissione, per i VLOP e i VLOSE) possono infliggere sanzioni pecuniarie fino al 6 % del fatturato annuo mondiale dell'intermediario.

Inoltre, gli utenti hanno il diritto di chiedere un risarcimento per i danni o le perdite subiti a causa di violazioni da parte degli intermediari online.

LA TUTELA DEL CONSUMATORE DIGITALE

Federico Galli

SOMMARIO: 1. Dall'e-commerce al commercio digitale. 2. La tutela del consumatore digitale: profili teorici. 3. Le clausole vessatorie e le pratiche commerciali scorrette. 3.1. Le clausole vessatorie. 3.2. Le pratiche commerciali scorrette. 4. La disciplina dei contratti conclusi a distanza. 4.1. La nozione di contratto a distanza. 4.2. Le informazioni precontrattuali. 4.3. Il diritto di recesso. 5. I contratti ad oggetto digitale. 5.1. La disciplina sulla vendita e le garanzie dei beni con elementi digitali. 5.2. La disciplina sui contratti di fornitura di contenuto digitale e di servizi digitali. 6. I contratti conclusi tramite piattaforme online. 7. Le ulteriori norme a tutela degli utenti-consumatori sulle piattaforme online. 7.1. La trasparenza della pubblicità online. 7.2. I sistemi di raccomandazione trasparenti e controllabili. 7.3. I *dark patterns*. 8. Profili applicativi.

1. Dall'e-commerce al commercio digitale

L'evoluzione tecnologica ha trasformato profondamente il commercio elettronico tradizionale. In poco più di vent'anni, dai primi siti di *e-commerce* per la vendita online di beni materiali si è passati a modelli di business nuovi e innovativi – dalle piattaforme di *social network* ai *marketplace* online dove i consumatori possono concludere contratti a distanza con professionisti – che permettono transazioni e scambi informativi in modi del tutto nuovi. Questa trasformazione digitale e il maggiore utilizzo di tali servizi hanno però dato origine a nuovi rischi e sfide per i consumatori, le imprese e la società nel suo complesso.

La normativa ha dovuto tenere il passo di tali cambiamenti. Basti pensare che l'Unione Europea, a oltre vent'anni dalla Direttiva 2000/31/CE sul commercio elettronico¹, ha ritenuto necessario intervenire con nuove regole armonizzate per i servizi digitali e di intermediazione online, come il recente Digital Services Act².

¹ Direttiva 2000/31/CE del Parlamento europeo e del Consiglio dell'8 giugno 2000 relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno (Direttiva sul commercio elettronico). Gazzetta ufficiale n. L 178 del 17/07/2000 pag. 0001 - 0016

² Regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio del 19 ottobre 2022 relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali), GU L 277 del 27.10.2022, pagg. 1-102.

Allo stesso modo, il Codice del consumo italiano (d.lgs. 206/2005) è stato oggetto di continui aggiornamenti per adeguarsi alla costante evoluzione dei mercati digitali e delle piattaforme³.

Negli ultimi anni in particolare sono state recepite importanti direttive europee che innovano la tutela del consumatore digitale: ad esempio, nel 2021 il legislatore italiano ha introdotto i d.lgs. 170/2021 e 173/2021 in attuazione delle Direttive (UE) 2019/771 e 2019/770, riguardanti rispettivamente la vendita di beni (anche con elementi digitali) e la fornitura di contenuti e servizi digitali. Il d.lgs. 7 marzo 2023 n. 26 ha attuato la Direttiva (UE) 2019/2161, cosiddetta Direttiva Omnibus, che ha modernizzato le regole di protezione dei consumatori per adeguarle all'era digitale⁴.

Con questa evoluzione, sia sul piano dello sviluppo tecnologico sia sul fronte dei cambiamenti normativi, si è passati da un focus sull'e-commerce "tradizionale", imperniato sulle vendite online di prodotti tangibili, a un "commercio digitale" che abbraccia aspetti economici e sociali molto più ampi: compravendita di beni materiali tramite piattaforme globali, fornitura di contenuti interamente digitali (file, streaming, cloud), servizi basati sulla monetizzazione dei dati degli utenti e interazioni basate su contenuti mediate da grandi intermediari online. La tutela del consumatore in questo contesto complesso ha richiesto un approccio integrato e aggiornato, che coniughi i principi tradizionali di protezione contrattuale con nuove norme su trasparenza, dati e responsabilità delle piattaforme.

Nel prosieguo, analizzeremo i vari profili di questa tutela, dalle questioni teoriche generali fino alle discipline specifiche (contratti a distanza, clausole abusive, contratti digitali, piattaforme online, ecc.), alla luce della normativa europea e nazionale vigente.

³ Tra le riforme di maggiore rilievo ricordiamo: il d.lgs. 21/2014, che ha recepito la Dir. 2011/83/UE sui diritti dei consumatori; il d.lgs. 130/2015, attuativo della Dir. 2013/11/UE sulla risoluzione alternativa delle controversie dei consumatori (ADR); il d.lgs. 101/2018, volto ad armonizzare la disciplina con il GDPR; il d.lgs. 170/2021, che ha recepito la Dir. (UE) 2019/771 sulla vendita di beni e la Dir. (UE) 2019/770 sui contenuti e servizi digitali; e da ultimo il d.lgs. 26/2023, attuativo della Direttiva (UE) 2019/2161 (Omnibus), che ha inciso in profondità sulla disciplina delle pratiche commerciali scorrette, delle clausole vessatorie e delle sanzioni. Si veda V. CUFFARO, A. BARBA, A. BARENGHI (a cura di), *Codice del consumo e norme collegate*, VI Edizione, Milano: Giuffrè Lefebvre, 2023.

⁴ Decreto Legislativo 7 marzo 2023, n. 26 recante l'attuazione della direttiva (UE) 2019/2161 del Parlamento europeo e del Consiglio, del 27 novembre 2019, che modifica la direttiva 93/13/CEE del Consiglio e le direttive 98/6/CE, 2005/29/CE e 2011/83/UE del Parlamento europeo e del Consiglio per una migliore applicazione e una modernizzazione delle norme dell'Unione relative alla protezione dei consumatori.

2. La tutela del consumatore digitale: profili teorici

La progressiva digitalizzazione dei mercati ha posto questioni teoriche peculiari per la tutela del consumatore e nuove sfide per il legislatore.

Tradizionalmente, il consumatore – ossia la “persona fisica che agisce per scopi estranei all’attività imprenditoriale, commerciale, artigianale o professionale eventualmente svolta”⁵ – è considerato la parte “debole” del rapporto contrattuale, meritevole di una protezione specifica volta a riequilibrare l’asimmetria informativa e di potere contrattuale rispetto al professionista.

Sotto il profilo teorico, dunque, la tutela del consumatore esprime un’applicazione del principio di eguaglianza sostanziale⁶, poiché mira a compensare le disuguaglianze di fatto che caratterizzano il rapporto contrattuale e a garantire che la libertà negoziale del consumatore sia effettiva e non solamente apparente.

Nell’era digitale, sebbene il consumatore digitale abbia accesso a una mole immensa di informazioni e opportunità di scelta online, permangono o si aggravano alcuni squilibri, mentre emergono criticità inedite⁷.

L’asimmetria informativa tipica dei rapporti B2C (tra professionista e consumatore) può aumentare a causa della complessità delle transazioni digitali. I contratti per servizi o contenuti digitali spesso contengono termini tecnici e condizioni d’utilizzo lunghe e di difficile comprensione. I consumatori raramente leggono o comprendono pienamente i termini e le condizioni dei contratti online, finendo per fornire il più delle volte un consenso meramente formale alle clausole predisposte unilateralmente dai fornitori dei servizi digitali. Una sfida rilevante è dunque garantire che l’informazione sia non solo disponibile, ma anche chiara e accessibile per permettere al consumatore di adottare decisioni realmente consapevoli.

Nell’economia digitale molti servizi apparentemente gratuiti in realtà vengono “pagati” con i dati personali dell’utente. Ciò ha richiesto un ripensamento teorico del concetto di corrispettivo: il legislatore europeo ha esplicitamente equiparato in certi casi il conferimento di dati personali a un pagamento, estendendo le tutele dei consumatori anche ai servizi digitali forniti in cambio di dati (ad esempio includendo queste tipologie di scambio nell’ambito di applicazione della normativa sui contratti a distanza).

⁵ Sebbene in parte simili fra loro, sono numerose le definizioni normative di “consumatore” introdotte nel corso del tempo. Quella qui proposta è contenuta nell’Art. 3, comma 1, lett. a), d.lgs. 6 settembre 2005, n. 206, Codice del consumo.

⁶ G. ALPA, A. CATRICALÀ, *Diritto dei consumatori*, Bologna: Il Mulino, 2016.

⁷ G. SARTOR, *New aspects and challenges in consumer protection*, Study for the committee on the Internal Market; Consumer Protection, Policy Department for Economic, Scientific; Quality of Life Policies, European Parliament, Luxembourg, 2020.

La sfida è assicurare protezione contrattuale e della privacy quando il consumatore cede dati invece di denaro, evitando che la monetizzazione dei dati personali comporti una riduzione delle garanzie di trasparenza, sicurezza e rimedi contrattuali che invece operano in caso di corrispettivo in denaro. In questo senso, il diritto dei consumatori e il diritto della protezione dei dati personali si intrecciano, dando vita a un doppio binario di tutela volto a garantire che l'utente non perda diritti solo perché paga con i propri dati.

Le imprese digitali spesso utilizzano algoritmi di profilazione e big data per personalizzare offerte, prezzi e condizioni contrattuali. Ciò può tradursi in una maggiore efficienza allocativa, in una migliore corrispondenza tra preferenze individuali e prodotti offerti e, in generale, in un'esperienza di consumo più rapida e mirata.

Allo stesso tempo, tuttavia, tali pratiche possono dar luogo a discriminazioni ingiustificate (come nel caso del *dynamic pricing*, ossia la determinazione del prezzo sulla base del profilo del singolo cliente) o ad altre strategie che rischiano di sfruttare vulnerabilità cognitive e comportamentali dei consumatori.

La sfida, tanto teorica quanto applicativa, consiste allora nel definire fino a che punto la personalizzazione possa spingersi senza violare i principi di buona fede e correttezza contrattuale, e sfociare in un'indebita influenza delle scelte del consumatore. In altre parole, occorre distinguere tra una personalizzazione "benigna", che facilita l'accesso a beni e servizi su misura, e una personalizzazione "manipolativa", che limita l'autonomia decisionale o sfrutta le vulnerabilità del consumatore a vantaggio esclusivo del professionista.

Attinente al punto precedente è il fenomeno dei *dark patterns*, ovvero interfacce e design dei siti/app concepiti per influenzare in maniera subdola le scelte dell'utente (per esempio rendendo difficile cancellare un abbonamento rispetto a sottoscriverlo, o spingendo con insistenza verso opzioni a pagamento)⁸. Tali pratiche sfruttano *bias* cognitivi e mettono in discussione la reale libertà di scelta del consumatore.

Come vedremo, a livello normativo, di recente il Digital Services Act definisce i *dark patterns* come interfacce che "deformano o alterano in modo consistente"⁹ la capacità dell'utente di prendere decisioni libere e informate, vietando alle piattaforme di progettare o organizzare le interfacce in modo da ingannare o manipolare l'utente o alterarne significativamente il comportamento di scelta. Il fatto stesso che si intervenga con un divieto puntuale di design manipolativo

⁸ Sul tema dei dark patterns si v. H. BRIGNULL, *Dark Patterns: inside the interfaces designed to trick you*, <https://www.darkpatterns.org>, 2010; J. LUGURI, L.J. STRAHILEVITZ, *Shining a light on dark patterns*, in *Journal of Legal Analysis*, 2021 (13), pp. 43-109.

⁹ Art. 25 del Digital Services Act.

sottolinea la rilevanza teorica del tema: la tutela del consumatore abbraccia ora non solo il contenuto del contratto, ma anche la forma digitale attraverso cui il contratto viene proposto.

Nel contesto digitale spesso il professionista ha sede all'estero o il consumatore acquista tramite piattaforme online globali dove l'identità e affidabilità del venditore possono non essere chiare. Ciò pone problemi di giurisdizione, legge applicabile e soprattutto di applicazione delle tutele (garanzie, rimedi, rimborsi) a livello transfrontaliero. Teoricamente, il consumatore digitale vive in un mercato senza confini, ma la tutela dei suoi diritti dipende ancora in larga misura da meccanismi nazionali.

La risposta normativa a questo problema è duplice: da un lato uniformare le regole sostanziali a livello UE (es. regolamenti come il DSA, direttive armonizzate), dall'altro potenziare la cooperazione tra autorità nazionali, come, ad esempio, ha fatto il Regolamento europeo 2017/2394 che ha rafforzato la rete CPC (*Consumer Protection Cooperation Network*) dando poteri coordinati alle autorità nazionali di protezione dei consumatori per affrontare infrazioni diffuse in più Stati¹⁰. Inoltre, obblighi come la tracciabilità dei venditori online introdotti dal DSA mirano a rendere meno anonimo il contesto digitale, facilitando identificazione e responsabilizzazione dei professionisti.

In definitiva, la tutela del consumatore digitale implica estendere principi tradizionali (trasparenza, buona fede, equilibrio contrattuale) a nuovi ambiti (dati personali, algoritmi, interfacce), tenendo conto delle sfide poste dalla tecnologia. Le sezioni seguenti illustrano come il diritto ha tradotto queste esigenze in norme concrete sui vari fronti: dai contratti a distanza ai nuovi diritti sui contenuti digitali, fino alla regolazione delle piattaforme e dei loro sistemi algoritmici.

3. Le clausole vessatorie e le pratiche commerciali scorrette

Nel contesto digitale, come in quello tradizionale, due insidie principali per il consumatore sono: (a) le clausole contrattuali vessatorie (dette anche "abusive") inserite nei contratti standard predisposti dalle controparti professionali, e (b) le pratiche commerciali scorrette messe in atto nelle fasi di pubblicità, marketing o vendita.

¹⁰ Regolamento (UE) 2017/2394 del Parlamento europeo e del Consiglio del 12 dicembre 2017 sulla cooperazione tra le autorità nazionali responsabili dell'esecuzione della normativa a tutela dei consumatori e che abroga il regolamento (CE) n. 2006/2004. La CPC (*Consumer Protection Cooperation*) è la rete che riunisce le autorità nazionali degli Stati membri competenti in materia di tutela dei consumatori, insieme alla Commissione europea. Essa consente di coordinare indagini e azioni transfrontaliere contro pratiche scorrette diffuse su larga scala, garantendo un'applicazione più uniforme e incisiva del diritto europeo dei consumatori.

L'ordinamento appresta tutele specifiche in entrambi i casi, attuando le norme di origine europea, rispettivamente contenute nella Direttiva 93/13/CEE sulle clausole abusive e nella Direttiva 2005/29/CE sulle pratiche sleali, entrambe recepite nel Codice del consumo.

Si tratta di due discipline orizzontali, destinate cioè ad applicarsi a tutti i settori economici, indipendentemente dall'oggetto del contratto o dal canale di vendita, e dunque perfettamente rilevanti anche per il commercio elettronico e per i contratti digitali. Proprio la loro natura generale le rende strumenti flessibili, in grado di essere adattati dall'interprete e dalle autorità ai contesti più moderni, come quello delle piattaforme online, della pubblicità digitale e delle interfacce utente basate su algoritmi¹¹.

Negli ultimi anni tali discipline sono state oggetto di riforma attraverso la Direttiva (UE) 2019/2161, la cosiddetta Direttiva Omnibus, che ha cercato di modernizzarne alcune disposizioni per renderle adatte ai nuovi contesti economici e tecnologici, in particolare al commercio elettronico, ai marketplace e alle pratiche digitali emergenti.

3.1. Le clausole vessatorie

Una clausola vessatoria in un contratto B2C è una clausola predisposta unilateralmente dal professionista che, malgrado la buona fede, provoca a carico del consumatore un significativo squilibrio nei diritti e negli obblighi contrattuali. In altri termini, sono clausole che alterano il normale equilibrio del contratto sfavorendo ingiustamente il consumatore, ad esempio imponendo oneri eccessivi al consumatore o limitando diritti essenziali, a fronte di un vantaggio per il professionista.

Questa definizione generale è contenuta nell'art. 33, co. 1 del Codice del Consumo. La vessatorietà presuppone tipicamente un contratto per adesione, con condizioni generali non negoziate: se invece una clausola è stata oggetto di trattativa individuale con il consumatore, non può essere considerata vessatoria (art. 34, co. 4). L'onere di provare l'eventuale trattativa spetta al professionista.

Il Codice del Consumo offre una tutela articolata: da un lato indica una "lista grigia" di clausole che si presumono vessatorie fino a prova contraria (art. 33, co. 2), dall'altro una "lista nera" di clausole considerate sempre vessatorie perché caratterizzate da uno squilibrio intrinseco (art. 36, co. 2)¹².

¹¹ Cfr. G. ALPA, A. CATRICALÀ, *Diritto dei consumatori*, cit.; H.W. MICKLITZ, N. REICH, P. ROTT, *Understanding EU consumer law*, Mortsel: Intersentia, 2009.

¹² Sul rapporto tra lista grigia e lista nera, v. V. ROPPO, *La definizione di clausola "vessatoria" nei contratti dei consumatori*, in *I Contratti*, 2000 (1), pp. 83-87.

Alcuni esempi di clausole nella lista grigia:

- l'esclusione o limitazione della responsabilità del professionista in caso di danni alla persona del consumatore;
- l'esclusione o limitazione delle azioni/diritti del consumatore in caso di inadempimento del professionista;
- l'imposizione di penali sproporzionate al consumatore in caso di ritardo dell'adempimento;
- la facoltà riconosciuta solo al professionista di recedere dal contratto senza analoga facoltà per il consumatore;
- il potere del professionista di modificare unilateralmente le condizioni contrattuali senza motivo valido;
- la fissazione di un foro competente diverso da quello di residenza del consumatore per le eventuali controversie.

La "lista nera" (art. 36) comprende clausole particolarmente onerose per il consumatore, come quelle che hanno per oggetto o effetto di escludere/limitare la responsabilità del professionista per morte o danno alla persona del consumatore, derivante da un atto od omissione del professionista stesso. Si tratta di clausole nulle anche se il consumatore le avesse specificamente approvate.

Le conseguenze giuridiche di una clausola vessatoria sono importanti: la clausola è affetta da nullità di protezione, ossia una nullità parziale e relativa che colpisce la clausola stessa a tutela del consumatore, lasciando però valido il resto del contratto (art. 36, co. 1 cod. cons.)¹³. Solo il consumatore, o il giudice d'ufficio¹⁴, può far valere questa nullità; il professionista non può invocarla.

Si parla appunto di nullità di protezione proprio perché serve esclusivamente a proteggere la parte debole: se il consumatore preferisce eseguire comunque il contratto, può anche non eccepire la nullità e la clausola rimarrà efficace nei suoi confronti. In ogni caso, la nullità non travolge l'intero contratto, a meno che non risulti impossibile per il contratto sussistere senza la clausola eliminata.

¹³ Si tratta di una tutela diversa rispetto a quella prevista dall'art. 1341 c.c. sulle condizioni generali di contratto, applicabile a tutti i rapporti contrattuali, anche non di consumo. In quel caso, alcune clausole particolarmente gravose (es. limitazioni di responsabilità, facoltà di recesso unilaterale del predisponente, deroghe al foro competente) necessitano di una doppia sottoscrizione specifica da parte dell'aderente per essere valide. Nel Codice del consumo, invece, la nullità di protezione opera automaticamente a favore del consumatore, senza necessità di una doppia firma, ed è azionabile soltanto da quest'ultimo.

¹⁴ La Corte di giustizia ha affermato già con la sentenza *Océano Grupo Editorial SA c. Rocío Murciano Quintero e a.* (cause riunite C-240/98–C-244/98, sentenza del 27 giugno 2000) che il giudice nazionale è tenuto a rilevare d'ufficio il carattere abusivo di una clausola contrattuale, anche se il consumatore non lo eccepisce, in quanto ciò è necessario per garantire l'effettività della tutela voluta dalla Direttiva 93/13/CEE.

Un esempio pratico nel contesto digitale: condizioni generali di un servizio *cloud* che escludano qualsiasi responsabilità del fornitore per perdita di dati imputabile al fornitore stesso sarebbero presumibilmente vessatorie. Se il consumatore subisce un danno e la clausola venisse considerata nulla per vessatorietà, il consumatore potrebbe agire per il risarcimento nonostante quella clausola. Altrimenti, una Autorità potrebbe agire per far inibire l'uso di tale clausola in generale (come vedremo più avanti per la tutela inibitoria e amministrativa).

Il recente d.lgs. 26/2023 (attuativo della Direttiva Omnibus) ha infatti potenziato la tutela amministrativa contro le clausole vessatorie: accanto all'azione individuale (il consumatore che solleva la nullità davanti al giudice) e all'azione inibitoria collettiva (associazioni consumatori o AGCM che ricorrono al tribunale per far cessare l'uso di clausole vessatorie in serie), ora vi sono procedure amministrative più incisive. Così, l'Autorità Garante della Concorrenza e del Mercato può intervenire d'ufficio o su segnalazione per valutare la vessatorietà di clausole diffuse nei contratti standard e imporre la cessazione delle stesse, comminando sanzioni. Lo scopo di queste misure è prevenire l'uso sistematico di clausole vessatorie nei settori del commercio digitale, spingendo le imprese ad adeguare proattivamente i propri modelli contrattuali a standard di correttezza e trasparenza.

L'identificazione su larga scala di clausole vessatorie all'interno dei contratti dei consumatori è attività complessa. Tuttavia, essa può oggi essere supportata anche da mezzi automatici, sfruttando tecniche di intelligenza artificiale e di elaborazione del linguaggio naturale. Un esempio celebre è rappresentato dal progetto *Claudette*, sviluppato dall'Università di Bologna e dall'Istituto Universitario Europeo che ha sperimentato l'uso del *machine learning* per riconoscere automaticamente clausole abusive nelle condizioni d'uso delle piattaforme online¹⁵. I risultati mostrano che l'algoritmo, addestrato su un corpus di contratti reali, può raggiungere un buon livello di accuratezza nell'evidenziare clausole sospette, rendendosi così uno strumento di ausilio sia per le autorità sia per le associazioni dei consumatori.

3.2. *Le pratiche commerciali scorrette*

Le pratiche commerciali scorrette attengono al comportamento del professionista prima, durante e dopo la conclusione di un contratto, nella fase del marketing, della pubblicità o della vendita. La normativa di riferimento è conte-

¹⁵ M. LIPPI, P. PALKA, G. CONTISSA, F. LAGIOIA, H.W. MICKLITZ, G. SARTOR, P. TORRONI, *Claudette: an automated detector of potentially unfair clauses in online terms of service*, in *Artificial Intelligence and Law*, 2019 (27), pp. 117-139.

nuta negli artt. 18-27 del Codice del consumo, attuativi della Direttiva 2005/29/CE, e trova applicazione anche al commercio digitale¹⁶.

Una pratica è “scorretta” se è contraria alla diligenza professionale e falsando in misura apprezzabile il comportamento economico del consumatore medio¹⁷ lo induce a prendere una decisione di natura commerciale che non avrebbe altrimenti preso (art. 20 cod. cons.). In particolare, due macro-categorie di pratiche scorrette sono le pratiche ingannevoli e le pratiche aggressive.

Le pratiche ingannevoli includono sia azioni che omissioni ingannevoli (artt. 21-22). Nel primo caso rientra qualsiasi informazione falsa o anche solo idonea a trarre in inganno il consumatore su elementi rilevanti (es. l'esistenza o la natura di un prodotto, il prezzo, le caratteristiche principali, i diritti del consumatore, ecc.), inducendolo a un acquisto che altrimenti non avrebbe fatto. Nel secondo caso (omissioni ingannevoli) si ha quando il professionista omette informazioni necessarie affinché il consumatore prenda una decisione consapevole, o le presenta in modo oscuro, ambiguo o intempestivo.

Le pratiche aggressive (art. 24) sono invece comportamenti che, attraverso molestia, coercizione (anche fisica) o indebiti condizionamenti, limitano la libertà di scelta o di comportamento del consumatore.

Il Codice del consumo contiene un elenco di pratiche ingannevoli e aggressive considerate sempre scorrette, cioè che non richiedono di valutarne la scorrettezza nel caso concreto. Vi figurano esempi classici come: dichiarare falso *endorsement* di terzi, pubblicità “esca” seguita da *upselling* forzato, piramidi, etc.

Con le modifiche introdotte dalla Direttiva Omnibus, questa lista nera è stata arricchita di nuove fattispecie legate proprio al contesto digitale e ai mercati online. Ad esempio, costituisce pratica scorretta fornire risultati di ricerca online senza chiarire che si tratta di risultati a pagamento di natura promozionale. Ciò risponde alla prassi per cui in un *marketplace* o motore di ricerca certi prodotti appaiono in cima perché sponsorizzati: se non viene indicato espressamente

¹⁶ Sul tema, v. G. DE CRISTOFARO (a cura di), *Pratiche commerciali scorrette e codice del consumo il recepimento della direttiva 2005/29/Ce nel diritto italiano (decreti legislativi nn. 145 e 146 del 2 agosto 2007)*, Torino: Giappichelli, 2008.

¹⁷ Il concetto di “consumatore medio” è stato a lungo discusso in dottrina e giurisprudenza. La nozione è stata elaborata dalla Corte di Giustizia, a partire dal caso *Gut Springenbeide* (CGUE, 16 luglio 1998, C-210/96), come parametro di valutazione oggettivo che corrisponde a un consumatore normalmente informato e ragionevolmente attento e avveduto. La direttiva 2005/29/CE e il Codice del consumo hanno recepito questa nozione come standard generale, pur prevedendo una tutela rafforzata per categorie di consumatori particolarmente vulnerabili (minori, anziani, persone in condizioni di fragilità).

che sono annunci sponsorizzati, si inganna il consumatore sulla rilevanza “naturale” del risultato¹⁸.

Anche la gestione delle recensioni online è oggetto di attenzione: la lettera *bb-ter*) del modificato art. 23 del Codice considera sempre ingannevoli le pratiche di false recensioni o valutazioni, cioè sia pubblicare recensioni false, sia dichiarare che le recensioni sono di acquirenti verificati senza aver adottato misure ragionevoli per verificarlo. Dunque, un sito che affermi “100 recensioni a 5 stelle da clienti reali” dovrà aver effettivamente controllato che i consumatori abbiano comprato il prodotto, altrimenti potrebbe incorrere in sanzioni.

Le pratiche commerciali scorrette nel contesto digitale assumono talvolta forme subdole: annunci pubblicitari mascherati da risultati “natural” o post di influencer non dichiarati come sponsorizzati, *countdown* fittizi su offerte lampo per creare urgenza artificiale, interfacce ingannevoli (*dark patterns* già citati). Si è discusso, ad esempio, se pratiche come la pubblicità mirata che sfrutta dati personali e tecniche di profilazione invasive per ripetere incessantemente messaggi commerciali o colpire categorie vulnerabili (ad esempio persone in difficoltà economica o affetti da dipendenze), possano qualificarsi come pratiche aggressive¹⁹. La Commissione europea ha ritenuto che, in tali casi, ci si possa trovare di fronte a un “indebito condizionamento” vietato dall’art. 24 della direttiva UCPD²⁰.

Il consumatore vittima di una pratica scorretta ha diritto ad esperire vari rimedi: può segnalare la pratica scorretta all’AGCM (che può aprire un procedimento e sanzionare il professionista con multe anche elevate, fino al 4% del fatturato annuo globale come prevede la Omnibus), e ha in ogni caso diritto a rifiutare la prestazione non richiesta (nel caso di fornitura non richiesta di servizi) senza costi.

In sintesi, clausole abusive e pratiche scorrette rappresentano due facce della tutela del consumatore basata su un’idea sfaccettata di equità contrattuale: la prima incide sul contenuto del contratto (epurandolo da condizioni ingiuste), la seconda sul comportamento precontrattuale e pubblicitario del professionista

¹⁸ V. art. 22, comma 4-*bis*, Codice del consumo, come modificato dal d.lgs. 26/2023 in attuazione della Direttiva (UE) 2019/2161, che modifica la Dir. 2005/29/CE imponendo obblighi specifici di trasparenza sui risultati di ricerca online.

¹⁹ F. GALLI, *Algorithmic Marketing and EU Law on Unfair Commercial Practices*, Cham: Springer, 2022.

²⁰ Commissione europea, *Linee guida sull’attuazione della direttiva 2005/29/CE relativa alle pratiche commerciali sleali*, SWD (2021) 274 final, p. 92–93, ove si chiarisce che tecniche di micro-targeting possono configurare un illecito quando limitano significativamente la capacità di scelta consapevole del consumatore.

(assicurando che la formazione del consenso non avvenga tramite inganno o coercizione).

Nel commercio elettronico entrambe le tutele sono cruciali: contratti standard online possono celare clausole sbilanciate, e la comunicazione digitale consente nuove forme di persuasione commerciale. Il quadro normativo – armonizzato a livello Ue – offre strumenti per contrastare efficacemente queste insidie, sebbene la rapidità di evoluzione delle tecniche di marketing digitale imponga alle autorità la necessità di un costante monitoraggio.

4. La disciplina dei contratti conclusi a distanza

Il commercio digitale rientra nella più ampia categoria giuridica dei contratti a distanza, definiti come quei contratti stipulati senza la presenza fisica simultanea delle parti, mediante l'uso esclusivo di uno o più mezzi di comunicazione a distanza (internet, telefono, email, ecc.).

La disciplina dei contratti a distanza costituisce da sempre uno dei pilastri della tutela del consumatore digitale, poiché la gran parte delle transazioni online – dall'acquisto di un bene su un sito e-commerce alla sottoscrizione di un servizio digitale – rientra in tale definizione. Il diritto europeo, a partire dalla Direttiva 97/7/CE del Parlamento europeo e del Consiglio del 20 maggio 1997 relativa alla protezione dei consumatori in materia di contratti a distanza²¹, e poi con la successiva Direttiva 2011/83/UE del Parlamento europeo e del Consiglio del 25 ottobre 2011 sui diritti dei consumatori²², ha progressivamente costruito un quadro organico di tutela del consumatore nei contratti a distanza.

Nel nostro ordinamento, tale disciplina è stata recepita nel Codice del Consumo (d.lgs. 206/2005), agli artt. 45-67, e prevede garanzie specifiche per i contratti conclusi online e a distanza. Si tratta in particolare di obblighi informativi precontrattuali rafforzati, volti ad assicurare un consenso realmente consapevole, e del diritto di recesso riconosciuto al consumatore come strumento essenziale di protezione.

²¹ Direttiva 97/7/CE del Parlamento europeo e del Consiglio, del 20 maggio 1997, relativa alla protezione dei consumatori in materia di contratti a distanza, GUCE L 144 del 4 giugno 1997, pp. 19 ss.

²² Direttiva 2011/83/UE del Parlamento europeo e del Consiglio, del 25 ottobre 2011, sui diritti dei consumatori, che modifica la direttiva 93/13/CEE del Consiglio e la direttiva 1999/44/CE del Parlamento europeo e del Consiglio e abroga la direttiva 85/577/CEE del Consiglio e la direttiva 97/7/CE del Parlamento europeo e del Consiglio, GUUE L 304 del 22 novembre 2011, pp. 64 ss.

4.1. La nozione di contratto a distanza

La disciplina si applica ai contratti B2C conclusi tramite tecniche di comunicazione a distanza organizzate dal professionista per vendere a distanza. Nel contesto digitale, ciò comprende tutti i contratti conclusi online tramite siti web, app mobili, piattaforme digitali, nonché via email o messaggistica.

La legge prevede alcune eccezioni: ad esempio, sono esclusi i contratti finanziari a distanza (disciplinati da norme *ad hoc*), i contratti relativi a servizi sociali, assistenza sanitaria, giochi d'azzardo online autorizzati, servizi turistici pacchetto (che hanno direttive specifiche), ecc. (cfr. art. 47 cod. cons.). Tali eccezioni sono motivate dalla natura peculiare di alcuni servizi o dall'esistenza di regimi speciali di tutela.

Va evidenziata inoltre una novità introdotta dalla già citata Direttiva Omnibus: l'estensione di molte tutele dei contratti a distanza anche ai servizi digitali senza corrispettivo in denaro pagati con i dati personali. Oggi, ai sensi dell'art. 45 cod. cons., per "contratto di vendita" o di servizio si intende anche quello in cui il consumatore fornisce dati personali come corrispettivo, salvo i casi in cui i dati siano trattati esclusivamente per erogare il servizio o per obbligo di legge.

Dunque, ad esempio, l'iscrizione a un *social network* come Instagram o ad un servizio di *cloud storage* gratuito come Google Drive previa registrazione rientra nel campo dei contratti a distanza tutelati, comportando obblighi informativi e diritto di recesso a carico del fornitore analoghi a quelli di un normale contratto oneroso. Questa evoluzione normativa risponde alla realtà del mercato digitale, dove il dato personale ha valore economico e la tutela del consumatore doveva colmare questo "gap" di protezione.

4.2. Le informazioni precontrattuali

Prima che il consumatore sia vincolato da un contratto a distanza, il professionista è tenuto per legge a fornire una serie di informazioni precontrattuali in modo chiaro e comprensibile (art. 49 cod. cons.). Tali obblighi informativi mirano a colmare la distanza fisica e l'impossibilità per il consumatore di ispezionare il bene o conoscere il servizio di persona prima dell'acquisto.

L'elenco delle informazioni da fornire è dettagliato²³. In sintesi, devono essere comunicati almeno:

- Caratteristiche principali dei beni o servizi offerti;
- Identità del professionista (denominazione, indirizzo geografico della sede, recapiti telefonici, email);

²³ Articolo 49 cod. cons.

- Prezzo totale dei beni o servizi, comprensivo di imposte, e ogni costo aggiuntivo di spedizione o altro (o, se non calcolabile in anticipo, indicazione che tali spese potrebbero essere addebitate);
- Modalità di pagamento, consegna ed esecuzione del contratto; data o termine entro cui il professionista si impegna a consegnare il bene o fornire il servizio;
- Informazioni sul diritto di recesso: condizioni, termini e procedure per esercitarlo, modulo tipo per il recesso, nonché l'eventuale informazione che – nei casi previsti dall'art. 59 cod. cons. – il diritto di recesso non si applica (o le circostanze in cui il consumatore ne perde il diritto);
- Costi di restituzione dei beni in caso di recesso, se non possono essere normalmente restituiti via posta, o indicazione che tali costi sono a carico del consumatore (se così stabilito dal venditore);
- Garanzie legali e commerciali: promemoria dell'esistenza della garanzia legale di conformità per i beni e, se del caso, eventuali garanzie commerciali aggiuntive offerte;
- Durata del contratto (se a esecuzione continuata o periodica) o le condizioni di rinnovo o risoluzione per contratti a tempo indeterminato o tacitamente rinnovabili;
- Meccanismi di risoluzione extragiudiziale dei reclami cui il professionista aderisce volontariamente, e come vi si può accedere.

Tutte queste informazioni formano parte integrante del contratto a distanza e non possono essere modificate se non con espresso accordo delle parti (art. 49, co. 5 cod. cons.). Esse vanno fornite prima della conclusione del contratto, cioè prima che il consumatore inoltri l'ordine o accetti l'offerta.

Nel caso di contratti conclusi mediante procedure elettroniche, il Codice impone anche che, subito prima di effettuare l'ordine vincolante, il professionista evidenzi in modo chiaro le informazioni essenziali – in particolare le caratteristiche principali, il prezzo totale, la durata del contratto e le condizioni di recesso – e che il consumatore confermi esplicitamente che l'ordine implica obbligo di pagamento (es. pulsante “Acquista – obbligo di pagamento”) pena la nullità del contratto (art. 51, co. 2-3 cod. cons.).

La legge sanziona duramente la mancata osservanza di questi obblighi informativi. In particolare, se il professionista omette di informare il consumatore sul diritto di recesso (condizioni, termini, procedure e modulo), la durata del recesso viene estesa di 12 mesi rispetto ai 14 giorni standard, dando così al consumatore fino a 12 mesi e 14 giorni per ripensarci. Se entro tale periodo il professionista fornisce comunque l'informativa mancante, il termine di 14 giorni decorre dal momento della ricezione tardiva delle informazioni da parte del

consumatore. Ciò incentiva fortemente i venditori online a rispettare gli obblighi informativi fin dall'inizio.

A seguito delle modifiche introdotte dalla Direttiva Omnibus, recepita in Italia col d.lgs. 26/2023, per i contratti conclusi tramite *marketplace*²⁴ online si sono aggiunti obblighi informativi specifici. In particolare, il gestore del mercato online deve informare il consumatore, “se del caso”, come sono ripartiti gli obblighi contrattuali tra il venditore terzo e la piattaforma stessa; questo per chiarire chi risponde di cosa (ad esempio, chi deve garantire la conformità del prodotto, chi gestisce resi e rimborsi). Inoltre deve essere comunicata la natura del venditore terzo, ossia se chi offre il bene/servizio sul marketplace agisce da professionista oppure da privato. Tale informazione è cruciale perché, se il venditore è un privato, il consumatore sa che non godrà delle tutele previste dal Codice del consumo, applicandosi quest'ultimo solo ai professionisti.

Parimenti, nei risultati di ricerca su una piattaforma, deve essere indicato se un certo posizionamento o offerta è frutto di inserzione a pagamento, cioè che sia un contenuto promozionale. La trasparenza sul *ranking* online è ora obbligatoria: i *marketplace* devono spiegare i parametri principali che determinano l'ordine dei risultati quando un consumatore effettua una ricerca, inclusa l'eventuale importanza data a sponsorizzazioni. Questo insieme di obblighi mira ad aumentare la fiducia e la consapevolezza del consumatore nelle compravendite online, rendendo l'esperienza di acquisto più trasparente riguardo alla natura delle offerte e all'identità delle controparti.

4.3. Il diritto di recesso

Il diritto di recesso è forse la più incisiva tutela riconosciuta al consumatore nei contratti a distanza. Disciplinato dagli artt. 52-59 cod. cons., esso consente al consumatore di «recedere dal contratto, senza alcuna penalità e senza obbligo di motivazione» entro un determinato termine.

In pratica, si concede al consumatore un periodo di ripensamento di 14 giorni di calendario, durante il quale può cambiare idea e recedere dal contratto ottenendo il rimborso di quanto pagato. Questo perché negli acquisti a distanza il consumatore non ha avuto la possibilità di vedere o testare la qualità del prodotto, o valutare pienamente il servizio, prima della conclusione; il recesso ri-

²⁴ Ai sensi dell'art. 18, comma 1, lett. n-ter), del Codice del consumo, come modificato dal d.lgs. 26/2023, per “mercato online” si intende «un servizio che utilizza un software, compreso un sito internet, una parte di un sito internet o un'applicazione gestiti dal professionista o per suo conto, che consente ai consumatori di concludere contratti a distanza con altri professionisti o consumatori». La definizione riprende quella inserita dalla Direttiva (UE) 2019/2161 (Omnibus), che ha modificato l'art. 2, punto 17, della Direttiva 2011/83/UE sui diritti dei consumatori.

stabilisce così l'equilibrio concedendo un "diritto al ripensamento". Durante il periodo in cui può essere esercitato il diritto di recesso, il contratto è valido e vincolante; con la comunicazione di recesso il rapporto si scioglie *ex nunc*.

Il termine di 14 giorni decorre in modo diverso a seconda della tipologia contrattuale:

- Per contratti di servizi, dal giorno della conclusione del contratto (cioè dell'accordo, poiché l'erogazione del servizio potrebbe iniziare subito dopo);
- Per contratti di vendita di beni, dal giorno in cui il consumatore (o un terzo da lui designato, diverso dal vettore) acquisisce il possesso fisico del bene. Nel caso di consegna multipla: l'ultimo bene consegnato (per ordini di beni molteplici), l'ultimo lotto o pezzo (per beni composti da più parti) o il primo bene consegnato (per consegne periodiche di beni durante un certo periodo).
- Per la fornitura di contenuto digitale non su supporto materiale (es. download o streaming fornito immediatamente online), il termine decorre dal giorno della conclusione del contratto.

Quest'ultima previsione chiarisce che, per i contenuti digitali forniti via internet (non su DVD o supporto tangibile), il conteggio parte subito: il legislatore ha previsto inoltre una disciplina particolare per il caso in cui il consumatore inizi l'esecuzione prima dei 14 giorni, come vedremo nelle eccezioni.

Per esercitare il diritto di recesso il consumatore deve inviare al professionista una dichiarazione esplicita della volontà di recedere (non è tenuto a motivarla) prima della scadenza dei 14 giorni. Può utilizzare il modulo tipo di recesso previsto (Allegato I parte B del Codice) oppure una qualsiasi altra dichiarazione purché chiara – ad esempio, una email con cui comunica l'intenzione di avvalersi del recesso. Se il professionista offre sul suo sito la possibilità di compilare online il modulo di recesso, dovrà poi trasmettere al consumatore conferma della ricezione del recesso senza indugio e su supporto durevole (es. email). Per rispettare il termine basta che la comunicazione sia inviata entro il 14° giorno (fa fede, in caso di lettera, il timbro postale di invio).

Gli effetti del recesso sono risolutivi: le parti sono liberate dai rispettivi obblighi contrattuali. Se il contratto non era ancora stato eseguito, cessa l'obbligo di eseguirlo; se era stata fatta un'offerta dal consumatore, questa si intende non perfezionata. Inoltre, il recesso risolve automaticamente anche eventuali contratti accessori collegati (es. contratti di credito al consumo finalizzati al bene acquistato a distanza), senza costi per il consumatore (art. 56, co. 2).

Una volta esercitato il recesso, sorgono obblighi di restituzione a carico di entrambe le parti.

Il professionista deve rimborsare tutti i pagamenti ricevuti dal consumatore, inclusi i costi di consegna iniziali (se non era stata scelta una consegna speciale più costosa). Il rimborso va effettuato senza indebito ritardo e comunque entro 14 giorni dalla comunicazione di recesso, usando lo stesso mezzo di pagamento usato dal consumatore (salvo accordo diverso, senza costi aggiuntivi). Può trattenere il rimborso finché non abbia ricevuto i beni indietro, oppure prova dell'avvenuta spedizione da parte del consumatore. È nullo qualsiasi patto che limiti il rimborso dovuto al consumatore in caso di recesso.

Il consumatore, da parte sua, deve restituire i beni al venditore entro 14 giorni dalla data in cui ha comunicato il recesso. I costi diretti di restituzione sono a carico del consumatore, salvo che il venditore abbia omesso di informarlo di ciò o abbia concordato di sostenerli egli stesso. Il consumatore deve custodire ed eventualmente utilizzare i beni solo nella misura necessaria a stabilirne natura, caratteristiche e funzionamento (come farebbe in un negozio); se li utilizza oltre tale limite e ne diminuisce il valore, può essere ritenuto responsabile della diminuzione di valore. Tuttavia, anche in caso di utilizzo e deprezzamento del bene, il Codice prevede che il consumatore non risponda di alcuna diminuzione di valore se il venditore non lo ha informato adeguatamente sul diritto di recesso: la mancata informazione sul recesso, dunque, esonera il consumatore da responsabilità per uso improprio durante il periodo di ripensamento.

Il diritto di recesso nei contratti a distanza conosce varie eccezioni (elencate nell'art. 59 cod. cons.), giustificate dalla natura dei beni o servizi. In tali casi il consumatore, pur acquistando a distanza, non può cambiare idea dopo l'acquisto.

Tra le principali eccezioni: forniture di beni confezionati su misura o chiaramente personalizzati; beni deperibili o che rischiano di scadere rapidamente; giornali, periodici; servizi completamente eseguiti prima dei 14 giorni con accordo del consumatore ad iniziare subito l'esecuzione e rinuncia al recesso; fornitura di contenuti digitali non su supporto materiale con inizio dell'esecuzione prima dei 14 giorni con consenso espresso e accettazione della perdita del recesso (esempio tipico: acquisto di un film in streaming o download immediato – il consumatore deve dare il consenso a scaricare subito e riconoscere che così perde il diritto di recesso). Questa ultima eccezione bilancia il fatto che, diversamente, un consumatore potrebbe fruire di un contenuto digitale (es. guardare un film) e poi recedere entro 14 giorni ottenendo rimborso: per evitarlo, la legge consente al trader di chiedere al consumatore di rinunciare al recesso se vuole l'accesso immediato al contenuto digitale.

In generale, la disciplina del recesso rappresenta un forte deterrente contro le vendite affrettate o aggressive online e rassicura i consumatori nell'effettuare acquisti in rete, sapendo di poter tornare sui propri passi. Le imprese di e-

commerce devono dunque strutturare con cura le proprie procedure di reso e rimborsi, e informare chiaramente i clienti di questo diritto, anche per evitare sanzioni e il prolungamento oneroso del termine di recesso in caso di omissioni informative.

5. I contratti ad oggetto digitale

Con l'espressione "contratti ad oggetto digitale" facciamo riferimento ai contratti che hanno per oggetto la fornitura di contenuti o servizi digitali, nonché ai contratti di vendita di beni che incorporano elementi digitali. Si tratta di un ambito che, fino a pochi anni fa, non godeva di una disciplina consumeristica specifica, mentre oggi – a seguito di due direttive europee gemelle del 2019 – presenta regole dettagliate a tutela dei consumatori. In particolare: la Direttiva (UE) 2019/770 sui contratti di fornitura di contenuto digitale e di servizi digitali e la Direttiva (UE) 2019/771 sui contratti di vendita di beni (inclusi i beni con elementi digitali). Entrambe sono state recepite in Italia ed entrate in vigore dal 1° gennaio 2022, modificando in profondità il Codice del consumo. Analizziamo separatamente i due filoni.

5.1. La disciplina sulla vendita e le garanzie dei beni con elementi digitali

La direttiva 2019/771, attuata in Italia col d.lgs. 170/2021, ha riscritto le norme in materia di garanzia legale di conformità e rimedi per i beni di consumo, adeguandole all'era digitale.

La principale novità che interessa la presente trattazione è l'esplicita estensione della disciplina anche ai "beni con elementi digitali", definiti come "qualsiasi bene mobile materiale che incorpora o è interconnesso con un contenuto o servizio digitale, in modo tale che l'assenza di quest'ultimo impedirebbe al bene di svolgere le sue funzioni". Esempi tipici: smartphone, smart TV, smartwatch, elettrodomestici "smart" con software integrato, auto con sistema operativo, ecc.

In sostanza, un bene materiale che dipende da software per funzionare rientra ora nella disciplina combinata di vendita di beni e aggiornamenti digitali. Dal 2022, infatti, gli artt. 128-135 del Codice del consumo – che regolano la conformità dei beni e le garanzie – sono stati integralmente sostituiti dal contenuto del d.lgs. 170/2021.

Al consumatore è sempre dovuta una garanzia biennale che il bene sia conforme al contratto: la novità è che per i beni con elementi digitali la conformità riguarda sia la parte fisica sia la parte digitale (software, servizi accessori). Il venditore deve consegnare beni conformi ai criteri soggettivi (quanto pattuito in

contratto: quantità, qualità, tipo, funzionalità, compatibilità, altri requisiti specificamente convenuti) e ai criteri oggettivi (idoneità all'uso abituale di beni dello stesso tipo, presenza degli accessori e istruzioni che il consumatore può ragionevolmente aspettarsi, qualità e corrispondenza alla descrizione anche fornite come demo/pubblicità, ecc.).

Per i beni con elementi digitali si aggiunge un obbligo di aggiornamento software: il professionista deve fornire gli aggiornamenti (sia migliorativi sia di sicurezza) necessari a mantenere la conformità del bene per il periodo che il consumatore può ragionevolmente aspettarsi, tenendo conto della tipologia e delle dichiarazioni. Ad esempio, chi vende uno smartphone deve assicurare che il consumatore riceva aggiornamenti del sistema operativo per un certo tempo, poiché un mancato aggiornamento che renda il dispositivo vulnerabile o non compatibile con app comuni potrebbe configurare difetto di conformità.

In caso di difetto di conformità che si manifesti entro 2 anni dalla consegna (per la legge italiana; la direttiva consentiva 2 anni come minimo), il consumatore ha diritto ai rimedi secondo la seguente gerarchia: riparazione o sostituzione gratuite come rimedi primari, e se non sono possibili o sono sproporzionati o il difetto persiste, riduzione del prezzo o risoluzione del contratto con restituzione del prezzo. La risoluzione non è ammessa per difetti minori (salvo eccezioni).

Rispetto al passato, la direttiva ha perfezionato alcuni aspetti: ad esempio, la riparazione deve essere completata in tempi ragionevoli, e se il venditore ritarda, il consumatore potrebbe rivolgersi altrove e chiedere il rimborso delle spese. Inoltre, per i beni con elementi digitali con fornitura continua di contenuti/servizi digitali (si pensi a una Smart TV con servizio smart incluso per 3 anni), la garanzia si estende per tutto il periodo di fornitura digitale concordato. Ciò introduce il concetto che la garanzia non sempre si esaurisce 2 anni dopo l'acquisto: se un consumatore acquista un bene il cui software deve funzionare 5 anni, questi beneficerà di una tutela di conformità sul software per quei 5 anni.

Un altro aspetto rilevante è l'onere probatorio: nei primi 12 mesi (in Italia esteso a 24 mesi con l'art. 135-ter cod. cons.), i difetti si presumono già esistenti alla consegna, salvo prova contraria del venditore. Questo facilita le richieste del consumatore. Per i contenuti o servizi digitali forniti continuativamente, se il difetto emerge durante il periodo di fornitura, si presume che vi sia stata una mancata conformità nel periodo in questione.

L'attuazione italiana della Direttiva ha mantenuto il periodo di prescrizione e decadenza sostanzialmente invariato: il consumatore deve denunciare il difetto entro 2 mesi dalla scoperta (pena decadenza dalla garanzia), e ha poi 26 mesi per agire. Questo meccanismo resta, anche se a livello europeo vi è una discussione se semplificarlo.

Infine, la Direttiva 2019/771 ha rafforzato la disciplina delle garanzie commerciali convenzionali (quelle ulteriori eventualmente offerte dal venditore o produttore): ora devono essere redatte in linguaggio semplice e comprensibile e fornire informazioni precise su diritti e modalità, altrimenti vincolano comunque il professionista alle condizioni presentate al consumatore (principio del vincolo delle dichiarazioni pubbliche). Importante per i beni digitali, se un produttore di smartphone promette aggiornamenti per 3 anni, ciò può considerarsi parte della garanzia convenzionale che il consumatore può far valere.

5.2. La disciplina sui contratti di fornitura di contenuto digitale e di servizi digitali

Parallelamente, la Direttiva 2019/770, recepita col d.lgs. 173/2021, ha introdotto per la prima volta una disciplina organica per i contratti di fornitura di contenuti digitali e servizi digitali.

Nel Codice del consumo è stata inserita un'intera nuova sezione (artt. 135-octies ss.) dedicata a questi contratti. Essa si applica a qualsiasi contratto B2C avente per oggetto la fornitura (*una tantum* o continuativa) di un contenuto digitale (dati prodotti e forniti in formato digitale, ad es. musica, video, ebook, software) o di un servizio digitale (servizio che permette al consumatore di creare, archiviare, condividere dati in formato digitale, come social media, cloud, servizi di *Software-as-a-Service*), sia quando il consumatore paga un prezzo sia quando fornisce dati personali come corrispettivo (salvo i casi particolari in cui i dati sono usati solo per erogare il servizio). Restano fuori solo i contenuti digitali forniti in supporto materiale (es. DVD venduto) e pochi altri casi.

I punti chiave di questa disciplina sono simili a quelli visti per i beni con elementi digitali, ma adattati alla natura intangibile dei contenuti/servizi digitali.

Prima di tutto, il professionista deve fornire il contenuto/servizio digitale come previsto dal contratto e, in aggiunta, assicurare che vengano forniti al consumatore gli aggiornamenti necessari a mantenere la conformità, incluse le *patch* di sicurezza, per il periodo di tempo: (a) previsto dal contratto in caso di fornitura continuativa, oppure (b) che il consumatore può ragionevolmente aspettarsi, tenuto conto del tipo e scopo del contenuto, anche in caso di fornitura singola (art. 135-octiesdecies). Ad esempio, se un consumatore acquista una *suite* software in licenza perpetua, dovrà ricevere per un certo tempo gli aggiornamenti di sicurezza; se sottoscrive il contratto di utilizzo di un social network, finché dura il contratto dovrà ricevere aggiornamenti continui.

In analogia coi beni, il contenuto/servizio digitale deve essere conforme ai requisiti soggettivi (quanto pattuito contrattualmente in termini di qualità, funzionalità, accessibilità, compatibilità, ecc.) e ai requisiti oggettivi (idoneità agli

scopi per cui si usano abitualmente servizi simili, quantità e qualità che il consumatore può ragionevolmente aspettarsi, corrispondenza alla versione di prova o demo mostrata, ecc., art. 135-novies). Un elemento peculiare qui è la integrazione con l'ambiente digitale del consumatore: si considera un difetto di conformità anche l'incompatibilità del contenuto digitale con hardware o software del consumatore, purché presenti i requisiti minimi dichiarati dal professionista. Ad esempio, se una app è dichiarata compatibile con un certo sistema operativo ma non lo è realmente, vi è un difetto.

Se il contenuto o servizio digitale è fornito in modo non conforme, il consumatore ha diritto ai rimedi gradualisti: innanzitutto a che il professionista ristabilisca la conformità (per lo più tramite una riparazione o aggiornamento del software) senza spese per il consumatore. Questo deve avvenire entro un termine congruo e senza eccessivi disagi. Se ciò non è possibile o il difetto è tale da non poter essere risolto, oppure il professionista non vi provvede in tempo, il consumatore può richiedere una riduzione proporzionale del prezzo o la risoluzione del contratto (art. 135-*quaterdecies*). Nel caso di servizi digitali continuativi, la risoluzione non comporta necessariamente la perdita di tutto ciò che è stato fornito prima: più spesso ha effetto *ex nunc*, liberando dalle obbligazioni future.

Per i contenuti digitali forniti in unica soluzione o in un periodo definito, il professionista risponde dei difetti di conformità che si manifestano entro 2 anni dal momento della fornitura (salvo possa provarne la causa esterna). Per quelli forniti in modo continuo (es. abbonamento a Spotify) risponde dei difetti che si manifestano o persistono durante il periodo di fornitura. Vigeva una presunzione pro-consumatore: eventuali difetti emersi si presumono dovuti alla mancata conformità del servizio, salvo prova contraria (art. 135-*terdecies*).

Se il contratto prevede la fornitura di un servizio digitale continuativo, il consumatore – oltre ai rimedi per difetti – mantiene anche il diritto di recesso “classico” di 14 giorni dall’attivazione, con una particolarità: se ha chiesto di iniziare il servizio subito e poi recede entro 14 giorni, deve pagare un importo proporzionale a quanto fornito fino al recesso (es. ha usato 7 giorni di servizio su 14 disponibili in periodo di recesso, paga quei 7 giorni).

Infine, riguardo agli effetti della risoluzione, il Codice fornisce regole dettagliate per tutelare ulteriormente il consumatore: in caso di risoluzione per difetto o recesso, il professionista deve astenersi dall’ulteriore utilizzo dei dati personali forniti o creati dal consumatore, e fornire al consumatore i mezzi per recuperare i contenuti eventualmente caricati dal consumatore stesso. Salvo eccezioni (contenuti privi di utilità al di fuori del servizio, o aggregati con altri dati in modo inscindibile, ecc.), il consumatore ha diritto di riottenere gratuitamente

tutti i contenuti da lui forniti o generati durante l'uso, in un formato utilizzabile e interoperabile.

Pensiamo a foto caricate su un cloud: se il consumatore recede o il servizio viene risolto perché il professionista è inadempiente, il consumatore avrà diritto a scaricare tutte le sue foto. Inoltre, il professionista deve rendere inaccessibile al consumatore il contenuto digitale fornito (ad esempio disattivando l'account) e il consumatore deve cessare di usarlo. Queste norme rispondono alla necessità di “sganciare” il consumatore dal servizio digitale in modo equo: il consumatore non perde irrimediabilmente i propri dati ma al contempo non può continuare a beneficiare del servizio gratuito dopo la risoluzione.

6. I contratti conclusi tramite piattaforme online

Le piattaforme online – come *marketplace*, *app store*, siti di annunci – svolgono un ruolo di intermediari per la conclusione di contratti tra professionisti e consumatori. In molti casi, il consumatore non acquista direttamente su un sito di e-commerce ma direttamente tramite una piattaforma (ad es. Amazon, eBay, Airbnb) beni o servizi offerti da venditori terzi professionali. Questa “triangolazione” (piattaforma – venditore – consumatore) ha posto il problema di come assicurare la tutela del consumatore, chiarendo responsabilità e obblighi informativi tra professionista e piattaforma.

L'Unione Europea ha recentemente affrontato il tema con il già menzionato Digital Services Act (Reg. UE 2022/2065), pienamente applicabile dal 17 febbraio 2024, che tra le varie cose introduce obblighi specifici proprio per le piattaforme online che consentono ai consumatori di concludere contratti a distanza con professionisti.

In realtà, come abbiamo visto, già la Direttiva Omnibus aveva gettato le basi per una maggiore trasparenza e correttezza nei confronti dei consumatori sulle piattaforme inserendo requisiti di informazione precontrattuale specifici per i contratti conclusi tramite mercato online. Vediamo però adesso le nuove tutele approntate dal DSA.

Il DSA definisce la “piattaforma online” come un «servizio di memorizzazione di informazioni (*hosting*) che, su richiesta di un destinatario del servizio, memorizza e diffonde informazioni al pubblico» (art. 3, lett. *ì*). Il Regolamento prevede una serie di obblighi per questi soggetti concernenti la moderazione dei contenuti, ad esempio l'obbligo di predisporre procedure trasparenti per la rimozione o la disabilitazione dell'accesso a contenuti illegali o incompatibili con le condizioni di utilizzo del servizio, l'obbligo di notificare agli utenti le decisioni di moderazione adottate (con motivazioni chiare e possibilità di reclamo), e la

creazione di sistemi di gestione dei reclami interni e di risoluzione extragiudiziale delle controversie.

Alcuni di questi obblighi riguardano specificamente un certo tipo di piattaforme, cioè quelle che consentono ai consumatori di concludere contratti a distanza con gli operatori commerciali (Capo III, Sezione 4)²⁵.

In particolare, l'art. 30 DSA impone ai gestori di piattaforme marketplace di raccogliere e verificare una serie di informazioni essenziali sui venditori professionali che operano sulla piattaforma. In pratica, prima di consentire a un professionista di vendere, la piattaforma deve ottenere: dati identificativi (nome, indirizzo, contatti telefonici ed email) del professionista; copia di documenti di identità o identificazione elettronica; dati di pagamento; eventuale iscrizione a registri imprese; e una autocertificazione del professionista in cui si impegna a offrire solo prodotti/servizi conformi alle norme Ue. Inoltre, la piattaforma deve compiere sforzi ragionevoli per verificare l'affidabilità di tali informazioni.

Questo obbligo di "tracciabilità" mira a evitare l'anonimato dei venditori e a prevenire frodi: sapendo chi c'è dietro uno shop online, si facilita l'azione contro prodotti illegali o venditori scorretti. Se la piattaforma ha motivo di credere che i dati forniti da un venditore siano falsi o incompleti, deve richiedere integrazione o correzione, e in mancanza sospendere il servizio a quel venditore.

Inoltre, la piattaforma deve rendere disponibili direttamente sull'interfaccia alcune di queste informazioni (almeno nome, contatti, registro imprese, ecc.), così che i consumatori possano sapere con chi stanno effettivamente contrattando. L'idea è creare un ambiente online più trasparente e affidabile per i consumatori, limitando la presenza di venditori fantasma.

Sono poi presenti alcuni obblighi di conformità "by design"²⁶ che richiedono alla piattaforma di progettare e organizzare la propria interfaccia in modo da consentire ai venditori terzi di rispettare facilmente i loro obblighi legali in materia di informazione precontrattuale, conformità e sicurezza dei prodotti.

In sostanza, un marketplace deve strutturare le schede prodotto e le procedure in modo che il venditore debba inserire tutte le informazioni obbligatorie ai sensi della normativa consumeristica (descrizioni veritiere, avvertenze, indicazioni di sicurezza, ecc.) e ne faciliti il controllo. Ad esempio, un marketplace di

²⁵ Tale categoria si avvicina – ma non corrisponde – alla definizione di "mercato online" introdotta nel Codice del consumo, come modificato dalla Omnibus, all'art. 18, lett. f-bis: qualsiasi servizio che, tramite software (sito web o app), permette ai consumatori di concludere contratti a distanza con altri professionisti o consumatori. Rientrano a pieno titolo nella categoria delle piattaforme online disciplinate dal DSA solamente i mercati online che, oltre a consentire la conclusione di contratti a distanza tra consumatori e professionisti, svolgono anche una funzione di *hosting* e diffusione al pubblico delle informazioni fornite (es. annunci, recensioni).

²⁶ Art. 31 del DSA.

prodotti elettronici dovrebbe prevedere campi per indicare la marcatura CE, la classe di efficienza energetica, ecc. La piattaforma deve anche verificare a campione prima e dopo che i venditori forniscano effettivamente queste informazioni minime.

È un approccio di “adeguamento fin dalla progettazione”, appunto “*by design*”²⁷, delle interfacce web: la conformità legale deve essere integrata nel design della piattaforma, non lasciata alla buona volontà del singolo venditore. Questo riduce il rischio che i consumatori ricevano offerte prive di informazioni fondamentali o prodotti non conformi e sposta l’asse della responsabilizzazione sulla piattaforma, che diventa non un semplice intermediario neutrale, ma un attore chiamato a garantire standard minimi di correttezza e trasparenza nell’ambiente digitale che gestisce.

Se la piattaforma viene a conoscenza che tramite il suo servizio è stato offerto un prodotto o servizio illecito (ad esempio un giocattolo non a norma di sicurezza, un farmaco non autorizzato, merce contraffatta) da parte di un venditore, ha l’obbligo di informarne tempestivamente tutti i consumatori che abbiano acquistato quel prodotto/servizio nei precedenti sei mesi²⁸. Tale disposizione è cruciale in ottica di sicurezza: consente ai consumatori di essere avvisati di potenziali pericoli (si pensi a un dispositivo ritirato dal mercato perché rischioso) e di attivarsi (richiedere rimborso, smettere di usarlo, ecc.). Anche questo obbligo spinge le piattaforme ad essere proattive nel monitorare la liceità dei prodotti offerti.

7. Le ulteriori norme a tutela degli utenti-consumatori sulle piattaforme online

Oltre alle disposizioni specifiche per i marketplace B2C, il DSA prevede ulteriori tutele generali per gli utenti delle piattaforme online, riguardanti aspetti trasversali dell’esperienza online: la trasparenza della pubblicità online, la trasparenza e controllo dei sistemi di raccomandazione algoritmica, e il contrasto ai cosiddetti *dark patterns* nelle interfacce digitali. Queste misure riflettono l’esigenza di garantire un ambiente online più corretto e centrato sull’utente, anche quando non si tratta necessariamente di concludere contratti, ma semplicemente di come le informazioni e le scelte vengono presentate agli utenti delle piattaforme.

²⁷ K. PRIFTI, J. MORLEY, C. NOVELLI, L. FLORIDI, *Regulation by design: features, practices, limitations, and governance implications*, in *Minds and Machines*, 2024 (34), p. 13.

²⁸ Art. 32 del DSA.

7.1. La trasparenza della pubblicità online

Le piattaforme digitali, dagli *e-commerce* ai *social network*, sono veicolo di massicce quantità di pubblicità mirata, cioè pubblicità online personalizzata in base ai dati raccolti sull'utente – ad esempio la sua cronologia di navigazione, gli acquisti precedenti, la geolocalizzazione, le interazioni social o persino profili di preferenze inferiti tramite algoritmi di *machine learning*²⁹.

La tutela del consumatore impone che la natura commerciale dei contenuti sia sempre riconoscibile: «pubblicità chiaramente identificabile come tale» è un principio cardine che era già presente nella Direttiva sul commercio elettronico (art. 6) e in quella sulle pratiche scorrette³⁰.

Il DSA rafforza questi obblighi prevedendo che i fornitori di piattaforme online assicurino che gli annunci pubblicitari visualizzati siano presentati in modo chiaro e distinguibile dal resto del contenuto. L'utente deve poter capire immediatamente che si tratta di un annuncio e sapere chi è l'inserzionista (chi ha pagato per quella pubblicità).³¹

Inoltre, all'utente deve essere fornita «un'informazione significativa sui parametri principali utilizzati per determinare il destinatario» (art. 26): in pratica, perché è mostrato questo piuttosto che quell'annuncio – ad esempio se è stato targettizzato in base a certe sue caratteristiche (interessi, età, posizione geografica, etc.). Viene dunque richiesto un livello di trasparenza maggiore rispetto al passato: non solo un'etichetta “pubblicità”, ma anche la possibilità per l'utente di capire su quali criteri è basata la personalizzazione dell'annuncio³². Questo è molto rilevante perché la pubblicità online è spesso “micro-targettizzata”; il le-

²⁹ G. SARTOR, F. LAGIOIA, F. GALLI, *Regulating targeted and behavioural advertising in digital services*, Brussels: Policy Department for Citizens' Rights and Constitutional Affairs. European Parliament, 2021.

³⁰ Si veda nello specifico F. GALLI, *La pubblicità mirata al tempo dell'Intelligenza artificiale: quali regole?*, in *Contratto e impresa*, 2022 (2).

³¹ Ai sensi dell'art. 3, lett. r), Reg. (UE) 2022/2065 (Digital Services Act), per “pubblicità” si intende «le informazioni progettate per promuovere il messaggio di un'impresa o di una persona fisica, indipendentemente dal fatto che siano a pagamento o meno e dalla forma che assumono».

³² Oltre a questi obblighi generali di trasparenza sugli annunci pubblicitari (art. 26 DSA), per le piattaforme di dimensioni molto grandi (VLOP) e i motori di ricerca di dimensioni molto grandi (VLOSE) si aggiunge l'obbligo, previsto dall'art. 39 DSA, di mettere a disposizione dei ricercatori qualificati e della Commissione europea un archivio facilmente accessibile con informazioni dettagliate sulla pubblicità mostrata tramite la piattaforma, compresi i contenuti dell'annuncio, la persona fisica o giuridica che lo ha finanziato, il periodo di visualizzazione, i parametri principali di targeting utilizzati e i dati relativi al numero di utenti raggiunti. Lo scopo è consentire un controllo pubblico e scientifico sulle dinamiche del mercato pubblicitario digitale, prevenendo fenomeni di manipolazione occulta o discriminazione algoritmica.

gislatore vuole dare al consumatore consapevolezza di come e perché sta vedendo certi messaggi commerciali.

A ciò si aggiunge il divieto di pubblicità mirata basata su categorie particolari di dati, cioè sui dati sensibili (es. orientamento politico, religioso, salute) e su minori: il DSA (art. 26(3) e art. 28) vieta alle piattaforme di mostrare annunci profilati sui minori usando i loro dati personali³³. Questo approccio deriva dalla percezione che certe forme di targeting possano essere particolarmente manipolative o invasive della privacy e dignità personale.

La Direttiva Omnibus, dal canto suo, ha specificato che non indicare il carattere promozionale di un risultato di ricerca (come già visto) concretizza una pratica scorretta di tipo ingannevole. Inoltre impone, tra gli obblighi informativi, di dichiarare se un prezzo è stato personalizzato attraverso meccanismi automatizzati basati sul comportamento (art. 13, co. 3 cod. cons. modif.). Ciò per evitare che il consumatore cada in “trappole di prezzo” senza saperlo (ad esempio prezzi che salgono perché l'utente ha visitato più volte quella pagina).

Tutte queste nuove norme convergono verso un principio: la pubblicità online deve essere trasparente e spiegabile. Il consumatore-utente deve avere le stesse garanzie che ha offline dove, ad esempio, un volantino o manifesto pubblicitario è chiaramente riconoscibile come tale. Questo riduce i rischi di confusione tra contenuto originale e sponsorizzato e permette scelte più informate.

7.2. I sistemi di raccomandazione trasparenti e controllabili

Un'altra innovazione del DSA riguarda i sistemi di raccomandazione che le piattaforme utilizzano per personalizzare il flusso di contenuti per gli utenti. Dalle *news feed* dei social network, alla sezione “consigliati per te” di un e-commerce, agli algoritmi di *ranking* dei video su YouTube: i sistemi di raccomandazione decidono cosa l'utente vede e in quale ordine, influenzando in modo incisivo la sua esperienza e le sue decisioni di consumo³⁴.

³³ Il Digital Services Act non fornisce una definizione autonoma di “minore”. Per ragioni di coerenza sistematica si può ritenere applicabile la definizione contenuta nel GDPR (art. 8, par. 1), secondo cui è minore chi non ha ancora compiuto 16 anni, con possibilità per gli Stati membri di abbassare tale soglia fino a 13 anni. Come noto, in Italia il legislatore, con il d.lgs. 101/2018, ha esercitato questa facoltà, fissando il limite a 14 anni (art. 2-quinquies del Codice della privacy, d.lgs. 196/2003).

³⁴ La definizione “sistema di raccomandazione” è contenuta all'art. 3, lett. s), del DSA: un sistema di piena o parziale automazione utilizzato da un prestatore di servizi di intermediazione per suggerire, dare priorità o mettere in evidenza informazioni agli utenti del servizio online, inclusa la presentazione di contenuti, beni o servizi, in un ordine specifico o mediante un profilo personalizzato.

Finora questi algoritmi sono stati progettati e utilizzati dalle piattaforme in modo opaco. Per contrastare questa tendenza, il DSA introduce obblighi di trasparenza e scelta (art. 27). In particolare, ogni piattaforma online che utilizza sistemi di raccomandazione deve indicare nei propri termini di servizio, in modo chiaro e intelligibile, quali sono i principali parametri utilizzati dall'algoritmo per suggerire contenuti o risultati agli utenti. Deve anche spiegare come l'utente può influenzare tali parametri. Questi "parametri principali" includono almeno i criteri più rilevanti per determinare i risultati e il loro rispettivo peso nel calcolo.

In pratica, se su un sito di shopping la classifica dei prodotti "consigliati" dipende da fattori come popolarità, cronologia di navigazione dell'utente, e sponsorizzazioni a pagamento, le condizioni di servizio della piattaforma dovrebbero dichiararlo esplicitamente: ad esempio "I consigli sono basati sui tuoi acquisti passati, sui prodotti che utenti simili hanno gradito e sulle offerte sponsorizzate dai venditori". Ciò consente agli utenti di comprendere il perché vedono certi suggerimenti.

Inoltre, se esistono opzioni diverse di raccomandazione, la piattaforma deve offrire all'utente una funzione per selezionare e modificare l'opzione preferita in qualsiasi momento (art. 27(3)). Ad esempio, un social network come Facebook potrebbe avere l'opzione di *feed* algoritmico vs *feed* cronologico: il DSA richiede che l'utente possa scegliere di vedere i post in ordine cronologico anziché basato sulla rilevanza decisa dall'algoritmo, se quella opzione esiste.

Per le piattaforme di dimensioni molto grandi (*Very Large Online Platforms*, VLOPs)³⁵, il DSA obbliga addirittura a fornire almeno un'opzione di raccomandazione non basata sulla profilazione (art. 38 DSA). Ad esempio, Twitter dovrebbe dare la possibilità di un *feed* "Ultimi tweet" senza ranking algoritmico personalizzato. L'accesso a queste impostazioni deve essere reso semplice e a portata di mano sull'interfaccia.

Lo scopo è restituire autonomia e controllo agli utenti: non subire passivamente quello che l'algoritmo decide di mostrare, ma essere informati e poter scegliere come ordinare le informazioni. Questo è un pezzo importante della tutela dei consumatori "digitali", che non riguarda tanto e solo l'acquisto dei prodotti ma come la selezione dei contenuti orienta i comportamenti e incide sulla sfera decisionale: sapere se sto vedendo prodotti perché pagati o perché

³⁵ Si tratta delle piattaforme che, ai sensi dell'art. 33, par. 1, Reg. (UE) 2022/2065 (Digital Services Act), raggiungono un numero medio mensile di destinatari attivi del servizio nell'Unione pari o superiore a 45 milioni di utenti (ossia circa il 10% della popolazione dell'UE).

coerenti coi miei interessi aiuta a contestualizzare la scelta; e poter disattivare la personalizzazione evita il rischio della cosiddetta *filter bubble*³⁶.

Da notare che la trasparenza sugli algoritmi è un terreno delicato – c'è sempre un bilanciamento con la tutela della proprietà intellettuale e il segreto industriale sul sistema di raccomandazione – ma il DSA cerca di trovare un equilibrio chiedendo di rivelare i parametri generali, non certo l'intero codice sorgente.

7.3. I dark patterns

Abbiamo anticipato il concetto di *dark patterns*, ossia interfacce studiate per ingannare o indurre l'utente a compiere azioni non realmente volute.

Sono molteplici gli esempi di *dark patterns* che troviamo quotidianamente online: pulsanti per sottoscrivere un abbonamento evidenziati in grande e colorati, mentre il pulsante per annullarlo è nascosto in fondo a una pagina o scritto in caratteri minuscoli; *countdown* fasulli che creano un senso di urgenza artificiale ("l'offerta scade tra 5 minuti" anche se in realtà l'offerta è permanente); messaggi di scarsità ingannevoli ("solo 2 pezzi rimasti" quando il magazzino è pieno); caselle preselezionate che obbligano l'utente a deselezionare manualmente opzioni onerose (ad es. assicurazioni o servizi aggiuntivi durante un acquisto); percorsi di cancellazione di un servizio volutamente complessi rispetto alla facilità di iscrizione (cd. "*roach motel*"); notifiche insistenti e invasive che ostacolano la normale navigazione finché l'utente non accetta un acquisto o un trattamento di dati.

Il Digital Services Act affronta il tema dei *dark patterns* di petto, stabilendo all'art. 25(1) rubricato "Progettazione e organizzazione delle interfacce online", un divieto generale per le piattaforme di progettare, organizzare o operare le interfacce in modo da ingannare o manipolare l'utente, oppure in modo da alterare materialmente la sua capacità di prendere decisioni libere e informate.

Il DSA consente alla Commissione europea di adottare linee guida per dettagliare queste pratiche vietate (art. 25(3)), dando esempi come: presentare interfacce che spingono l'utente a dare un certo consenso enfatizzando graficamente un pulsante rispetto all'altro; chiedere in continuazione all'utente di fare una scelta già fatta (come *pop-up* ripetuti); rendere la procedura di cancellazione di un servizio più complessa di quella di sottoscrizione.

³⁶ La *filter bubble* è l'effetto per cui i sistemi di raccomandazione e profilazione personalizzata tendono a mostrare all'utente contenuti sempre più affini alle sue preferenze pregresse, limitando la varietà delle informazioni accessibili e creando una sorta di "bolla informativa" autoreferenziale. L'espressione è stata resa popolare da E. PARISER, *The Filter Bubble: What the Internet is Hiding from You*, London: Penguin, 2011.

Un aspetto interessante è l'interazione con il diritto consumeristico generale: l'art. 25(2) DSA specifica che il divieto sui *dark patterns* non si applica alle pratiche coperte già dalla direttiva sulle pratiche commerciali scorrette (vedi par 3.2.) o dal GDPR. Questo per evitare doppia regolamentazione: se un *dark pattern* configura già una pratica scorretta (ad es. un finto conto alla rovescia per promuovere vendite impulsive, che potrebbe ricadere nella fattispecie di pratica ingannevole), si useranno le norme in materia di pratiche commerciali scorrette. Se è un meccanismo che non permette di fornire un consenso valido al trattamento dei dati personali, interverrà il GDPR. Si evince dunque che il DSA si applica un po' come "rete di sicurezza" per quei design manipolativi che non rientrano esattamente nelle categorie esistenti.

Per il consumatore, il divieto di *dark patterns* può significare un'esperienza digitale più lineare e onesta: ad esempio, procedure di cancellazione semplificate (già alcuni grandi fornitori hanno dovuto, su pressione delle autorità, introdurre un facile "*cancel button*"), niente caselle preselezionate per servizi extra a pagamento, chiarezza nel design dei consensi privacy. Infatti, con i *dark patterns* si era notato un abuso delle conoscenze di psicologia comportamentale a scapito degli utenti – ora c'è uno stop normativo che equipara quelle astuzie a pratiche illecite.

In conclusione, queste ulteriori norme (pubblicità trasparente, algoritmi di raccomandazione trasparenti, divieto di interfacce ingannevoli) completano la tutela del consumatore digitale affrontando il contesto ambientale in cui le decisioni di consumo maturano. Non basta fornire diritti contrattuali se poi il consumatore viene di fatto pilotato o ingannato nella fase informativa. L'approccio Ue mira a un ambiente online in cui l'utente sia consapevole: sa quando qualcosa è pubblicità, sa perché vede certe offerte e può controllare la personalizzazione, e non è vittima di trucchetti di design pensati per fargli spendere di più o intrappolarlo nei servizi.

Questa è una frontiera nuova della tutela del consumatore digitale in continuo sviluppo. Allo stato attuale, la Commissione europea sta lavorando a un'ulteriore disciplina regolamentare, il *Digital Fairness Act* (DFA). Si tratta di una proposta legislativa finalizzata a colmare alcune lacune rimaste negli strumenti esistenti (come DSA, DMA, norme sui consumatori e GDPR) e ad affrontare pratiche manipolative non ancora sufficientemente disciplinate, quali *dark patterns*, design digitalmente "*addictive*", marketing non trasparente da parte degli influencer, personalizzazione predatoria dei prezzi, difficoltà e ostacoli

nelle cancellazioni degli abbonamenti, nonché dinamiche ingannevoli nei contratti digitali³⁷.

8. Profili applicativi

La tutela sostanziale dei diritti del consumatore nel commercio digitale è efficace solo se accompagnata da adeguati strumenti applicativi. In caso di violazione delle norme discusse all'interno di questo capitolo, il consumatore deve poter ottenere rimedio e le imprese scorrette, siano essi professionisti in genere, marketplace o piattaforme online, devono essere sanzionate e obbligate a conformarsi. I profili procedurali coinvolgono sia l'azione individuale davanti al giudice, sia l'intervento di autorità amministrative nazionali, nonché meccanismi di cooperazione e coordinamento a livello europeo.

In Italia, le principali autorità chiamate a vigilare sulla tutela del consumatore digitale sono:

- l'AGCM (Autorità Garante della Concorrenza e del Mercato), competente in materia di pratiche commerciali scorrette, pubblicità ingannevole, clausole vessatorie (tutela collettiva e amministrativa) e, più in generale, per l'applicazione del Codice del consumo;
- l'AGCOM (Autorità per le Garanzie nelle Comunicazioni), che è stata designata come Coordinatore dei Servizi Digitali, ovvero l'autorità competente a vigilare sull'applicazione del DSA, e che già aveva competenze su alcuni aspetti (ad es. tutela dei minori online, diritti nei servizi media) e ora avrà il ruolo di monitorare le piattaforme digitali in base al DSA.

Il d.lgs. 26/2023, attuativo della Direttiva Omnibus, ha meglio definito la tutela amministrativa contro le clausole vessatorie: ora l'AGCM può dichiarare vessatorie clausole di un contratto tipo e vietarne l'ulteriore uso, con sanzioni. Questo affianca la tradizionale azione inibitoria giudiziaria, che in Italia poteva essere promossa dall'AGCM stessa o dalle associazioni consumatori dinanzi al tribunale. Inoltre, per la violazione delle norme su informazioni precontrattuali, recesso, ecc., sono previste sanzioni pecuniarie amministrative che l'AGCM può irrogare. La Omnibus ha anche aumentato l'importo massimo delle sanzioni: l'AGCM può ora comminare multe fino al 4% del fatturato annuo mondiale dell'impresa per infrazioni gravi di portata UE. Ciò recepisce l'idea che le multe devono essere dissuasive anche per i colossi globali.

³⁷ Il Digital Fairness Act è in fase di consultazione pubblica dal 17 luglio 2025 fino al 9 ottobre 2025; la Commissione prevede di presentare una proposta legislativa nel terzo trimestre del 2026.

Sul fronte del DSA, come detto, l'AGCOM vigilerà sull'ottemperanza degli obblighi del DSA da parte delle piattaforme stabilite in Italia, in coordinamento con la Commissione Europea (che ha poteri diretti sulle VLOPs, le *Very Large Online Platforms*, e i VLOSE, cioè i *Very Large Online Search Engine*). Già si prevede una difficile ripartizione di competenze: AGCOM per obblighi derivanti dal DSA, AGCM per l'applicazione del Codice del consumo. Sarà cruciale il coordinamento, ad esempio se una violazione coinvolge sia *dark patterns* (AGCOM, DSA) sia pratiche ingannevoli (AGCM, Codice), le due autorità dovranno cooperare per evitare lacune di protezione o sovrapposizioni.

Oltre alle Autorità non bisogna dimenticare il ruolo del giudice ordinario: molti diritti del consumatore (garanzie di vendita, risarcimento danni, nullità di clausole vessatorie) vanno fatti valere, in ultima istanza, in sede giudiziale civile se il professionista non adempie spontaneamente. Il foro competente di regola è quello del luogo di residenza del consumatore (art. 66-*bis* cod. cons. lo prevede come foro inderogabile). Il consumatore può agire individualmente o, per controversie di modesta entità, ricorrere a strumenti di risoluzione alternativa delle dispute (ADR).

A tal proposito l'Ue ha predisposto la piattaforma ODR (*Online Dispute Resolution*) per le dispute transfrontaliere online: un portale web dove consumatore e professionista di diversi paesi Ue possono tentare la conciliazione avvalendosi di organismi ADR notificati. Molti grandi *marketplace* come Amazon aderiscono a sistemi di risoluzione extragiudiziale interni o convenzionati per gestire in via rapida i reclami dei clienti, spesso prima che degenerino in cause legali.

Il DSA stesso prevede che le piattaforme instaurino un sistema interno di gestione dei reclami per le decisioni di moderazione (art. 17) e che garantiscano agli utenti accesso a un organismo indipendente di risoluzione extragiudiziale per eventuali controversie sul blocco di contenuti o account (art. 18). Queste misure non riguardano tanto i contratti di acquisto, ma i rapporti utente-piattaforma in tema di contenuti. Tuttavia, indirettamente rafforzano la posizione dell'utente/consumatore anche in tali contesti (ad esempio, se un account venditore viene sospeso, dev'esserci un reclamo possibile; se un contenuto utente è rimosso erroneamente, *idem*).

A livello europeo, come accennato, opera la rete di cooperazione CPC (*Consumer Protection Cooperation*) tra autorità nazionali di tutela dei consumatori, sotto la regia della Commissione. Questa rete consente operazioni coordinate (per esempio le "*sweeps*" annuali, indagini a tappeto su temi specifici e interventi contro infrazioni diffuse in più Stati. Con le nuove norme, la Commissione può avviare con tale rete azioni coordinate contro professionisti che violino su larga scala i diritti dei consumatori europei.

In ambito DSA, invece, per le *VLOP* (piattaforme con oltre 45 milioni utenti EU) la sorveglianza spetta direttamente alla Commissione europea con eventuale coinvolgimento del Comitato europeo per i servizi digitali, organo di coordinamento tra le autorità nazionali competenti in ciascun stato membro ad applicare il DSA (art. 61 DSA). Le sanzioni DSA per i grandi fornitori possono arrivare al 6% del fatturato totale realizzato a livello mondiale su base annua, a dimostrazione della volontà di rendere effettivo e incisivo il sistema di *enforcement*.

Non va dimenticata la possibilità per le associazioni dei consumatori di agire a tutela collettiva: sia attraverso la segnalazione alle autorità, sia mediante strumenti giudiziali come le azioni inibitorie (già menzionate per clausole abusive e pratiche scorrette) o le nuove azioni rappresentative risarcitorie previste dalla direttiva 2020/1828 (una sorta di class action sul modello americano) consentiranno alle associazioni qualificate di agire anche per ottenere rimedi compensativi per gruppi di consumatori vittime di violazioni diffuse.

PARTE V – SICUREZZA

LA CYBERSICUREZZA NELLA TRASFORMAZIONE DIGITALE

Raffaella Brighi¹

SOMMARIO: 1. Introduzione: gli impatti della Cyber(in)sicurezza sulla società digitale. – 2. Definizioni e nuovi paradigmi. – 3. Progettare la Cybersicurezza. – 3.1 I requisiti fondamentali: dalla triade CIA agli ambienti cyberfisici. – 3.2 Incidenti, minacce e vulnerabilità. – 3.3 Il rischio e la sua *governance*. – 3.4 Il *framework* NIST e i controlli di sicurezza. – 4. Cybersicurezza e Intelligenza Artificiale, tra opportunità e nuove sfide. – 5. Un approccio armonizzato alla Cybersicurezza.

1. Introduzione: gli impatti della cyber(in)sicurezza sulla società digitale

Nell'attuale società digitale dove ogni aspetto della vita individuale e collettiva – dall'erogazione dei servizi pubblici all'istruzione, dal lavoro all'economia, fino ai processi democratici – dipende da infrastrutture digitali, reti informatiche e tecnologie complesse, la cybersicurezza rappresenta una sfida di primaria importanza. La transizione al digitale produce benefici evidenti in termini di efficienza, accessibilità e innovazione, ma espone anche a rischi sempre più sofisticati, mirati e pervasivi. Negli ecosistemi digitali di oggi – complessi, dinamici e iperconnessi – la superficie d'attacco cresce costantemente, esponendo nuove vulnerabilità e molteplici punti di accesso che possono essere sfruttati da soggetti malevoli per compromettere dati, sistemi e processi istituzionali o aziendali.

¹ La ricerca è stata svolta nell'ambito del progetto PNRR “Partenariato Esteso” Progetto “Security and Rights in the CyberSpace – SERICS”, a valere sul Piano Nazionale di Ripresa e Resilienza (PNRR) – Missione 4 Istruzione e ricerca – Componente 2 Dalla ricerca all'impresa - Investimento 1.3, D.D. 341 del 15/03/2022, codice proposta PE00000014, CUP J33C22002810001– Next Generation EU ed anche nell'ambito del progetto ERC Computable Law (“CompuLaw”)–Grant Agreement 833647.cerca all'impresa - Investimento 1.3, D.D. 341 del 15/03/2022, codice proposta PE00000014, CUP J33C22002810001– Next Generation EU ed anche nell'ambito del progetto ERC Computable Law (“CompuLaw”)–Grant Agreement 833647. Il presente capitolo riprende alcune delle argomentazioni e delle tematiche trattate in R. BRIGHI, G. ADINOLFI (a cura di), *Governare la sicurezza degli (eco)sistemi cyberfisici. Regolamentazione, diritti e politiche*, Torino: Giappichelli, 2025. Il libro è risultato delle ricerche condotte dall'autrice nell'ambito del progetto EcoCyber per il partenariato esteso SERICS.

La cybersicurezza, o meglio la cyber(in)sicurezza, non è più un problema settoriale o tecnico, limitato all'ambito delle tecnologie dell'informazione e della telecomunicazione (ICT), ma rappresenta oggi un rischio sistemico che incide trasversalmente su tutti i settori della vita sociale, economica e politica, con impatti profondi e duraturi.

I report pubblicati da associazioni del settore e agenzie istituzionali in materia di cybersicurezza documentano quanto, a fronte della crescente esposizione alle minacce informatiche, un livello di protezione adeguato sia ancora lontano dall'essere raggiunto². Secondo il Rapporto Clusit 2025, che analizza gli incidenti cyber più gravi avvenuti nel 2024 su scala globale, il numero di attacchi informatici ha continuato a crescere in modo costante e allarmante. Negli ultimi cinque anni, la media mensile degli incidenti confermati è quasi raddoppiata, passando da 156 nel 2020 a 295 nel 2024. Solo nel 2024, si è registrato un aumento del 27,4% rispetto all'anno precedente, con 3.541 attacchi noti, contro i 2.779 del 2023. Tuttavia, non è solo la frequenza degli attacchi ad aumentare. Anche la gravità media degli incidenti (*severity*) si è aggravata costantemente nel corso degli ultimi cinque anni. Nel 2024, circa l'80% degli attacchi è stato classificato come grave o critico, a fronte del 50% registrato nel 2020³. Considerando che si tratta solo di attacchi andati a segno e resi pubblici, il fenomeno reale è probabilmente ben più ampio.

Nel complesso, i dati mostrano un mutamento strutturale nello scenario della cybersicurezza, segnato da un netto peggioramento rispetto al periodo 2011-2019. L'accelerazione della transizione digitale dovuta alla pandemia, l'intensificarsi delle tensioni geopolitiche (che hanno portato a una situazione di vera e propria guerra cibernetica diffusa) e la rapidissima diffusione dell'intelligenza artificiale sono tra i principali fattori di questo incremento. A questo mutamento non è corrisposto un adeguato rafforzamento delle difese, né in termini di consapevolezza culturale né di risorse tecniche, normative e organizzative.

Le minacce informatiche colpiscono un'ampia gamma di soggetti, dai privati cittadini alle grandi aziende, fino agli enti pubblici e le istituzioni governative. Il settore più colpito risulta essere quello governativo, seguito da sanità, istruzione e servizi finanziari, a dimostrazione del fatto che nessun ambito può considerarsi immune. In aggiunta a rischi noti come disuguaglianze, discriminazioni, controllo sociale e concentrazione del potere digitale, le tensioni geopolitiche e i conflitti in corso hanno reso evidente che il rischio cibernetico è una questione globale e prioritaria. Gli attacchi informatici, sempre più sofisticati e offensivi,

² Tra tutti, ENISA *Threat Landscape* 2025; Relazione annuale (2024) al Parlamento della Agenzia per la Cybersicurezza nazionale; Rapporto Clusit 2025 sulla sicurezza ICT.

³ Il Rapporto Clusit è liberamente scaricabile all'indirizzo: <https://clusit.it/rapporto-clusit/>.

non minacciano solo la sicurezza dei dati o dei servizi digitali, ma possono veicolare minacce sistemiche, colpendo infrastrutture critiche, alimentando il terrorismo internazionale, i conflitti tra Stati, le attività economiche illecite e le campagne di disinformazione.

Queste considerazioni confermano come la tutela dei diritti fondamentali delle persone, la sicurezza pubblica e la difesa delle infrastrutture critiche nazionali non possano oggi prescindere dall'adozione di processi, tecnologie e strategie orientate alla prevenzione e alla resilienza degli ambienti digitali. La cybersicurezza assume dunque una crescente centralità non solo a livello tecnico, ma anche politico, legislativo e strategico, alimentando investimenti pubblici e privati e ridefinendo priorità istituzionali a livello nazionale ed europeo⁴.

L'Unione Europea ha riconosciuto l'importanza della cybersicurezza vedendola come elemento abilitante alla trasformazione digitale. Questo si è tradotto nell'emanazione di tre diverse *Strategie* che, sin dal 2013, promuovono un approccio di tipo globale, basato sulla cooperazione internazionale, la condivisione di informazioni e la redistribuzione di responsabilità tra settore pubblico e privato⁵. In questo quadro, sono stati adottati o proposti diversi atti giuridici che lungo tre macroaree di intervento – la resilienza, il contrasto al cybercrimine, la cyberdifesa e la cyberdiplomazia – definiscono un nuovo assetto normativo in materia di cybersecurity ed è stato potenziato e rafforzato il ruolo dell'ENISA (Agenzia dell'Unione Europea per la cybersicurezza). In Italia, la creazione dell'Agenzia per la Cybersicurezza Nazionale (ACN) nel 2021, all'interno del Piano Nazionale di Ripresa e Resilienza (PNRR), rappresenta un passo significativo verso un sistema di sicurezza più coordinato e robusto⁶.

⁴ La letteratura scientifica in argomento è molto ampia. *Ex multis*, T.F. GIUPPONI, *Il governo nazionale della cybersicurezza*, in *Quaderni Costituzionali*, 2024 (2); R. URSI (a cura di), *La sicurezza nel cyberspazio*, Milano: Franco Angeli, 2023; F. CASAROSA, G. COMANDÉ, *Aspettando la NIS2: ovvero il diritto privato della Cybersecurity*, in *Il Diritto dell'informazione e dell'Informatica*, 2024 (XL/1); S. ROSSA, *Cybersicurezza e Pubblica Amministrazione*, Napoli: Editoriale scientifica, 2023; R. BRIGHI, P.G. CHIARA, *La cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto UE*, in *Federalismi*, 2021(21), pp. 18-42; G. ZICCARDI, *La Cybersecurity nel quadro tecnologico (e politico) attuale*, in P. PERRI, G. ZICCARDI (a cura di) *Tecnologia e Diritto*, Milano: Giuffrè Francis Lefebvre, 2019, pp. 207-210. Particolare rilievo assumono anche gli investimenti destinati alla ricerca in materia di cybersicurezza in Italia previsti dal Piano Nazionale di Ripresa e Resilienza, finanziato dall'Unione europea attraverso il programma NextGenerationEU. Tali risorse hanno sostenuto numerosi progetti di ricerca sviluppati nell'ambito del Partenariato Esteso SERICS – Security and Rights in the Cyberspace (<https://serics.eu/>) negli ultimi tre anni.

⁵ Commissione europea e alto rappresentante dell'UE per gli affari esteri e la politica di sicurezza JOIN (2013) 1 final; JOIN (2017) 450 final; JOIN (2020) 18 final.

⁶ L'Agenzia, che è il cardine della infrastruttura italiana di cybersecurity, è stata istituita con il d.l. 82/2021 e organizzata con il d.p.c.m. 223/2021.

Da branca specialistica dell'informatica, la cybersicurezza si è rapidamente evoluta in una scienza multidisciplinare, dove convergono competenze tecniche, gestionali, organizzative e giuridiche.

In questo contesto, il ruolo del giurista risulta essenziale: non solo nella definizione di cornici normative adeguate alla complessità del rischio digitale, ma anche nella progettazione di modelli di governance efficaci, nella valutazione delle responsabilità, nella tutela dei diritti e nella regolazione degli equilibri tra sicurezza e libertà individuali. Per questo, è fondamentale acquisire familiarità con i concetti tecnici di base e, allo stesso tempo, saper riconoscere il ruolo del diritto nella definizione degli obblighi, delle responsabilità e dei limiti che regolano gli interventi in ambito cibernetico. Tale consapevolezza rappresenta un passaggio cruciale per comprendere come il diritto possa contribuire alla costruzione di un ecosistema digitale sicuro, affidabile e rispettoso dei valori costituzionali.

2. Definizioni e nuovi paradigmi

Il concetto di cybersicurezza (derivato dall'espressione inglese *cybersecurity*) ha origini nell'ambito della sicurezza informatica, una disciplina che ha cominciato a definirsi tra gli anni '80 e '90, quando la rapida diffusione delle tecnologie ICT in settori produttivi, istituzionali e privati rese evidente l'esigenza di adottare misure specifiche per la protezione di sistemi e dati dalle prime minacce digitali⁷. Con l'espansione delle reti e dei servizi digitali, il panorama delle minacce si è rapidamente evoluto. Nei primi anni duemila, l'interconnessione globale ha favorito l'emergere di attacchi distribuiti, come i Denial of Service (DDoS), usati anche per scopi geopolitici (ad esempio, in Estonia nel 2007). Al contempo, spyware, trojan e rootkit hanno iniziato a essere impiegati per sottrarre dati e accedere in modo occulto a infrastrutture critiche.

In questa fase, la sicurezza informatica si è sviluppata sotto il profilo teorico e metodologico attraverso norme tecniche, elaborate da organismi di standardizzazione internazionali (come ISO, NIST, CEN e CENELEC), che hanno introdotto definizioni fondamentali e fornito un quadro concettuale di riferimento non solo per i tecnici ma anche per il diritto. L'adozione di standard tecnici ha svolto un ruolo chiave nella definizione di requisiti, metodologie operative e strumenti funzionali alla protezione dei sistemi informativi, contribuendo alla costruzione di un linguaggio tecnico condiviso. È noto, del resto, che il diritto

⁷ Per approfondimenti, sia consentito il rimando a R. BRIGHI, *Introduzione al concetto di cybersicurezza: una prospettiva informatico-giuridica*, in R. BRIGHI, G. ADINOLFI (a cura di), *Governare la sicurezza degli (eco)sistemi cyberfisici. Regolamentazione, diritti e politiche*, cit.

ha progressivamente recepito tali standard tecnici, riconoscendo la centralità della sicurezza informatica nella regolazione degli ambienti digitali⁸.

L'approccio originario alla sicurezza informatica era focalizzato essenzialmente sulla protezione del computer o più in generale del sistema informatico, dei suoi apparati, dei programmi informatici e delle infrastrutture, come sintetizzato dalle espressioni *Computer security* e la successiva estensione *Network security*. Con l'evolversi della società verso modelli fortemente basati sulla produzione, circolazione e valorizzazione dell'informazione – la c.d. 'società dei dati' – si è progressivamente affermata una nozione di sicurezza orientata alla salvaguardia dell'informazione in quanto tale, sintetizzata nel concetto di *Information security*.

Una definizione ampiamente condivisa è stata fornita dal NIST (*National Institute of Standards and Technology*) secondo cui la sicurezza informatica è «la protezione fornita a un sistema informativo allo scopo di ottenere, come obiettivo applicabile, la conservazione dell'integrità, della disponibilità e della confidenzialità delle risorse del sistema informativo stesso (inclusendo hardware, software, firmware, dati e sistemi di telecomunicazione)». Tale definizione evidenzia l'orientamento della disciplina, che mira a garantire, in modo integrato attraverso l'adozione di politiche e misure tecniche, i principali requisiti della sicurezza – riservatezza, integrità e disponibilità – dei sistemi e dei loro componenti. Accanto a questi tre principi cardine, cui gli esperti del settore di riferiscono con l'acronimo RID, si sono affermati ulteriori requisiti fondamentali per garantire la certezza tecnica e giuridica delle relazioni digitali, tra cui *autenticità* dell'informazione e *non ripudio*⁹.

Con l'evoluzione tecnologica e la trasformazione digitale, di fronte a un ambiente sociotecnico interconnesso e dinamico, i paradigmi della sicurezza informatica sono confluiti nel concetto di "cybersecurity" – trasversale a discipline diverse – di cui i termini *computer security* e *information security* sono in realtà solo un sottoinsieme¹⁰. Tale concetto si configura come significativamente più

⁸ Per una introduzione informatico giuridica alla cybersicurezza si veda in particolare P. PERRI, *Sicurezza giuridica e sicurezza informatica dal d. lgs. n. 196/2003 al Regolamento generale sulla protezione dei dati*, in P. PERRI, G. ZICCARDI (a cura di), *Tecnologia e Diritto*, Milano: Giuffrè Francis Lefebvre, 2019, pp. 3-24; il capitolo dedicato alla Cybersicurezza in S. PIETROPAOLI *Informatica criminale. Diritto e sicurezza nell'era digitale*, Torino: Giappichelli, 2023; P.G. CHIARA, *Il diritto della Cybersicurezza*, in F. CASA (a cura di) *Intelligenza artificiale: diritto, etica e democrazia*, Bologna: Il Mulino, 2025, pp. 101-113.

⁹ La CIA triad (RID in italiano: Riservatezza, Integrità e Disponibilità) è alla base di molteplici norme tecniche per la sicurezza informatica. Si veda, tra tutti, NIST (National Institute of Standards and Technology), *Handbook on Computer security* o anche UNI/EN ISO 27001). Queste proprietà sono approfondite in § 3.1

¹⁰ L'evoluzione del paradigma è analizzata in R. BRIGHI, *Cybersecurity. Scenari tecnologici e regolamentazione di un'area in espansione*, in Th. CASADEI, S. PIETROPAOLI (a cura di), *Diritto e tecnologie informatiche. Que-*

ampio rispetto a quello originario, in quanto non si limita alla protezione tecnica delle reti, dei sistemi informativi e dei dati digitali, ma si estende alla salvaguardia dell'intero cyberspazio, inteso come ambito in cui interagiscono infrastrutture digitali, individui, organizzazioni e processi. Limitare il concetto di sicurezza informatica alla sola protezione delle reti e dei sistemi informativi è oggi fuorviante e anacronistico: il contesto in cui agire e i valori da proteggere sono enormemente più complessi.

Questa espansione semantica pone nuove sfide. Il termine assume significati diversi a seconda dei contesti – tecnico, politico, normativo – e delle minacce affrontate. Anche il concetto di cyberspazio risulta difficilmente delimitabile, estendendosi oggi a dispositivi fisici interconnessi, infrastrutture critiche e ambienti socio-digitali. L'evoluzione verso sistemi cyberfisici (CPS), diffusi in ambiti pubblici (sanità, trasporti, energia) e privati (smart home, industria 4.0), impone di pensare la sicurezza come integrazione tra dimensione digitale, fisica e sociale¹¹. Qualsiasi attacco a questi sistemi può avere effetti concreti sulla vita delle persone, rendendo la cybersecurity una priorità collettiva¹².

La varietà di definizioni presenti nei documenti degli organismi tradizionali di standardizzazione riflette tale complessità. Il *National Institute of Standards and Technology* (NIST) degli Stati Uniti, ad esempio, adotta una definizione focalizzata sulla componente intenzionale della minaccia, definendo la cybersecurity come la «capacità di proteggere o difendere l'uso del cyberspazio da attacchi informatici», con un accento esplicito sull'origine dolosa delle violazioni. Diversamente, le organizzazioni europee di standardizzazione – in particolare CEN e CENELEC – propongono un'accezione più articolata, secondo cui la cybersecurity riguarda la “sicurezza del cyberspazio”, definito come «l'insieme dei collegamenti e delle relazioni tra oggetti accessibili attraverso una rete di telecomunicazioni generalizzata, nonché degli oggetti stessi, qualora dotati di interfacce che ne consentano il controllo remoto, l'accesso ai dati o l'interazione con altri dispositivi e sistemi».

A differenza dei concetti tradizionali più tecnici, non esiste una definizione univoca e universalmente condivisa di “cybersicurezza”. Le definizioni adottate nei documenti normativi e tecnici risultano pertanto funzionali a orientare le

zioni di informatica giuridica, prospettive istituzionali e sfide sociali, Milano: Wolters Kluwer, 2024, pp. 75-87.

¹¹ L'“Internet of Medical Things” (IoMT) è un esempio significativo di come la cybersecurity stia progressivamente integrando considerazioni legate alla safety, poiché le tecnologie di cybersecurity devono garantire l'integrità della vita contro gli attacchi informatici.

¹² Per approfondimenti sulla sicurezza negli ambienti cyberfisici si veda in particolare, R. BRIGHI, G. ADINOLFI (eds.), *EU cybersecurity policies in cyber-physical ecosystems: challenges and perspectives*, in *European Journal of Risk Regulation*, 2025 (16/2).

pratiche di sicurezza in relazione agli scopi e alle priorità dell'organizzazione che le impiega, piuttosto che a cristallizzare una nozione stabile e definitiva.

A contribuire a una nuova concettualizzazione della cybersecurity è anche l'approccio che l'Unione europea ha messo in atto a partire dal 2013, attraverso l'adozione delle già menzionate tre *Cybersecurity Strategy* e, soprattutto, con l'approvazione del Cybersecurity Act (Reg. UE 2019/881).

Mentre la Strategia del 2013 adottava una visione prevalentemente tecnica e infrastrutturale – focalizzata sulla protezione del ciberdominio civile e militare da minacce informatiche – il Cybersecurity Act segna un punto di svolta introducendo una concezione più ampia e inclusiva, che riconosce la cybersicurezza come insieme di «tutte le attività necessarie per proteggere i sistemi di rete e di informazione, gli utenti di tali sistemi e le altre persone interessate dalle minacce informatiche». Essa non si limita alla protezione dei sistemi e degli utenti, ma si estende anche a soggetti che, pur non essendo attori diretti, possono subire conseguenze dannose da minacce informatiche. Si afferma così una concezione di cybersicurezza come strumento di sicurezza collettiva: essa contribuisce alla stabilità delle istituzioni democratiche, alla protezione degli interessi nazionali e, più in generale, alla salvaguardia dell'ordinato vivere civile¹³.

In definitiva, cybersecurity si presenta come un termine avvolgente, la cui definizione non può essere univoca né universalmente valida, poiché dipende dal contesto istituzionale, tecnico e politico in cui viene utilizzata. Essa racchiude una molteplicità di significati e funzioni, riflettendo una crescente complessità nella natura delle minacce, nella varietà dei soggetti coinvolti e nell'eterogeneità degli asset da proteggere.

3. Progettare la cybersicurezza

Le norme tecniche definiscono, sin dalle fasi iniziali della progettazione, principi di sicurezza di alto livello che rappresentano i fondamenti della cybersicurezza e trovano riscontro negli strumenti giuridici attualmente in vigore. Per questo motivo, è essenziale che anche il giurista – soprattutto se opera in ambito aziendale – conosca le metodologie e i requisiti tecnici di base che ispirano obblighi e adempimenti previsti dalla normativa nazionale ed europea. Si pensi, ad esempio, al ruolo centrale della sicurezza informatica nel GDPR (in particolare nella valutazione d'impatto sui dati personali) o nei requisiti stabiliti dalla direttiva NIS2 per la protezione delle infrastrutture critiche¹⁴.

¹³ M. PIETRANGELO, *La dimensione plurale della cybersicurezza: da potere invisibile a processo collaborativo*, in *Rivista Italiana di Informatica e Diritto*, 2024 (2), pp. 13-24.

¹⁴ Cfr. M. BUFFA, *La direttiva NIS II cybersecurity in Europa: tra innovazione, formazione e diritto vivente*,

Ad un alto livello di astrazione la sicurezza informatica si estrinseca nello studio, progettazione e implementazione di strategie volte a proteggere la dimensione digitale da un pericolo (o dalla minaccia di un pericolo) di natura volontaria o accidentale. Le attività riguardano limitatamente l'adozione di strumenti tecnologici quanto, piuttosto, la definizione di politiche (norme, regole amministrative e procedure organizzative), la predisposizione di meccanismi di controllo e la promozione di comportamenti individuali corretti.

3.1. I requisiti fondamentali: dalla triade RID agli ambienti cyberfisici

Alla base di qualsiasi strategia di cybersicurezza vi sono alcuni requisiti fondamentali che ne guidano la progettazione, la gestione e il controllo¹⁵. Tali requisiti costituiscono le basi anche per la conformità alle normative giuridiche e agli standard internazionali più diffusi, come la norma ISO/IEC 27001. Come anticipato nella §2 il modello classico, noto come triade CIA (o RID in italiano), individua tre obiettivi cardine.

Confidentiality o *riservatezza* consiste nel garantire che i dati e le informazioni siano accessibili solo da soggetti autorizzati. La riservatezza deve essere mantenuta lungo l'intero ciclo di vita dell'informazione: dall'archiviazione alla trasmissione, fino alla consultazione. Violazioni tipiche di questo requisito includono attacchi man-in-the-middle (intercettazione di dati in transito), furto di credenziali, attacchi di social engineering e configurazioni errate dei sistemi che permettono accessi non autorizzati. Un esempio concreto è l'utilizzo di credenziali deboli su sistemi esposti a Internet, come accaduto in noti attacchi ransomware contro ospedali e pubbliche amministrazioni.

Integrity o *integrità* riguarda la garanzia che i dati non siano in alcun modo alterati o modificati ad opera di soggetti non autorizzati. Anche modifiche minime possono compromettere l'affidabilità delle informazioni. Ciò significa prevenire modifiche non autorizzate da parte di soggetti diversi ma anche garantire che le informazioni stesse siano univocamente identificabili e verificabili in tutti i contesti in cui vengono utilizzate. L'integrità include quindi la tracciabilità e la verifica dei dati. Un esempio di violazione è l'iniezione di codice maligno nei log di sistema o la manomissione di dati contabili tramite malware, con potenziali conseguenze giuridiche gravi in ambito fiscale o bancario.

Availability o *disponibilità* implica che le informazioni e i servizi siano accessibili e funzionanti nei modi e nei tempi previsti ai soggetti autorizzati. La disponibilità può essere minata da attacchi DoS (Denial of Service), guasti hardware,

in *Democrazia e Diritti Sociali*, 2023 (1).

¹⁵ Si veda G. D'ANGELO, G. GIACOMELLO, *Cybersicurezza*, Bologna: Il Mulino, 2023.

errori software o disastri naturali. Ne è un esempio il blackout informatico di un ente sanitario causato da un'interruzione prolungata dell'alimentazione elettrica non prevista nei piani di continuità operativa.

I requisiti di RID, così come definiti dalle norme tecniche, stabiliscono i parametri fondamentali sulla base dei quali un sistema informatico – o uno dei suoi componenti – può essere considerato sicuro. Tali requisiti, oltre ad avere una funzione tecnica, assumono rilievo giuridico: numerose disposizioni normative, infatti, li richiamano espressamente come standard di riferimento per la valutazione della sicurezza. Ne è un esempio l'articolo 32 del Regolamento (UE) 2016/679 (GDPR), che, nel disciplinare la sicurezza del trattamento dei dati personali, impone al titolare e al responsabile del trattamento di mettere in atto misure tecniche e organizzative atte a garantire un livello di sicurezza adeguato al rischio, tenendo conto, tra gli altri fattori, proprio della riservatezza, integrità e disponibilità dei dati e dei sistemi. In tal modo, i parametri RID diventano veri e propri indicatori normativi di conformità, integrando la valutazione tecnico-giuridica delle misure adottate.

Con il passaggio al paradigma dalla *Information security* e lo sviluppo di sistemi di intelligenza artificiale, alla triade RID si sono affiancati altri requisiti, oggi essenziali per garantire un uso corretto e responsabile delle informazioni: l'*autenticità* che è la proprietà che un'entità (soggetto o risorsa) sia ciò che afferma di essere e il *non ripudio* che è la capacità di provare che un'azione o un evento ha avuto luogo, in modo tale che non si possa successivamente affermare che tale azione non sia avvenuta. L'*accountability*, infine, richiamata da diversi testi di legge comunitari, è la capacità di rendicontare con certezza e accuratezza le attività svolte da un'entità sul sistema. Firme elettroniche, marche temporali, algoritmi di hash, fino ad architetture complesse come la blockchain, sono risposte specifiche a queste esigenze.

In scenari data-driven, non è sufficiente che i dati siano protetti: devono anche essere accurati, consistenti e adatti all'uso previsto, specialmente quando vengono elaborati da sistemi automatici o utilizzati in processi decisionali automatizzati (es. algoritmi predittivi, intelligenza artificiale).

Nelle infrastrutture altamente tecnologiche attuali (trasporti, energia, sanità, industria manifatturiera), inoltre, i sistemi IT (Information Technology) si integrano sempre più con i sistemi OT (Operational Technology), che hanno la funzione monitoraggio ed esecuzioni dei processi fisici, generando ambienti cyberfisici complessi. La sicurezza informatica (sicurezza IT) e la sicurezza della tecnologia operativa (sicurezza OT), pur facendo riferimento a concetti differenti, si intersecano così sempre più spesso in un ecosistema che intreccia informazioni e aspetti operativi. La sicurezza OT richiede standard e approcci differenziati, che integrano protezioni

fisiche, segmentazione delle reti, sistemi di rilevamento delle anomalie in tempo reale e strategie di resilienza. La sfida principale risiede nell'equilibrio tra sicurezza e continuità operativa: è necessario garantire la protezione delle informazioni senza compromettere la disponibilità e l'efficienza dei processi fisici sottostanti.

3.2. Incidenti, minacce e vulnerabilità

Un incidente informatico rappresenta qualsiasi evento, doloso o colposo, che comprometta la sicurezza (ovvero l'integrità, la disponibilità o la riservatezza) delle risorse materiali, immateriali e umane di valore per un sistema o un'organizzazione. Tali eventi non si limitano agli attacchi deliberati esterni, come le intrusioni da parte di *hacker*, ma comprendono anche errori umani, comportamenti impropri da parte degli utenti, guasti hardware, malfunzionamenti software o eventi naturali.

Una particolare categoria di incidente informatico è rappresentata dalla *violazione dei dati (data breach)*, ossia «ogni evento che comporti, in modo accidentale o illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trattati da un'organizzazione», secondo quanto definito all'articolo 4 del GDPR. Questa definizione evidenzia come non sia solo la perdita di riservatezza a configurare una violazione, ma anche l'alterazione, la cancellazione o l'indisponibilità dei dati. Ne sono esempi concreti la divulgazione indebita di un database, lo smarrimento di un dispositivo contenente informazioni sensibili, l'inoltro errato di e-mail con dati personali visibili o un'interruzione temporanea dei sistemi informatici.

La sicurezza informatica si fonda sull'interazione tra procedure, controlli, comportamenti e strumenti tecnologici. Il primo importante passo, dal punto di visto metodologico, è l'identificazione degli *asset* da proteggere, la loro classificazione in base al valore e l'analisi dei *pericoli*, intesi come combinazione tra *minacce* e *vulnerabilità* dell'*asset*.

Gli standard tecnici, tra cui la famiglia ISO/IEC 27000 riferimento internazionale per la gestione della sicurezza delle informazioni, forniscono un glossario di base per la comprensione di questi concetti in chiave informatico-giuridica¹⁶:

¹⁶ Un riferimento importante per una inquadratura meno tecnica è anche il Glossario di ACN, redatto al fine di supportare chi si trova per la prima volta a dover gestire un incidente di sicurezza cibernetica, per facilitarne le comunicazioni con il CSIRT. Cfr. <https://www.acn.gov.it/portale/-csirt-italia/glossario>.

- la *minaccia* è rappresentata da un'azione, accidentale o deliberata, che può portare alla violazione dei requisiti di sicurezza definiti¹⁷. Non tutte le minacce si concretizzano in attacchi, né tutti gli attacchi riescono;
- la *vulnerabilità*, invece, è una debolezza strutturale del sistema (di design, implementazione, configurazione o gestione) che può essere sfruttata da una minaccia per causare un danno. Anche i sistemi apparentemente affidabili presentano vulnerabilità, seppur non sempre attivamente sfruttate.

Per chi opera, in senso ampio, nell'ambito della cybersicurezza, informatico o giurista, è importante conoscere il panorama delle minacce e restare informato sulle vulnerabilità dei sistemi. Per questo associazioni di settore e agenzie istituzionali, tra cui l'ACN¹⁸, pubblicano periodicamente report che analizzano l'andamento degli incidenti informatici, prendendo in esame i vettori di attacco, gli attori e le motivazioni. Le stesse svolgono operazioni di monitoraggio e campagne di condivisione delle vulnerabilità per consentirne la *patch* nel più breve tempo possibile.

Senza addentrarsi nei dettagli, in un contesto segnato da un'evoluzione rapida e incessante delle minacce e delle vulnerabilità, secondo l'*ENISA Threat Landscape 2024*, le principali minacce informatiche oggi riguardano in particolare gli attacchi alla disponibilità dei servizi, come i DDoS, seguiti dal ransomware, dal furto o dalla perdita di dati sensibili, dalla diffusione di malware, dalle frodi basate sull'ingegneria sociale, dalla disinformazione e dagli attacchi alla catena di approvvigionamento (*supply chain*). Le motivazioni che spingono questi attacchi sono perlopiù di natura economica, come il profitto derivante da estorsioni o vendite illecite di dati, ma non mancano obiettivi geopolitici, ideologici o legati allo spionaggio. Gli attori coinvolti comprendono gruppi criminali organizzati, hacker sponsorizzati da Stati, attivisti e aziende private specializzate in strumen-

¹⁷ È interessante notare la diversa prospettiva evidenziata nel Glossario ACN alla voce minaccia: «Espressione impiegata per indicare l'insieme delle condotte controindicate che possono essere realizzate nel e tramite il cyber-space ovvero in danno di quest'ultimo e dei suoi elementi costitutivi. Si sostanzia in attacchi cibernetici: azioni di singoli individui o organizzazioni, statuali e non, finalizzate a distruggere, danneggiare o ostacolare il regolare funzionamento dei sistemi e delle reti e/o dei sistemi attuatori di processo da essi controllati, ovvero a violare l'integrità e la riservatezza di dati/informazioni».

¹⁸ Di recente pubblicazione, l'Operational Summary presenta numeri e indicatori relativi alle attività operative svolte dall'Agenzia per la Cybersicurezza Nazionale (ACN) nel primo semestre del 2025, mettendoli a confronto con quelli del primo semestre del 2024. I dati analizzati provengono dal CSIRT Italia, articolazione tecnico-operativa dell'Agenzia e punto di riferimento nazionale per le notifiche obbligatorie e volontarie di incidenti previste dalla normativa (tra cui, Perimetro di Sicurezza Nazionale Cibernetica, Legge n. 90 del 2024, D.lgs n.138 del 2024, che recepisce la c.d. Direttiva NIS2).

ti offensivi. I settori più colpiti sono quelli considerati critici per il funzionamento della società, come la pubblica amministrazione, i trasporti, il comparto bancario e assicurativo, i servizi digitali, le telecomunicazioni, l'industria e la sanità, a conferma di un panorama di minacce sempre più sofisticato e trasversale, che richiede risposte integrate e una forte cultura della sicurezza.

Conoscere le tecniche di attacco può aiutare le organizzazioni a prioritizzare gli obiettivi e gli strumenti di protezione. Inoltre, avere un'idea delle intenzioni degli attaccanti le aiuta a concentrare i propri sforzi di difesa sullo scenario di attacco più probabile per ogni asset.

3.3. Il rischio e la sua governance

Il concetto di sicurezza è strettamente legato al concetto di *rischio*. Nella norma ISO 73:2009 il Rischio (R) viene definito come la combinazione della gravità (G) dell'impatto e della probabilità (P) di accadimento di un evento dannoso ($R = G \times P$). Il rischio quantifica l'incertezza rispetto al verificarsi di una minaccia e ai suoi effetti. Può derivare da un'azione dolosa (ad esempio, un attacco informatico) oppure da eventi accidentali (quali blackout, incendi o errori umani).

La gestione del rischio, cuore della sicurezza informatica, ha come obiettivo la sua riduzione mediante misure organizzative, comportamentali e tecniche. Il rischio può essere eliminabile, riducibile o tollerabile, ma non completamente azzerabile: nessun sistema può considerarsi esente da minacce. Di conseguenza, la sicurezza non va intesa come assenza di rischio, bensì come capacità di prevenirlo, gestirlo e reagire in modo efficace.

La progettazione efficace della sicurezza – attraverso procedure, controlli, comportamenti e tecnologie – è guidata dalla *gestione del rischio*.

Le metodologie e i processi per la gestione e la valutazione del rischio sono stati sviluppati nell'ambito della standardizzazione tecnica internazionale proprio per fornire ai destinatari delle norme (ad esempio, le aziende) metriche quantificabili basate su ipotesi probabilistiche che consentano di prendere decisioni sullo sfondo di potenziali scenari avversi o favorevoli. Tra questa, la norma tecnica ISO 31000 è stata progettata per assistere qualsiasi organizzazione, indipendentemente dalle dimensioni e dal settore di attività, con una metodologia che suddivide il processo di gestione del rischio in diverse fasi successive. La *gestione del rischio* è generalmente descritta come il processo che comporta «l'applicazione sistematica di politiche, procedure e pratiche alle attività di comunicazione e consultazione, di definizione del contesto e di valutazione, trattamento, monitoraggio, revisione, registrazione e reporting del rischio». Fase prodro-

mica è dunque la *valutazione del rischio* che richiede un processo di identificazione e comprensione del rischio.

Ogni disciplina si confronta inevitabilmente con forme di rischio caratterizzate da incertezza. Il rischio, infatti, può assumere la funzione di principio organizzativo, come accade nella sociologia, dove viene impiegato per interpretare le dinamiche funzionali delle società contemporanee; può essere valutato e gestito mediante approcci standardizzati, tipici dell'ingegneria; oppure può essere oggetto di regolazione giuridica.

I sistemi giuridici, da sempre, affrontano il rischio con l'obiettivo di ridurre la complessità del reale. Negli ultimi anni, la regolazione orientata al rischio è divenuta il paradigma prevalente nella legislazione dell'Unione europea, in particolare a partire dalla pubblicazione della strategia per il mercato unico digitale. La legislazione europea nei settori dei dati, dei contenuti online e dell'intelligenza artificiale è infatti ispirata da un approccio basato sul rischio, pur declinato in modo differenziato a seconda dell'ambito considerato.

Nel caso della normativa europea in materia di protezione dei dati personali, ad esempio, i rischi da considerare sono quelli connessi all'impatto potenzialmente negativo sui diritti, sulle libertà e sugli interessi degli interessati. Il Regolamento generale sulla protezione dei dati (GDPR) adotta esplicitamente una logica *risk based*, affidando ai titolari del trattamento la responsabilità di individuare e adottare le misure più adeguate a fronteggiare i rischi derivanti dalle operazioni di trattamento, al fine di proteggere i diritti e le libertà delle persone (cfr. art. 25, par. 1, GDPR).

Anche la normativa europea in materia di cybersicurezza si fonda su un approccio basato sul rischio. Tuttavia, gli obiettivi e i contesti di applicazione si discostano dall'impostazione del GDPR, che privilegia un modello "di rischio per i diritti".

La valutazione e la gestione del rischio costituiscono dunque il nucleo fondativo dell'intera disciplina della sicurezza informatica e rappresentano il cardine della più recente normativa dell'Unione europea in materia. In una prospettiva *multirischio*, essa non si limita a contemplare i rischi per reti e sistemi informativi, ma si estende anche ai rischi sociali, ai rischi per l'integrità fisica e, più in generale, ai rischi per i diritti e le libertà fondamentali. In tal modo, il quadro normativo europeo ha progressivamente ampliato la nozione di cybersicurezza, includendo nella governance anche una pluralità di rischi di diversa natura, evitando definizioni restrittive o riduttive.

I parametri di riferimento per la valutazione del rischio – come il grado di esposizione, la probabilità di accadimento e la gravità potenziale degli incidenti – rappresentano la base per determinare l'adozione di misure di sicurezza in-

formatica conformi allo stato dell'arte e in linea con gli standard europei (ETSI, CEN) e internazionali (ISO/IEC). A tali standard si collegano inoltre obblighi di notifica degli incidenti e meccanismi di adesione a schemi di certificazione della conformità.

3.4. Il framework NIST e i controlli di sicurezza

In termini generali la sicurezza informatica si articola in tre direttici: (i) realizzare sistemi robusti in grado di resistere agli attacchi, (ii) progettare metodi per il rilevamento di minacce ed anomalie al fine di garantire la resilienza dei sistemi; (iii) definire le risposte agli attacchi per ripristinare sistemi e servizi¹⁹.

La robustezza (i) è la dimensione della prevenzione: tutte le parti del sistema devono essere configurate, gestite e mantenute secondo criteri di protezione. Si valutano e gestiscono rischi noti sulla base di esperienze pregresse. Nei sistemi odierni, dove la natura dei problemi cambia e i rischi possono emergere in modo diverso, è tuttavia necessario integrare la dimensione della prevenzione con metodologie e soluzioni flessibili che, in chiave proattiva, siano in grado di adattare e aggiustare il sistema a seguito dell'evento avverso, perché anche durante la perturbazione si possano realizzare gli obiettivi (continuità operativa) trovando una nuova condizione di normalità, ovvero la *resilienza*(ii). È la fase in cui l'organizzazione, seguendo un piano prestabilito, adotta misure per mitigare i danni dell'incidente informatico e mantenere l'operatività, rileva danni e responsabilità, segnala alle autorità competenti eventuali violazioni e getta le basi della ripresa in cui saranno ripristinati i dati e la piena operatività. La (cyber) resilienza è un requisito emergente nel quadro giuridico comunitario, politico e nei piani di investimento. La *risposta* (iii) è la predisposizione di strategie misure e controlli che permettano di rispondere all'incidente o all'attacco con la riattivazione del sistema e delle sue funzioni. Ciascuna area comprende una vasta gamma di soluzioni tecniche e misure organizzative.

Per progettare in modo efficace la sicurezza di un sistema complesso, è necessario seguire un percorso metodologico articolato in più fasi:

- in primo luogo, occorre individuare le risorse (*asset*) da proteggere e valutarne il valore, considerando sia gli aspetti materiali (come dispositivi e infrastrutture) sia quelli immateriali (come dati, know-how o reputazione);

¹⁹ G. D'ANGELO, G. GIACOMELLO, *Cybersicurezza*, cit.

- successivamente, si passa all'analisi delle minacce e delle vulnerabilità che potrebbero compromettere tali risorse, stimando il danno potenziale e calcolando il livello di rischio associato (*risk assessment*);
- una volta identificati i rischi, è possibile progettare e implementare *controlli o contromisure* per ridurre o gestire quelli considerati non accettabili. Tali contromisure possono includere misure tecniche, organizzative, fisiche, procedurali o relative al comportamento del personale;
- infine, il sistema di sicurezza deve essere costantemente *monitorato e aggiornato*, affinché l'efficacia delle contromisure adottate sia mantenuta nel tempo e migliorata in risposta ai cambiamenti interni ed esterni.

Una politica della sicurezza ben strutturata deve tener conto dei vincoli specifici del contesto in cui opera il sistema informativo: vincoli tecnici, logistici, amministrativi, giuridici ed economici. Attraverso un'accurata analisi e gestione dei rischi, si devono identificare e valutare le misure più idonee a ridurre il rischio residuo globale a un livello accettabile per l'organizzazione.

Numerose metodologie, framework e standard internazionali sono di supporto agli esperti nella progettazione e gestione della sicurezza informatica, guidandoli attraverso tutte le fasi del processo, dall'analisi dei rischi alla definizione di contromisure, fino alla verifica dei risultati ottenuti. Questi strumenti forniscono linee guida operative, *best practices* e metriche di valutazione e, in molti casi, permettono anche di certificare formalmente il livello di sicurezza raggiunto.

Tra gli organismi di riferimento a livello europeo e internazionale si segnalano ENISA (European Union Agency for Cybersecurity), che elabora strategie comuni e raccomandazioni tecniche, e l'EDPB (European Data Protection Board), che fornisce indicazioni sulla protezione dei dati personali in ambito digitale. A livello globale, il NIST (National Institute of Standards and Technology) pubblica framework di riferimento ampiamente adottati in materia di cybersecurity. In Italia, il Framework Nazionale per la Cybersecurity e la Data Protection, sviluppato dal CINI (Consorzio Interuniversitario Nazionale per l'Informatica), adatta e promuove questi modelli nel contesto nazionale. Rilevante è anche il contributo degli standard ISO/IEC 27000, che costituiscono un sistema organico di norme per la gestione della sicurezza delle informazioni.

In particolare, il *NIST Cybersecurity Framework*²⁰ è alla base del *Framework Nazionale per la Cybersecurity e la Protezione dei Dati*²¹ e della tassonomia adottata dal decreto attuativo del Perimetro Nazionale di Sicurezza Cibernetica (PSNC),

²⁰ NIST (National Institute of Standards and Technology) Framework, <https://www.nist.gov/cyberframework>

²¹ CINI, Cyber Security National Lab, 2019, <https://www.cybersecurityframework.it>

Dpcm 14 *aprile* 2021, n. 81 in materia di notifiche degli incidenti e misure di sicurezza. Si tratta dunque di un modello particolarmente utile anche per l'analisi giuridica, poiché molte delle sue componenti trovano riscontro nelle normative europee e internazionali.



Figura 1: Le cinque funzioni del NIST Cybersecurity Framework

La sua articolazione in cinque funzioni fondamentali – *Identify*, *Protect*, *Detect*, *Respond*, *Recover* – consente alle organizzazioni di affrontare in modo strutturato le diverse fasi della gestione della cybersicurezza, integrando misure tecniche, organizzative e legali.

La prima funzione, *Identify*, si concentra sull'identificazione delle risorse critiche, siano esse sistemi, dati, infrastrutture, dispositivi, persone o processi, nonché sulle minacce e vulnerabilità a cui tali asset sono esposti. Questa fase costituisce il fondamento dell'intera strategia di sicurezza, poiché consente di valutare i rischi in modo sistematico, anche attraverso strumenti come la *data protection impact assessment* prevista dall'art. 35 del GDPR. In contesto giuridico, il processo di identificazione permette anche di mappare i trattamenti di dati personali, classificare le informazioni secondo il loro livello di sensibilità o di segretezza – ad esempio, dati giudiziari o sanitari o informazioni tutelate dal segreto industriale – e attribuire le responsabilità, come nel caso della nomina del responsabile della protezione dei dati o del responsabile della sicurezza.

Segue la funzione *Protect*, che mira a prevenire gli incidenti attraverso l'implementazione di controlli adeguati alla protezione degli asset. In questa fase si adottano misure quali la cifratura dei dati, l'autenticazione a più fattori per accedere ai sistemi critici e la definizione di politiche di controllo degli accessi, secondo il principio del minimo privilegio. Anche la formazione del personale, inclusa quella giuridica su temi come la protezione dei dati e la gestione dei consensi, assume un ruolo centrale. Si tratta di un ambito in cui le contromisure

tecniche si integrano con le scelte organizzative e normative, in linea con il principio di “privacy by design” e “security by design” richiesto dalla legislazione europea.

La terza funzione, *Detect*, fa riferimento alla capacità dell'organizzazione di identificare tempestivamente eventi anomali o potenziali incidenti di sicurezza. A tal fine, vengono adottati sistemi di monitoraggio continuo, raccolta e analisi dei log, strumenti per la gestione degli eventi (*Security Information and Event Management* – SIEM), oltre a tecnologie avanzate per il rilevamento delle intrusioni. L'obiettivo non è soltanto l'individuazione precoce delle minacce, ma anche la raccolta sistematica delle informazioni necessarie alla loro documentazione e analisi. In tale contesto, assume crescente rilevanza la *digital forensics*. La funzione di rilevazione è fondamentale per garantire la conformità agli obblighi normativi relativi alla notifica delle violazioni di dati personali (articoli 33 e 34 del GDPR), nonché per soddisfare gli standard di sorveglianza e prontezza operativa richiesti dalla direttiva NIS2 ai soggetti che rientrano nell'ambito di applicazione.

La funzione *Respond* si attiva nel momento in cui viene rilevato un incidente di sicurezza, e comprende tutte le attività finalizzate a contenerne l'impatto, mitigare i danni e preservare l'integrità dei sistemi e delle prove digitali. È in questa fase che vengono attivati i piani di risposta agli incidenti, si attivano le procedure di comunicazione interna ed esterna e si procede, se necessario, alla notifica alle autorità competenti. Dal punto di vista giuridico, ciò include sia l'obbligo di notificare i *data breach* al Garante per la protezione dei dati, sia gli ulteriori adempimenti introdotti dalla direttiva NIS2, che rafforza l'obbligo di comunicare rapidamente ogni incidente significativo all'autorità nazionale competente in materia di cybersicurezza. La direttiva stabilisce inoltre una responsabilità più ampia in capo al management delle organizzazioni e introduce sanzioni rilevanti in caso di inadempienza, rendendo essenziale una stretta collaborazione tra tecnici della sicurezza e consulenti legali.

Infine, la funzione *Recover* ha l'obiettivo di ripristinare tempestivamente le funzionalità compromesse da un incidente, garantendo la continuità operativa e la resilienza dell'organizzazione. Il ripristino si basa su piani di continuità operativa e di *disaster recovery*, che prevedono la possibilità di recuperare dati e servizi attraverso copie di sicurezza affidabili e misure di *backup* sicuri. Anche questa fase ha implicazioni legali, soprattutto in relazione alla responsabilità per eventuali interruzioni di servizio, alla conservazione delle evidenze digitali per fini probatori e alla trasparenza verso gli utenti e le autorità.

In conclusione, un approccio metodologicamente strutturato alla gestione della sicurezza informatica è strategico non solo per i professionisti tecnici, ma anche per i giuristi che devono tradurre gli obblighi normativi in pratiche opera-

tive coerenti, promuovendo una cultura della sicurezza condivisa e orientata alla tutela concreta dei diritti fondamentali nel contesto digitale.

4. Cybersicurezza e intelligenza artificiale, tra opportunità e sfide

L'intelligenza artificiale (IA) sta progressivamente trasformando l'ecosistema della cybersicurezza, ponendosi al contempo come risorsa strategica e fonte di nuove vulnerabilità. Le tecniche avanzate di IA permettono una protezione proattiva, adattiva e tempestiva dalle minacce informatiche potenziando la capacità di monitoraggio e risposta; tuttavia, in ragione della sua natura *dual use* la stessa è annoverata anche tra i pericoli emergenti per la sicurezza informatica. Le potenzialità della IA possono infatti essere sfruttate anche in senso offensivo, incrementando la sofisticazione, la precisione e l'asimmetria degli attacchi cyber. Inoltre, anche i sistemi di IA non sono esenti da vulnerabilità intrinseche che possono portare ad errori o essere sfruttate dagli attaccanti²².

Sul piano della difesa, le applicazioni dell'IA migliorano significativamente il rilevamento di anomalie nei sistemi e nei comportamenti degli utenti, la *threat intelligence*, la protezione degli *endpoint*, la gestione degli accessi e la protezione delle reti. Le capacità di analisi, apprendimento e adattamento della IA consentono di processare grandi volumi di dati in tempi significativamente inferiori rispetto all'intervento umano, generando spunti utili in tutto il ciclo della sicurezza: dalla valutazione preventiva del rischio, alla progettazione e implementazione delle misure protettive, fino alle attività di risposta e recupero post-incidente. L'integrazione tra IA e Big Data, nella cybersicurezza, automatizza processi decisionali complessi, basati su una molteplicità di fattori spesso non perfettamente determinabili a priori; incrementa l'efficacia operativa degli strumenti di difesa informatica e contribuisce alla costruzione di architetture di sicurezza più dinamiche, adattive e resilienti.

Sul piano *offensivo*, l'intelligenza artificiale sta diventando uno strumento sempre più utilizzato anche dagli attori malevoli, che ne sfruttano le potenzialità per condurre attacchi sofisticati. Le stesse tecniche di cyber intelligence utilizzate per la difesa vengono impiegate per costruire vettori di attacco personalizzati: link, e-mail, chatbot o contenuti deepfake difficili da distinguere dal reale. Grazie all'apprendimento rinforzato, le minacce informatiche possono eludere i sistemi di rilevamento, adattarsi ai cambiamenti dell'ambiente, scoprire vulnerabi-

²² In argomento, M.E. BONFANTI, *Artificial intelligence and the offense–defense balance in cyber security*, in *Cyber Security Politics*, 2022, pp. 64-78; R. BRIGHI, *Cybersicurezza e Intelligenza Artificiale. Un'analisi critica*, in *Biolaw Journal*, 2024 (1), pp.111-124. Per una prospettiva più tecnica si veda M. MALATJI, A. TOLAH, *Artificial intelligence (AI) cybersecurity dimensions: a comprehensive framework for understanding adversarial and offensive AI*, in *AI Ethics*, 2024.

lità specifiche e restare attive a lungo all'interno dei sistemi infetti. Un malware dotato di IA è in grado di modificare il proprio comportamento per evitare di essere individuato e raccogliere dati utili per attacchi futuri. In questo scenario, detto *Offensive AI*, gli aggressori possono anche manipolare i dati di addestramento per creare backdoor nei sistemi di intelligenza artificiale o identificare vulnerabilità da sfruttare in modo mirato.

Parallelamente, i sistemi di IA sono vulnerabili a una serie di attacchi informatici che colpiscono direttamente le loro architetture e i meccanismi interni. Le comunità open-source dell'IA, pur favorendo la condivisione della conoscenza, espongono i modelli a rischi come il reverse engineering o lo sfruttamento di interfacce pubbliche per estrarre dati sensibili. Gli attacchi di *data poisoning* consistono nella manipolazione dei dati di addestramento, alterando il comportamento del modello per allinearli agli scopi dell'attaccante. Gli *attacchi avversari*, invece, inseriscono input progettati per confondere il sistema e produrre classificazioni errate. Questi scenari, che ricadono sotto la categoria di *Adversarial AI*, rappresentano una sfida critica: l'uso malevolo dell'IA può compromettere la solidità degli strumenti di difesa informatica, minando la sicurezza stessa dei sistemi digitali su cui si fondano.

Ciò impone di riflettere sui rischi, legati alle specificità tecniche dei sistemi di IA, che sono oggetto del dibattito dottrinale più recente. La raccolta, conservazione e analisi massiva di dati, anche personali e comportamentali degli utenti, è essenziale per lo sviluppo di strumenti di difesa cibernetica basati su IA, a condizione che tali dati siano di qualità, aggiornati e provenienti da fonti diverse per descrivere in modo completo l'ambiente. Tuttavia, l'utilizzo di dati parziali o incompleti per addestrare i modelli di IA può generare *bias* nei modelli, portando a decisioni non accurate e potenzialmente discriminatorie²³. Inoltre, l'analisi stessa dei dati personali e comportamentali (attività online, comunicazioni, comportamenti di utilizzo, dati di localizzazione) rappresenta un rischio significativo per la privacy degli utenti e il diritto alla protezione dei dati personali, creando una tensione tra sicurezza e i diritti degli individui ed il monitoraggio continuo e pervasivo dei sistemi e degli utenti, per identificare minacce e anomalie, se non regolato può trasformare le pratiche di cybersicurezza in strumenti di sorveglianza persistenti e pervasivi. Infine, l'opacità e la complessità dei modelli di IA rappresentano una criticità significativa anche per la governance della cybersicurezza nella misura in cui le soluzioni basate su IA non saranno in grado di giustificare i risultati (dal rilevamento al processo decisionale) e renderli

²³ Modelli di IA addestrati su una determinata area geografica o su uno specifico gruppo di utenti (categorie professionali, gruppi demografici, genere) porteranno a una protezione inadeguata, alla penalizzazione di certi gruppi, a discriminazioni e disuguaglianze

comprensibili all'essere umano, soprattutto laddove le decisioni automatizzate abbiano conseguenze gravi, come l'attribuzione di un indice di rischio ai comportamenti degli utenti interni ai sistemi. Per questo, anche in questo ambito è cruciale sviluppare modelli spiegabili e affiancare l'automazione con la supervisione umana, per garantire trasparenza, equità e tutela dei diritti.

È difficile peraltro fare una stima a medio-lungo termine del perimetro e dell'impatto delle vulnerabilità dei componenti di IA. Si tratta di innovazioni emergenti, la ricerca e le applicazioni negli ultimi anni hanno compiuto progressi molto rapidi e quindi è ragionevole supporre che molte vulnerabilità siano sconosciute e i potenziali abusi debbano ancora essere esplorati. Le implicazioni per la cybersicurezza in questo campo sono ancora meno prevedibili che in altri contesti.

È opportuno anche in questo contesto richiamare i tre fattori per la diffusione di un'intelligenza artificiale affidabile (*trustworthy* AI) elaborati dal High-Level Expert Group on Artificial Intelligence nel 2019²⁴. (1) rispetto dell'articolato quadro normativo in materia; (2) garanzia dei principi e dei valori etici; (3) solidità dei sistemi AI da un punto di vista tecnico e sociale.

Dal punto di vista giuridico, la cybersicurezza dell'intelligenza artificiale, insieme ad accuratezza e robustezza, è disciplinata dal nuovo Regolamento (UE) 1689/2024, noto come AI Act, in particolare all'articolo 15. Nei considerando 75 e 76, il legislatore evidenzia che la robustezza tecnica rappresenta un requisito fondamentale affinché i sistemi di IA ad alto rischio possano resistere a comportamenti dannosi o indesiderati derivanti da errori, malfunzionamenti o situazioni impreviste. Allo stesso modo, la sicurezza informatica risulta essenziale per tutelare tali sistemi dagli attacchi di soggetti malintenzionati che cercano di sfruttarne le vulnerabilità. A tale proposito, si noti che sul piano della governance, la Legge 23 settembre 2025, n. 132, recante "Disposizioni e deleghe al Governo in materia di intelligenza artificiale", designa proprio l'Agenzia per la Cybersicurezza Nazionale (ACN) quale Autorità nazionale per vigilare – con poteri ispettivi – sull'adeguatezza e la sicurezza dei sistemi. Il coordinamento con altri strumenti normativi, come il Cyber Resilience Act, risulta essenziale infine per garantire un'architettura regolativa coerente e sinergica.

La possibilità di trarre reale beneficio dalle tecnologie di IA emergenti, per garantire un futuro digitale più sicuro, giusto e resiliente, dipenderà non solo dalla capacità delle organizzazioni sia pubbliche che private di fare progressi nelle ricerche su IA e cybersicurezza, nella loro applicazione e nello sviluppo

²⁴ I-HLEG, HIGH-LEVEL EXPERT GROUP ON ARTIFICIAL INTELLIGENCE, *Ethics Guidelines for Trustworthy AI*, European Commission, 2019.

delle competenze, ma anche dallo studio critico degli impatti di queste tecnologie sulle dimensioni giuridiche, sociale ed etica.

5. Un approccio armonizzato alla cybersicurezza

Nel quadro dinamico e incerto delineato dall'evoluzione delle minacce digitali, il concetto di cybersicurezza ha assunto una connotazione sempre più dinamica e ampia. La trasformazione digitale accelerata, l'emergere di nuove tecnologie come l'intelligenza artificiale e la crescente interconnessione tra ambienti fisici e virtuali impongono una revisione dei tradizionali paradigmi di sicurezza, sollecitando l'adozione di una prospettiva olistica, capace di integrare componenti tecniche, politiche, giuridiche, economiche e sociali. Le minacce non si limitano più a colpire sistemi informatici isolati, ma si estendono alla *supply chain*, agli ambienti cyberfisici e agli ecosistemi digitali emergenti, come il metaverso, in cui la manipolazione dei dati comportamentali, l'abuso dei sistemi di IA e la vulnerabilità dei dispositivi intelligenti rappresentano i nuovi vettori di rischio.

In questa prospettiva, la cybersicurezza si configura come un concetto stratificato e multidimensionale, articolato lungo tre livelli interconnessi: la dimensione fisica, relativa alle infrastrutture materiali come hardware, cavi e router; la dimensione logica, che attiene ai sistemi software, ai protocolli e alle architetture digitali; e infine la dimensione sociale e semantica, che riguarda l'interazione umana, le pratiche d'uso e le dinamiche comportamentali degli utenti. Tale articolazione impone un approccio multirischio, in grado di considerare non soltanto le minacce di natura tecnica e fisica, ma anche i fattori contestuali, organizzativi, sociali ed economici.

Si afferma così una concezione della cybersicurezza come infrastruttura di tutela degli interessi pubblici, strettamente connessa con le finalità proprie della sicurezza nazionale e della stabilità delle istituzioni democratiche²⁵. In questo quadro, particolare rilievo assumono tanto le strategie di cyberresilienza tecnico-economica quanto la diffusione capillare di una cultura della sicurezza informatica, intesa come prerequisito per la partecipazione consapevole alla vita civile in ambienti digitali.

L'eterogeneità dell'ecosistema digitale ha richiesto l'adozione di una prospettiva olistica, capace di cogliere la complessità dei livelli di interazione e delle interdipendenze che attraversano il cyberspazio. In tale direzione, la costruzione di un ambiente digitale sicuro non può limitarsi al potenziamento delle misure

²⁵ M. PIETRANGELI, *La dimensione plurale della cybersicurezza: da potere invisibile a processo collaborativo*, in *Rivista Italiana di Informatica e Diritto*, 2024 (2), pp. 13-24.

di difesa tecnologica, ma si fonda su un'integrazione efficace tra politiche pubbliche, pratiche sociali, processi formativi diffusi e responsabilità condivise, orientati a garantire la sostenibilità e la resilienza delle infrastrutture digitali nel lungo periodo.

Sulla necessità di investire nella formazione e nella sensibilizzazione insiste tanto la citata Strategia europea quanto la Strategia nazionale di cybersicurezza del nostro Paese che prevede interventi formativi a tutti i livelli: dai programmi scolastici e universitari alla formazione nelle pubbliche amministrazioni, fino allo sviluppo di un sistema di certificazione nazionale per valutare le conoscenze e le competenze in materia di cybersecurity e uno strumento di formazione e sensibilizzazione online rivolto al grande pubblico per l'autoverifica delle competenze acquisite²⁶.

In una società digitale, una cultura della cybersecurity dovrebbe essere imperativa.

In questa prospettiva, il giurista è chiamato ad assumere un ruolo attivo, partecipando alla definizione di standard, alla valutazione dei rischi e all'attuazione di misure che siano insieme efficaci e rispettose dei principi dello Stato di diritto. La governance della cybersicurezza, per essere davvero efficace, non può prescindere da questa competenza informatico giuridica diffusa, capace di integrare l'approccio tecnico con una visione critica, sistemica e orientata alla promozione del bene pubblico.

²⁶ Molteplici iniziative di formazione e educazione sono esito del già citato paternariato SERICS. Si veda, in particolare, Th. CASADEI, V. BARONE, B. ROSSI (a cura di), *Giovani in rete. Guida per un uso consapevole delle tecnologie*, Torino: Giappichelli 2025.

II DIRITTO UE DELLA CYBERSICUREZZA: IL QUADRO NORMATIVO

*Pier Giorgio Chiara**

SOMMARIO: 1. Introduzione. 2. La Cybersicurezza delle reti e dei sistemi informativi: le Direttive NIS e NIS2. 3. *Segue*: la Cybersicurezza nel settore finanziario: il Regolamento DORA. 4. Il Quadro Europeo di Certificazione della Cybersicurezza: il Cybersecurity Act. 5. La Cybersicurezza dei prodotti con elementi digitali: il Cyber Resilience Act. 6. Solidarietà nella cybersicurezza: il Cyber Solidarity Act. 7. Riflessioni conclusive.

1. Introduzione

Il progressivo processo di digitalizzazione – per diversi studiosi una vera e propria “rivoluzione”¹ – ha ormai raggiunto le infrastrutture di ogni ambito e settore della società, dai trasporti all’energia ed alla sanità, passando per le telecomunicazioni, la finanza, lo spazio e la difesa. I soggetti che operano in questi settori, pubblici e privati, fanno affidamento su reti, sistemi informatici, sistemi informativi e dispositivi mobili sempre più (inter)connessi. In tal senso si assiste alla progressiva integrazione tra la dimensione digitale e la dimensione fisica, rendendo sempre più complesso operare tra queste distinzioni nette. Un esempio paradigmatico di ciò è dato dal c.d. “Internet delle cose” o *Internet of Things* (IoT)², ossia dispositivi connessi alla rete internet che interagiscono continuamente con la realtà fisica, attraverso sistemi di sensori e attuatori (secondo l’associazione internazionale del settore telco GSMA saranno nel pianeta 25 miliardi entro il 2025)³.

* Questo lavoro è stato sviluppato nell’ambito del progetto SERICS (PE00000014) under the MUR National Recovery and Resilience Plan funded by the European Union – NextGenerationEU.

¹ *Ex multis*, si veda L. FLORIDI, *La quarta rivoluzione: come l’infosfera sta trasformando il mondo*, Milano: Raffaello Cortina, 2020.

² A. RAYES, S. SALAM, *Internet of Things From Hype to Reality*, Cham: Springer Nature 2019. Si veda inoltre L. DENARDIS, *Internet in ogni cosa - Libertà, sicurezza e privacy nell’era degli oggetti iperconnessi*, Roma: Luiss University, 2021.

³ GSMA, *The Internet of Things by 2025*, 2019, <https://www.gsma.com/iot/wp-content/uploads/2018/08/GSMA-IoT-Infographic-2019.pdf>.

Questo cambiamento porta con sé innegabili benefici ed opportunità; d'altra parte, la compenetrazione della dimensione digitale nella dimensione fisica determina inevitabilmente un aumento delle vulnerabilità ad attacchi ed incidenti informatici. Il panorama delle minacce, in progressivo aumento da un punto di vista quantitativo e miglioramento da un punto di vista qualitativo, è costantemente in evoluzione⁴. Un attacco alla catena di approvvigionamento può causare danni significativi imprevedibili per una moltitudine di soggetti, privati e non; attacchi informatici sempre più sofisticati possono paralizzare le infrastrutture critiche di un paese, ma potrebbero anche portare a violazioni dei dati con gravi ripercussioni sulla protezione dei dati personali degli individui e, eventualmente, su altri diritti fondamentali (es., libertà di espressione).

In questo contesto, negli anni recenti, il concetto di “sicurezza informatica” o “cybersicurezza” è stato continuamente ri-definito, a livello nazionale, sovranazionale (es, UE) e internazionale (es, ONU). Nato dal termine *cyber space*⁵, il termine *cybersecurity* viene comunemente utilizzato da professionisti IT, consulenti, lobbisti e politici per affrontare i problemi di sicurezza nello spazio cibernetico. I tradizionali concetti cardine della sicurezza informatica quali *computer*⁶ e *information security*⁷ rappresentano ormai due sottoinsiemi della più ampia concezione di cybersicurezza che amplia il perimetro dei rischi, dei beni di protezione

⁴ L'Agenzia dell'Unione europea per la cybersicurezza (ENISA), stabilita ad Atene nel 2004 dal regolamento (CE) n. 460/2004, pubblica ogni anno dei report al fine di approfondire lo stato dell'arte della minaccia informatica (*threat landscapes*): a tal fine, vengono identificati le principali tendenze evolutive, gli attori in gioco e le loro motivazioni, le principali tecniche di attacco nonché le misure di mitigazione più efficaci. Si veda ENISA, *ENISA Threat Landscape 2024*, <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024>.

⁵ Il termine “cibernetico” è stato sviluppato nel libro di N. WIENER, *Cybernetics or Control and Communication in the Animal and the Machine*, Cambridge, Mass.: MIT Press, 1948, ed utilizzato in riferimento al controllo di sistemi complessi nel mondo animale e nelle reti meccaniche, in particolare ai sistemi di controllo autoregolanti.

⁶ Indica la protezione fornita ad un sistema informativo allo scopo di ottenere la conservazione della confidenzialità (l'accesso all'informazione risulta disponibile nei modi e nei tempi previsti alle persone che possono e devono fruirne), dell'integrità (garanzia che le informazioni non possano essere modificate o cancellate per azioni non autorizzate, volontarie o involontarie, ma anche per danni o malfunzionamenti dei sistemi), della disponibilità (garanzia che i dati e le risorse siano preservati dal possibile utilizzo o accesso da parte di soggetti non autorizzati) – c.d. triade CIA, RID in italiano – delle risorse del sistema informativo stesso (includendo hardware, software, firmware, dati e sistemi di telecomunicazione). Si veda la pubblicazione dell'agenzia governativa US NIST, *NIST SP 800-14*.

⁷ Concezione della sicurezza informatica maggiormente orientata alla protezione delle informazioni e dei dati. La triade della *computer security* si completa con ulteriori obiettivi di sicurezza: la non ripudiabilità e l'autenticità e, infine, i principi di *accountability* (responsabilità) e di *auditability* (verificabilità).

e degli attori coinvolti⁸. Limitare il concetto di sicurezza informatica alla sola protezione dei sistemi informativi ed informatici è ormai anacronistico, dal momento che il contesto operativo della sicurezza deve prendere in considerazione non solo fattori tecnici connessi ad un computer o alla rete internet, ma anche non-tecnici (giuridici, geopolitici, etc.).

In tal senso, cybersicurezza risulta essere un concetto operativo e funzionale che sfugge a definizioni precise. Così, i comitati europei di normazione CEN e CENELEC concludono come non sia necessaria una definizione di cybersicurezza in senso stretto, considerata l'ampiezza dell'ambito che questa identifica, ma che piuttosto siano rilevanti delle definizioni contestuali⁹. Ciò non di meno, è opportuno sottolineare come nel diritto dell'Unione europea esista dal 2019 una definizione puntuale di cybersicurezza, enucleata nel Regolamento (UE) 2019/881¹⁰ (c.d. *Cybersecurity Act*, si veda la sezione 3): l'insieme delle attività necessarie per proteggere la rete e i sistemi informativi, gli utenti di tali sistemi e altre persone interessate dalle minacce informatiche¹¹.

Da questione puramente tecnica, la cybersicurezza ha acquisito progressivamente rilevanza sociale, strategica e giuridica, diventando un obiettivo primario delle politiche dell'Unione europea e dei singoli Stati membri. Sul fronte unionale, è opportuno sottolineare come i Trattati dell'UE non conferiscano all'Unione una competenza esplicita a regolamentare in materia, sulla base del principio di attribuzione, i cui criteri sono stabiliti nell'articolo 5 del Trattato sull'UE (TUE)¹². Di conseguenza, non esiste a livello di diritto primario dell'UE una base giuridica autonoma per la politica dell'Unione nell'ambito della cybersicurezza.

Questo capitolo si propone pertanto di illustrare il quadro normativo dell'Unione europea in materia di cybersicurezza, mettendo in luce altresì le principali sfide normative sottese all'attuazione degli atti giuridici rilevanti. A tal fine, verrà evidenziato come le diverse strategie in materia di cybersicurezza dell'UE abbiano guidato l'evoluzione del quadro normativo e come il perimetro concettuale ed applicativo del concetto di cybersicurezza sia nel tempo cambiato.

⁸ R. BRIGHI, P.G. CHIARA, *Cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto dell'Unione Europea*, in *Federalismi*, 2021 (21), pp. 18-19.

⁹ CEN/CENELEC, CYBER SECURITY FOCUS GROUP, *Rec#2 – Definition of Cybersecurity*, 2020, p. 38, <https://2020.standict.eu/sites/default/files/CybersecurityDefinition%20v1.1.pdf>.

¹⁰ Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019 relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cibersicurezza»), GU L 151 del 7.6.2019, pagg. 1-55.

¹¹ Art. 2, par. 1, *Cybersecurity Act*.

¹² In base al principio di attribuzione, l'Unione agisce solo nei limiti delle competenze che le sono state conferite dagli Stati membri nei trattati per conseguire gli obiettivi in essi indicati.

2. La cybersicurezza delle reti e dei sistemi informativi: le direttive NIS e NIS2

Il tema della sicurezza in ambito digitale inizia ad acquisire rilevanza normativa a livello comunitario e nazionale tra gli anni '80 e '90. Sul finire degli anni '90, si osservano tre grandi cambiamenti sul piano politico, sociale e tecnico: la globalizzazione; la liberalizzazione e la convergenza. Già all'alba del nuovo millennio, larga parte delle comunicazioni di rete risulta transfrontaliera e la maggior parte delle reti è costituita da prodotti commerciali di imprese o gruppi internazionali e multinazionali. Inoltre, la proprietà e la gestione di tali reti sono affidate in prevalenza a soggetti privati: in questo contesto, la sicurezza diventa un aspetto dell'offerta del mercato. Infine, le reti di comunicazione sono sempre più interconnesse tra loro, veicolano lo stesso tipo di servizi permanenti e personalizzati e condividono, in una certa misura, le stesse infrastrutture.

Lo spiegamento congiunto di questi tre fenomeni, in materia di sicurezza delle reti e dei sistemi informativi, rese evidente l'inefficacia di una regolamentazione nazionale a fronte di una politica di armonizzazione a livello comunitario. Pertanto, la necessità da parte dell'allora Comunità europea di dotarsi di un quadro normativo comunitario adeguato e unitario in materia di sicurezza delle reti e dei sistemi informativi venne avvertita come urgenza pressante¹³. Inizialmente, infatti, la regolazione in materia appariva frammentata tra diversi quadri normativi, in particolare in materia di telecomunicazioni¹⁴, protezione dei dati personali¹⁵ e contrasto al crimine informatico¹⁶. Le necessarie misure strategiche in materia di sicurezza delle reti e dell'informazione sarebbero state complementari ai più maturi quadri normativi sopra citati¹⁷.

Ulteriore elemento catalizzatore per una politica comunitaria di sicurezza delle reti e dei sistemi informativi è stato il cambio paradigmatico della minaccia

¹³ Commissione europea, *Sicurezza delle reti e sicurezza dell'informazione: proposta di un approccio strategico europeo*, COM(2001), 298 final.

¹⁴ Direttiva 90/387/CEE del Consiglio, del 28 giugno 1990, sull'istituzione del mercato interno per i servizi delle telecomunicazioni mediante la realizzazione della fornitura di una rete aperta di telecomunicazioni (Open Network Provision - ONP), GU L 192 del 24.7.1990, pagg. 1-9; Direttiva 90/388/CEE della Commissione, del 28 giugno 1990, relativa alla concorrenza nei mercati dei servizi di telecomunicazioni, GU L 192 del 24.07.1990, pagg. 10-16.

¹⁵ Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, GU L 281 del 23.11.1995, pagg. 31 - 50; Direttiva 97/66/CE del Parlamento europeo e del Consiglio del 15 dicembre 1997 sul trattamento dei dati personali e sulla tutela della vita privata nel settore delle telecomunicazioni, GU L 24 del 30.1.1998, pagg. 1-8.

¹⁶ Si veda ad esempio la L. n. 547/1993 del 30 dicembre 1993. È invece del 2001 la c.d. Convenzione di Budapest sulla criminalità informatica, ratificata in Italia nel 2008.

¹⁷ Commissione europea, *Sicurezza delle reti e sicurezza dell'informazione: proposta di un approccio strategico europeo*, cit., p. 3.

cibernetica, conseguenza della progressiva digitalizzazione delle infrastrutture non solo di mercato ma anche degli apparati statali. All'inizio degli anni 2000 iniziano a registrarsi significativi attacchi informatici coordinati alle infrastrutture critiche di Stati. Uno degli esempi più eclatanti – per magnitudine e coordinamento – fu l'attacco subito dall'Estonia nel 2007. Come conseguenza, l'Estonia è stato il primo Stato membro dell'UE ad adottare una strategia nazionale volta a mitigare i rischi di cybersicurezza¹⁸.

In questo contesto, nel 2013 viene adottata la prima Strategia dell'Unione europea in materia di cybersicurezza. La Strategia si conforma ad un approccio *multi-stakeholder*, vista la necessità di coordinare risposte efficaci tra l'UE, gli Stati Membri, le imprese e i cittadini al fine di rafforzare la cybersicurezza¹⁹. La cybersicurezza diventa pertanto una politica dell'Unione e il termine *cybersecurity* entra così ufficialmente a far parte del linguaggio istituzionale dell'Unione. Da un punto di vista definitorio, la Strategia riconosce alla cybersicurezza un perimetro operativo potenzialmente ampio, dal momento che questa si riferirebbe «alle precauzioni e agli interventi che si possono prendere per proteggere il ciberdominio, in campo sia civile che militare»²⁰. Dall'altra, gli obiettivi della cybersicurezza sono ancora saldamente legati ai paradigmi dell'*information security*: «la cybersicurezza si propone di salvaguardare la disponibilità e l'integrità delle reti e dell'infrastruttura e la riservatezza delle informazioni che esse contengono»²¹.

Ad un alto livello, la Strategia delinea un quadro articolato di interventi specifici che comprendono una serie di strumenti giuridici e di investimenti che coinvolgono attori a diversi livelli (istituzioni UE; Stati membri e operatori del settore privato). Sono cinque le priorità strategiche individuate: 1) raggiungere la cyber resilienza; 2) il contrasto al cybercrimine²²; 3) sviluppare una politica e capacità di cyberdifesa²³; 4) sviluppare risorse industriali e tecnologiche per la cybersicurezza; 5) creare una politica internazionale dell'UE sul cyberspazio.

¹⁸ Estonia – Ministero della Difesa, *Cyber Security Strategy*, 2008.

¹⁹ Commissione europea e Alto Rappresentante dell'UE per gli Affari Esteri e la Politica di Sicurezza, *Strategia dell'Unione europea per la cybersicurezza: un ciber spazio aperto e sicuro*, JOIN, 2013, 1 final, p. 4.

²⁰ *Ibid.*, p. 3.

²¹ *Ibid.*

²² Per cybercrimine la Commissione intende generalmente l'ampia gamma di attività criminali in cui i sistemi informatici costituiscono l'arma primaria oppure il bersaglio. «Il cybercrimine comprende reati tradizionali (ad es. frode, contraffazione o furto di identità), reati connessi ai contenuti (ad es. distribuzione in linea di materiale pedopornografico o incitamento all'odio razziale) e reati peculiari ai sistemi informatici e ai sistemi informativi (ad es. attacchi contro i sistemi informativi, rifiuto di servizio o software maligni (malware)» (*ibid.*, p. 3).

²³ La cyberdifesa, invece, è intesa dalla Commissione quale lo sviluppo di una politica e capacità in termini di preparazione, rilevamento e risposta, connesse al quadro della Politica di sicu-

In questa sezione ci concentreremo prevalentemente sulle misure legislative che hanno implementato la prima area d'azione della Strategia. La direttiva (UE) 2016/1148 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (c.d. direttiva NIS) è considerata il primo atto giuridico dell'Unione sulla cybersicurezza in senso stretto. Come già ricordato, dal momento che non vi è una competenza esplicita nei Trattati che permetta all'UE di adottare misure di cybersicurezza, l'articolo 114 TFUE è stato scelto come base giuridica per la direttiva NIS, avente per oggetto il ravvicinamento delle disposizioni legislative degli Stati membri concernenti l'instaurazione e il funzionamento del mercato interno. Coerentemente con questa scelta, la direttiva NIS parte, pertanto, dall'assunto che la sicurezza e l'affidabilità delle reti, dei sistemi e dei servizi informativi sia innanzitutto necessaria «per le attività economiche e sociali e in particolare ai fini del funzionamento del mercato interno»²⁴.

Anche se la direttiva NIS è stata abrogata dalla cd. direttiva NIS2 a partire dall'ottobre 2024, è importante illustrare, seppur brevemente, gli istituti principali dello strumento del 2016 per capire la *ratio* delle scelte fatte dal legislatore UE nel processo di revisione. In primo luogo, la direttiva NIS imponeva agli Stati membri di dotarsi di una strategia nazionale in materia di sicurezza della rete e dei sistemi informativi che definisse obiettivi e interventi strategici concreti da attuare²⁵. Inoltre, gli Stati avevano l'obbligo di designare autorità nazionali competenti, punti di contatto unici e gruppi di intervento per la sicurezza informatica in caso di incidente ("CSIRT")²⁶. Al fine poi di promuovere e sostenere la cooperazione strategica e lo scambio di informazioni tra Stati membri, nell'interesse comune di conseguire un livello elevato di cybersicurezza, la direttiva istituiva un gruppo di cooperazione composto da rappresentanti degli Stati, della Commissione e dell'ENISA²⁷, nonché una rete pan-europea dei CSIRT degli Stati membri, con il segretariato dell'ENISA²⁸.

rezza e di difesa comune (PSDC), a supporto pertanto di interessi inerenti alla sicurezza nazionale. Non è sempre facile operare, nella pratica, una distinzione tra le azioni che rientrano sotto la seconda e terza priorità strategica. Sul punto si veda J. ODERMATT, *The European Union as a cybersecurity actor*, in S. BLOCKMANS, P. KOUTRAKOS (a cura di), *Research Handbook on EU Common Foreign and Security Policy*, Cheltenham: Edward Elgar Publishing, 2018, p. 361.

²⁴ Considerando 1, Direttiva NIS.

²⁵ Art. 1, par. 2, lett. a; Art. 7, Direttiva NIS.

²⁶ Art. 1, par. 2, lett. e; Art. 8; Art. 9, Direttiva NIS.

²⁷ Art. 11, Direttiva NIS.

²⁸ Art. 12, Direttiva NIS.

In secondo luogo, la direttiva stabiliva obblighi di sicurezza²⁹ e di notifica³⁰ per due categorie di soggetti, gli operatori di servizi essenziali (OSE) e i fornitori di servizi digitali (FSD). I primi erano identificati dagli Stati membri tra i soggetti eroganti servizi essenziali per il mantenimento di attività sociali ed economiche fondamentali in 7 settori (energia, trasporti, bancario, infrastrutture dei mercati finanziari, sanitario, fornitura e distribuzione di acqua potabile, infrastrutture digitali)³¹, a condizione che rispettassero diversi criteri³². I secondi invece erano direttamente identificati dall'Allegato III: sarebbero stati ricompresi nell'ambito di applicazione della NIS tutti i fornitori di servizi di i) mercato online, ii) motore di ricerca online e iii) cloud computing.

Per altro verso, la direttiva NIS, pur lasciando un ampio margine agli Stati membri nella scelta delle misure di *enforcement*, differenziava il regime applicabile agli OSE e ai FSD: mentre le autorità competenti avrebbero potuto richiedere ai primi di fornire i) informazioni necessarie per valutare la sicurezza delle loro reti e sistemi; e ii) la prova dell'effettiva attuazione delle politiche di sicurezza³³, nei confronti dei secondi avrebbero adottato misure di vigilanza solo quando avessero ottenuto la prova di non conformità di un fornitore (*ex post*)³⁴. Infine, ogni aspetto inerente alle norme relative alle sanzioni da irrogare in caso di violazione delle disposizioni NIS era lasciato all'apprezzabilità dei legislatori nazionali³⁵.

Nonostante la direttiva NIS abbia aperto la strada a un significativo cambiamento di mentalità per i soggetti privati rientranti nel perimetro in parola, nonché di approccio regolamentare e istituzionale alla cybersicurezza in molti Stati membri, questa ha sin da subito mostrato diversi e significativi limiti³⁶. L'ambito di applicazione è parso indebitamente circoscritto; connesso a ciò, le regole rivolte agli Stati membri per l'identificazione degli OSE sono state giudicate poco chiare. Un'eccessiva frammentazione del quadro normativo è derivata anche dalla diversità di implementazione tra gli atti di recepimento nazionale delle regole in materia di misure di sicurezza e di notifica degli incidenti. Il re-

²⁹ Operatori e fornitori adottano misure tecniche e organizzative adeguate e proporzionate alla gestione dei rischi posti alla sicurezza delle reti e dei sistemi informativi che usano nelle loro operazioni (Art. 14, par. 1) e nel contesto dell'offerta di servizi (Art. 16, par. 1).

³⁰ Operatori e fornitori notificano senza indebito ritardo all'autorità competente o al CSIRT qualsiasi incidente avente un impatto rilevante sulla continuità dei servizi essenziali prestati (Art. 14, par. 3) e sulla fornitura di un servizio (Art. 16, par. 3).

³¹ Allegato II, Direttiva NIS.

³² Art. 5, par. 2, Direttiva NIS.

³³ Art. 15 Direttiva NIS.

³⁴ Art. 17 Direttiva NIS.

³⁵ Art. 21 Direttiva NIS.

³⁶ COMMISSIONE EUROPEA, *Study to support the review of the NIS Directive – Executive Summary*, 2021, <https://data.europa.eu/doi/10.2759/334751>.

gime di supervisione ed *enforcement* è stato giudicato inefficace alla luce della riluttanza delle autorità competenti a comminare sanzioni. Gli Stati membri hanno dimostrato un diverso grado di maturità e preparazione. Infine, la pressoché totale mancanza di condivisione delle informazioni rilevanti tra gli Stati, a detrimento di una consapevolezza situazionale comune a livello UE, è stata l'ultimo problema sistemico individuato³⁷.

Pertanto, nel dicembre 2020 la Commissione ha proposto una nuova direttiva NIS (c.d. NIS2) che abrogasse la precedente, insieme con un disegno di revisione della legislazione in materia di resilienza dei soggetti critici³⁸. La proposta di questo nuovo atto giuridico è da inquadrarsi nel contesto della terza Strategia dell'UE per la cybersicurezza³⁹, pubblicata non a caso contestualmente con la revisione del primo strumento di diritto dell'Unione in materia di cybersicurezza *stricto sensu*. In linea di continuità con le precedenti Strategie, il nuovo documento programmatico contiene un quadro di proposte a livello normativo, di investimento e politico, per tre macrosettori di intervento: i) resilienza, sovranità tecnologica e leadership; ii) sviluppo delle capacità operative volte alla prevenzione, alla dissuasione e alla risposta; e, iii) promozione di un ciberspazio globale e aperto.

La direttiva (UE) 2022/2555 (c.d. "NIS2"), in vigore dal 16 gennaio 2023 e applicabile dal 17 ottobre 2024⁴⁰, si propone di aumentare il livello di "cyber resilienza" di tutti i settori, pubblici e privati, che svolgono una funzione essenziale per l'economia e la società. La prima grande differenza con la precedente direttiva riguarda l'ambito di applicazione. La distinzione tra OSE e FSD è sostituita con una classificazione tra soggetti "essenziali" ed "importanti", che tiene conto del livello di criticità del settore o del tipo di servizio fornito, nonché del livello di dipendenza da altri settori o servizi. Per garantire una maggiore armonizzazione, ed eliminare pertanto le divergenze tra gli Stati nell'identificazione dei soggetti, la direttiva introduce un criterio quantitativo⁴¹: la NIS2 si applica a

³⁷ Commissione europea, *Proposta di DIRETTIVA DEL PARLAMENTO EUROPEO E DEL CONSIGLIO relativa a misure per un livello comune elevato di cybersicurezza nell'Unione, che abroga la direttiva (UE) 2016/1148* COM(2020) 823 final, p. 4.

³⁸ Commissione europea, *Proposta di DIRETTIVA DEL PARLAMENTO EUROPEO E DEL CONSIGLIO sulla resilienza dei soggetti critici*, COM(2020) 829 final. Poi pubblicata in Gazzetta Ufficiale dell'UE il 14 dicembre 2022 come Direttiva (UE) 2022/2557, la c.d. 'direttiva CER' (*critical entities resilience*) stabilisce obblighi per gli Stati membri e i soggetti critici volti a rafforzare la loro resilienza e la loro capacità di fornire servizi essenziali per il mantenimento di funzioni vitali della società o di attività economiche. Occorre sottolineare come tale direttiva non si applichi alla materia disciplinata dalla NIS2, e cioè la cybersicurezza (Art. 1, par. 2, Direttiva CER).

³⁹ Commissione europea e Alto Rappresentante dell'UE per gli Affari Esteri e la Politica di Sicurezza, *La strategia dell'UE in materia di cybersicurezza per il decennio digitale*, JOIN(2020), 18 final.

⁴⁰ In Italia è stata recepita dal d. lgs. 138/2024.

⁴¹ Art. 2, par. 1, Direttiva NIS2.

tutte le medie e grandi imprese che operano nei settori individuati dagli Allegati I (settori ad alta criticità)⁴² e II (altri settori critici)⁴³. Sono previste poi eccezioni per le quali determinati soggetti, indipendentemente dalle loro dimensioni, dovranno essere conformi alle disposizioni della direttiva⁴⁴.

Sotto il profilo della governance, la NIS2 opera sulla falsa riga della direttiva del 2016 – prevedendo, cioè, che gli Stati membri adottino delle strategie nazionali per la cybersicurezza, designino autorità competenti e punti di contatto unici nonché uno o più CSIRT. Rispetto alla precedente, tuttavia, entra in un maggior grado di dettaglio per quanto riguarda, ad esempio, le misure strategiche che gli Stati devono adottare nell’ambito delle strategie nazionali o, ancora, i requisiti, le capacità tecniche e i compiti dei CSIRT⁴⁵. Le novità invece sono rappresentate, da una parte, dall’obbligo per gli Stati membri di dotarsi di quadri nazionali di gestione delle crisi di cybersicurezza su vasta scala, nell’ambito dei quali devono designare una autorità competente e un piano nazionale di risposta⁴⁶ e, dall’altra, dalla divulgazione coordinata delle vulnerabilità, facente perno sui CSIRT quali intermediari tra l’entità notificante e il fabbricante interessato⁴⁷. In questo contesto è elaborata e gestita dall’ENISA una banca dati europea delle vulnerabilità note comprendente le relative *patch*.

Anche la cooperazione – altro punto dolente della precedente direttiva – risulta rafforzata, sia a livello nazionale (tra i diversi organismi di governance della cybersicurezza, vale a dire autorità competenti, punti di contatto unici e CSIRT) che a livello dell’Unione, ed internazionale. Ai preesistenti gruppi di cooperazione⁴⁸ e rete di CSIRT, si affianca la nuova rete europea delle organizzazioni di collegamento per le crisi informatiche (EU-CyCLONE), istituita al fine di sostenere la gestione coordinata a livello operativo degli incidenti e delle crisi di cybersicurezza su vasta scala e di garantire il regolare scambio di infor-

⁴² I settori considerati sono: energetico, bancario, trasporti, infrastrutture digitali, mercati finanziari, sanitario, acqua potabile, acque reflue, pubblica amministrazione, spazio e gestione dei servizi TIC.

⁴³ I settori considerati sono: servizi postali e di corriere; gestione dei rifiuti; produzione, trasformazione e distribuzione di alimenti; fabbricazione, produzione e distribuzione di sostanze chimiche; fabbricazione; fornitori di servizi digitali e ricerca.

⁴⁴ Art. 2, par. 2, 3, 4, Direttiva NIS2.

⁴⁵ Art. 11, Direttiva NIS2.

⁴⁶ Art. 9, Direttiva NIS2.

⁴⁷ Art. 12, Direttiva NIS2.

⁴⁸ Nuovo compito del gruppo di cooperazione è stabilire la metodologia e gli aspetti organizzativi delle revisioni tra pari di cui all’Art. 19 aventi l’obiettivo di trarre insegnamenti dalle esperienze condivise, rafforzare la fiducia reciproca, conseguire un livello comune elevato di cybersicurezza e migliorare le capacità e le politiche di cybersicurezza degli Stati membri.

mazioni pertinenti tra gli Stati membri e le istituzioni e gli organismi dell'Unione⁴⁹.

Un'ulteriore riforma significativa ha investito i quadri di misure di gestione del rischio di cybersicurezza e la procedura di notifica degli incidenti, attraverso requisiti più stringenti e procedure più dettagliate. Sotto il primo profilo, tutti i soggetti a cui si applica la NIS2 devono adottare misure tecniche, operative e organizzative adeguate e proporzionate ai rischi contenute in un elenco minimo, non esaustivo⁵⁰. Il riferimento esplicito ai criteri dell'adeguatezza e della proporzionalità cui i soggetti NIS devono conformarsi nell'implementazione delle misure di gestione del rischio evidenzia chiaramente come anche la direttiva NIS2 si basi sul c.d. approccio al rischio, coerentemente con la recente legislazione UE in materia digitale⁵¹. I soggetti dovranno pertanto valutare *in concreto* la proporzionalità delle singole misure tenendo conto del grado di esposizione dell'ente ai rischi, delle sue dimensioni e della probabilità che si verifichino incidenti e della loro gravità, compreso il loro impatto sociale ed economico, adottando un approccio "multi-rischio" (che tenga, cioè, in considerazione anche i rischi fisici e ambientali es., furti, incendi, interruzioni di corrente, ecc.). Inoltre, dovranno essere tenuti in considerazione lo stato dell'arte, nonché la possibilità di applicare standard tecnici europei (norme tecniche armonizzate europee sviluppate da ETSI, CEN e CENELEC) o internazionali (ad esempio, ISO/IEC).

Per quanto riguarda invece gli obblighi di segnalazione degli incidenti, il nuovo quadro procedurale della NIS2 risulta più dettagliato⁵². Sono specificati i criteri in base ai quali un incidente è considerato "significativo" e quindi soggetto all'obbligo di notifica alle autorità competenti o ai CSIRT nazionali. Inoltre, la notifica è suddivisa in fasi progressive con termini diversi: un preallarme entro 24 ore da quando il soggetto viene a conoscenza dell'incidente; la notifica entro 72 ore dal momento in cui il soggetto viene a conoscenza dell'incidente; una relazione intermedia su richiesta dell'autorità; e una relazione finale entro un mese dalla notifica. Un nuovo obbligo per i soggetti NIS consiste nella comunicazione ai destinatari dei loro servizi potenzialmente interessati da una minaccia informatica significativa qualsiasi misura o rimedio in risposta a tale mi-

⁴⁹ Art. 16, Direttiva NIS2.

⁵⁰ Art. 21 e 22, Direttiva NIS2. Queste includono, ad esempio, politiche di analisi dei rischi; gestione degli incidenti; continuità operativa (come la gestione del backup e il ripristino in caso di disastro) e gestione delle crisi; sicurezza della catena di approvvigionamento; ecc.

⁵¹ G. DE GREGORIO, P. DUNN, *The European Risk-Based Approaches: Connecting Constitutional Dots in the Digital Age*, in *Common Market Law Review*, 2022 (59/2).

⁵² Art. 23, Direttiva NIS2.

naccia⁵³. Tale disposizione riflette un approccio proattivo alle minacce informatiche che è una componente vitale della gestione del rischio di *cybersecurity*.

Nell'ottica di risolvere la debolezza strutturale della direttiva NIS in tema di condivisione delle informazioni, come visto, la NIS2 istituisce da una parte delle procedure per la creazione di accordi volontari di condivisione di informazioni pertinenti alla cybersicurezza⁵⁴. Dall'altra, è prevista la possibilità per i soggetti NIS (nonché ai soggetti esclusi dall'applicazione della NIS2) di notificare volontariamente alle autorità nazionali incidenti (che non siano significativi, nel caso dei soggetti NIS), minacce informatiche e quasi-incidenti⁵⁵.

Infine, ulteriore elemento di discontinuità col passato è dato dalle novità in materia di vigilanza ed esecuzione. La NIS2 rafforza i poteri di *enforcement* delle autorità competenti attraverso un elenco minimo di compiti e poteri per garantire l'effettivo rispetto della normativa⁵⁶. Anche il regime sanzionatorio riduce il margine di discrezionalità lasciato dalla precedente direttiva agli Stati membri adottando l'approccio scalare dell'articolo 83 GDPR: violazioni più gravi andranno in conto a sanzioni amministrative pecuniarie più pesanti⁵⁷.

3. *Segue: la cybersicurezza nel settore finanziario: il regolamento DORA*

Il 14 dicembre 2022, insieme con la direttiva NIS2 e la direttiva CER, viene pubblicato nella G.U. dell'Unione anche il regolamento (UE) 2022/2554 relativo alla resilienza operativa digitale per il settore finanziario (c.d. DORA, dall'inglese *digital operational resilience act*)⁵⁸. Il DORA è da considerarsi atto giuridico settoriale rispetto alla NIS2 (che invece pone misure orizzontali) per quanto riguarda i soggetti del settore finanziario⁵⁹.

Brevemente, il DORA mira ad armonizzare gli obblighi in materia di resilienza operativa digitale per tutte le entità finanziarie, superando il duplice pro-

⁵³ Art. 23, par. 2, Direttiva NIS2.

⁵⁴ Art. 29, Direttiva NIS2.

⁵⁵ Art. 30, Direttiva NIS2.

⁵⁶ Art. 31 – 33, Direttiva NIS2. Ai soggetti importanti si applicherà un regime di vigilanza “più leggero”, consistente cioè in un approccio alla vigilanza ex-post, che ricorda per certi aspetti il c.d. approccio “leggero” accordato ai fornitori di servizi digitali nell'ambito della direttiva NIS.

⁵⁷ Art. 34, Direttiva NIS2. Circa l'approccio regolatorio della Commissione facente perno sulla mimesi degli istituti del GDPR per altre normative digitali dell'UE si veda V. PAKONSTANTINOU, P. DE HERT, *The Regulation of Digital Technologies in the EU: Act-ification, GDPR Mimesis and EU Law Brutality at Play*, Abingdon: Routledge, 2024.

⁵⁸ Regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014, (UE) n. 909/2014 e (UE) 2016/1011, GU L 333 del 27.12.2022, pp. 1–7.

⁵⁹ Considerando 28, Direttiva NIS2; considerando 16, DORA.

blema rappresentato, da una parte, dalle disomogeneità legislative a livello nazionale e dall'altra dalla frammentazione dei requisiti in materia di rischi informatici, con conseguente nocumento del funzionamento del mercato dei servizi finanziari.

Ad un alto livello, gli obblighi e i requisiti armonizzati dal DORA poggiano su cinque pilastri che, nel complesso, determinano la modalità di declinazione da parte del regolamento del c.d. “approccio al rischio”: i) gestione dei rischi informatici; ii) gestione, classificazione e segnalazione degli incidenti informatici; iii) test di resilienza operativa digitale; iv) gestione dei rischi informatici derivanti da terzi; v) meccanismi di condivisione delle informazioni.

Per quanto riguarda il primo pilastro, le entità finanziarie devono predisporre un quadro di gestione e di controllo interno dei rischi informatici – dietro approvazione dell'organo di gestione dell'entità che si assume la responsabilità finale per la gestione di tali rischi – al fine di acquisire un livello elevato di resilienza operativa digitale⁶⁰. A tal riguardo, la resilienza operativa digitale è definita dal regolamento come «la capacità dell'entità finanziaria di costruire, assicurare e riesaminare la propria integrità e affidabilità operativa, garantendo, direttamente o indirettamente tramite il ricorso ai servizi offerti da fornitori terzi di servizi TIC, l'intera gamma delle capacità connesse alle TIC necessarie per garantire la sicurezza dei sistemi informatici e di rete utilizzati dall'entità finanziaria, su cui si fondano la costante offerta dei servizi finanziari e la loro qualità, anche in occasione di perturbazioni»⁶¹.

Adottando un approccio “olistico” alla gestione del rischio, il quadro di gestione sopra menzionato ricomprende non solo il piano operativo (tecnologie per l'informazione e la comunicazione – *infra*, TIC – necessarie per proteggere tutti i patrimoni informativi e risorse, compresi software, hardware e server) ma anche quello organizzativo (strategie, politiche, procedure e protocolli). Connesso a ciò, i quadri di gestione dei rischi informatici adottati dalle entità finanziarie devono soddisfare gli obiettivi posti dalle funzioni classiche in materia di gestione del rischio: identificazione; protezione e prevenzione; individuazione, risposta e ripristino; apprendimento; evoluzione e comunicazione. Il regolamento prevede infine un quadro di gestione semplificato per alcuni soggetti, contenuti in un elenco tassativo secondo vari criteri (ad es., la grandezza del soggetto)⁶².

Le entità finanziarie, poi, devono definire e attuare politiche e meccanismi specifici per il trattamento di tutti gli incidenti connessi alle TIC e per la segna-

⁶⁰ Art. 5, DORA.

⁶¹ Art. 3, punto 1, DORA.

⁶² Art. 16, DORA.

lazione degli incidenti più gravi connessi alle TIC all'autorità competente ex Art. 46. Se il DORA prevede tre step progressivi (notifica iniziale, relazione intermedia e relazione finale) che ricalcano i tre passaggi della segnalazione di incidenti significativi ai sensi della NIS2, diversamente da quest'ultima non fissa direttamente i termini per questi obblighi. Questi sono infatti stabiliti dalle autorità europee di vigilanza (ABE, EOPA, ESMA), in consultazione con ENISA e la Banca Centrale Europea, attraverso delle norme tecniche di regolamentazione comuni. Questi progetti di standardizzazione, comunque, proseguono nella direzione di un allineamento con i termini previsti da altre normative aventi simili obblighi (es., NIS2 e GDPR)⁶³.

Il terzo pilastro concerne le politiche per i test su processi, controlli e sistemi delle TIC allo scopo di valutare la preparazione alla gestione degli incidenti connessi a tali tecnologie, di identificare punti deboli, carenze e lacune della resilienza operativa digitale e, quindi, di attuare tempestivamente misure correttive⁶⁴. Similmente a quanto visto con riguardo all'Art. 21 NIS2, l'Art. 25 DORA identifica attraverso un elenco minimo e non esaustivo alcuni test di resilienza operativa digitale che le entità finanziarie dovranno attuare⁶⁵. Adottando poi un approccio scalare, alcuni soggetti, ritenuti più critici, devono effettuare in aggiunta alcuni test avanzati di penetrazione guidati dalla minaccia (TLPT).

Il quarto pilastro è rappresentato dalla gestione dei rischi informatici derivanti da terzi. Le sempre più marcate dipendenze da fornitori terzi di infrastrutture e servizi contribuiscono ad un ampliamento del panorama delle minacce e delle vulnerabilità⁶⁶. Pertanto, il regolamento comprende alcuni principi chiave per una solida gestione del rischio di terze parti tenendo in considerazione la complessità delle dipendenze connesse alle TIC. In tale contesto, assume centrale importanza l'obbligo per le entità finanziarie di mantenere e aggiornare un registro di informazioni su tutti gli accordi contrattuali per l'utilizzo di servizi TIC prestati da fornitori terzi, da tenere a disposizione delle autorità competenti e, comunque, oggetto di comunicazione in merito ad eventuali variazioni (es.,

⁶³ Si veda il Report Finale prodotto da EBA, EIOPA ed ESMA, *Draft Regulatory Technical Standards on the content of the notification and reports for major incidents and significant cyber threats and determining the time limits for reporting major incidents and Draft Implementing Technical Standards On the standard forms, templates and procedures for financial entities to report a major incident and to notify a significant cyber threat*, 17 luglio 2024 https://www.esma.europa.eu/sites/default/files/2024-07/JC_2024-33_Final_report_on_the_draft_RTS_and ITS_on_incident_reporting.pdf.

⁶⁴ Art. 24, DORA.

⁶⁵ Ad es., valutazione e scansione delle vulnerabilità, analisi open source, valutazioni della sicurezza delle reti, analisi delle carenze, esami della sicurezza fisica, questionari e soluzioni di scansione del software, esami del codice sorgente, ecc.

⁶⁶ Considerando 2, DORA.

nuovi accordi) su base almeno annuale⁶⁷. Il regolamento individua poi obblighi di *due diligence* da rispettare in fase precontrattuale⁶⁸, nonché alcune disposizioni che gli accordi devono contenere per garantire condizioni di maggiore parità tra l'entità finanziaria e il fornitore terzo di servizi⁶⁹. Inoltre, il DORA prevede uno speciale quadro di controllo per i fornitori terzi di servizi TIC considerati “critici” ai sensi dell'Art. 31.

Il quinto pilastro interessa invece i meccanismi di condivisione delle informazioni. Già nella sezione precedente, con riguardo alla NIS2, si è vista l'importanza strategica di una condivisione mirata delle informazioni rilevanti dal punto di vista della cybersicurezza. Infatti, non solo la *ratio*, ma anche gli aspetti procedurali dei meccanismi di condivisione di informazione di cui all'Art. 45 DORA ricalcano gli accordi di cui all'Art. 29 NIS2.

Infine, per quanto riguarda l'impianto sanzionatorio, fatto salvo il diritto degli Stati membri di prevedere specifiche sanzioni penali per violazioni del regolamento, le autorità competenti possono imporre una serie di sanzioni amministrative o misure di riparazione. A differenza di quanto visto in altri strumenti giuridici, come il GDPR e la NIS2, il DORA non individua i criteri di calcolo delle sanzioni amministrative bensì demanda, secondo lo schema già visto, alle Autorità competenti tale onere⁷⁰.

4. Il quadro europeo di certificazione della cybersicurezza: il Cybersecurity Act

Facciamo adesso un passo indietro. Nel 2017 la Commissione e l'Alto Rappresentante adottano la seconda Strategia dell'Unione europea per la cybersicurezza⁷¹. La necessità di aggiornare la politica dell'UE in materia dopo soli 4 anni dalla prima Strategia deriva da due fattori principali: l'inesorabile e progressiva dipendenza della società e del mercato interno dalle tecnologie digitali e il conseguente mutamento ed amplificazione del panorama delle minacce e degli incidenti, soprattutto alla luce di prodotti digitali (come *devices IoT*) insicuri.

Il modello di governance della Strategia del 2017 rimane imperniato sull'approccio *multi-stakeholder* già introdotto nel 2013. Infatti, la cybersicurezza è sempre di più rappresentata come una sfida sociale comune, dal momento che ad essere minacciato non è solo il mercato unico digitale, ma anche – e soprat-

⁶⁷ Art. 28, par. 3, DORA.

⁶⁸ Art. 28, par. 4 e 5, DORA.

⁶⁹ Art. 30, DORA.

⁷⁰ Art. 51, DORA.

⁷¹ Commissione europea e Alto Rappresentante dell'UE per gli Affari Esteri e la Politica di Sicurezza, *Resilienza, deterrenza e difesa: verso una cybersicurezza forte per l'UE*, JOIN, 2017, 450 final.

tutto – «il funzionamento stesso delle nostre democrazie, le nostre libertà e i nostri valori»⁷². Pertanto, dovrebbero essere coinvolti in questa sfida «molteplici livelli dell'amministrazione pubblica, dell'economia e della società»⁷³.

Le cinque priorità strategiche della Strategia del 2013 vengono accorpate in tre macro-filoni di intervento: i) rafforzamento della cyber resilienza; ii) creazione di una cyber deterrenza a livello UE efficace; e iii) rafforzamento della cooperazione internazionale sulla cybersicurezza. A livello legislativo, gli sviluppi più significativi coinvolgono soprattutto il primo filone.

In particolare, il regolamento UE 2019/881 (c.d. *Cybersecurity Act*) si propone di raggiungere due obiettivi strategici per il rafforzamento della (cyber)resilienza dell'UE: 1) il rafforzamento del ruolo dell'ENISA, attraverso un mandato permanente e nuove funzioni; 2) la creazione di un meccanismo di certificazione della cybersicurezza a livello UE per supportare la crescita del mercato unico della cybersicurezza.

Il Cybersecurity Act è il primo atto giuridico dell'UE a prevedere una definizione di “cybersicurezza”, coerente con la visione della Strategia del 2017. In tal senso, paiono superati i tradizionali paradigmi dell'*information security* cui ancora la definizione della Strategia del 2013 rimaneva ancorata. La ‘cybersicurezza’, pertanto, ricomprende «l'insieme delle attività necessarie per proteggere la rete e i sistemi informativi, *gli utenti di tali sistemi e altre persone interessate dalle minacce informatiche* [enfasi aggiunta]»⁷⁴.

Con la seconda Strategia, inizia infatti a consolidarsi la consapevolezza che un elevato livello comune di cybersicurezza è possibile nella misura in cui la società tutta adotti una corretta “postura cyber”. In tal senso, «la cybersicurezza diventa una responsabilità di tutti»⁷⁵; degli Stati membri *in primis*, quindi del settore privato che detiene larghe quote del “cyberspazio” e in ultimo dei singoli individui che attraverso pratiche di “cyber igiene” possono essere determinanti nel ridimensionare la minaccia.

Un altro aspetto fondamentale che rivela l'evoluzione paradigmatica del concetto di “cybersicurezza” rispetto al 2013 risiede nella maggiore attenzione posta sulla formazione di competenze e sulla sensibilizzazione e consapevolezza situazionale del rischio cyber. In una prospettiva d'autonomia strategica, l'Unione deve sviluppare le proprie capacità in materia di cybersicurezza, ad ogni livello: vengono pertanto poste le basi per la creazione di una rete di centri

⁷² *Ibid.*, p. 2.

⁷³ *Ibid.*, p. 4.

⁷⁴ Art. 2, punto 1, Cybersecurity Act.

⁷⁵ Commissione europea e Alto Rappresentante dell'UE per gli Affari Esteri e la Politica di Sicurezza, *Resilienza, deterrenza e difesa: verso una cybersicurezza forte per l'UE*, cit., p. 12.

di competenza sulla cybersicurezza, il coordinamento dei quali è assicurato dal “Centro Europeo di Ricerca e di Competenza sulla Cybersicurezza”⁷⁶.

Il Cybersecurity Act è diviso in due parti. Nella prima parte viene specificato e potenziato il ruolo dell’ENISA attraverso un mandato permanente⁷⁷, con nuovi obiettivi, compiti e aspetti organizzativi⁷⁸. Dal momento che la missione principale di ENISA è contribuire al conseguimento di un elevato livello di cybersicurezza nell’Unione, l’Agenzia vede pertanto assegnarsi compiti di assistenza e consulenza circa lo sviluppo delle strategie, delle politiche e delle normative di cybersicurezza dell’Unione, nonché di promozione di un’attuazione coerente del quadro normativo pertinente. ENISA assume anche rilevanti compiti di assistenza nei confronti degli Stati membri nell’area strategica – non a caso, ricondotta spesso nell’ambito della sicurezza nazionale – del consolidamento delle capacità per prevenire gli incidenti e gli attacchi. Di pari rilevanza, poi, è il ruolo di coordinamento tra tutti i portatori di interessi, promuovendo ad esempio la cooperazione tra settore pubblico e privato e facilitando lo scambio di conoscenze e delle migliori pratiche. Sotto quest’ultimo profilo, occorre sottolineare poi l’attività dell’ENISA in materia di sensibilizzazione dell’opinione pubblica e del settore privato sui rischi di cybersicurezza.

La seconda parte del Cybersecurity Act introduce il quadro europeo di certificazione della cybersicurezza, con l’obiettivo di garantire un livello adeguato di cybersicurezza dei prodotti, servizi e processi TIC e, dal 2025, anche dei servizi di sicurezza gestiti⁷⁹ nell’Unione, di evitare la frammentazione del mercato interno per quanto riguarda i sistemi di certificazione in materia di cybersicurezza nonché di rafforzare la fiducia dei consumatori⁸⁰. Infatti, «la mancanza di programmi di certificazione riconosciuti in tutta l’Unione che integrino parametri più elevati di resilienza nei prodotti in modo da sostenere la fiducia del mercato a livello dell’UE» è vista dalla Commissione come un ostacolo alla crescita del mercato della cybersicurezza nell’UE⁸¹.

I sistemi europei di certificazione della cybersicurezza attestano che i prodotti, servizi e processi TIC, e i servizi di sicurezza gestiti, valutati nel loro ambito sono conformi a determinati requisiti di sicurezza volti a «proteggere la di-

⁷⁶ Nel dicembre 2020, Bucarest è stata scelta come sede per ospitare il centro, c.d. ECCC, istituito con il Regolamento (UE) 2021/887.

⁷⁷ Dal 2004 il mandato è stato prorogato con regolamenti per tre volte, nel 2008, nel 2011 e infine nel 2013.

⁷⁸ Art. 1, par. 1, lett. a, Cybersecurity Act.

⁷⁹ Modifica introdotta del Regolamento (UE) 2025/37.

⁸⁰ Art. 1, par. 1, lett. b, Cybersecurity Act.

⁸¹ Commissione europea e Alto Rappresentante dell’UE per gli Affari Esteri e la Politica di Sicurezza, *Resilienza, deterrenza e difesa: verso una cybersicurezza forte per l’UE*, cit., p. 5.

sponibilità, l'autenticità, l'integrità o la riservatezza dei dati conservati, trasmessi o trattati o le funzioni o i servizi offerti da tali prodotti, servizi e processi o accessibili tramite essi per tutto il loro ciclo di vita⁸². Evidentemente, tali requisiti non possono essere dettagliati dal regolamento in considerazione dell'impossibilità di formulare requisiti generali di cybersicurezza validi per tutti i prodotti, servizi e processi TIC. Asset diversi, infatti, hanno esigenze (di sicurezza) diverse. Pertanto, l'approccio del legislatore è stato quello di definire degli obiettivi di cybersicurezza⁸³ di carattere generale da prendere in considerazione al momento della progettazione dei sistemi europei di certificazione.

Da un punto di vista procedurale, il meccanismo di certificazione UE della cybersicurezza è avviato dalla richiesta della Commissione UE all'ENISA di preparare una proposta di sistema⁸⁴. L'ENISA quindi elabora la proposta consultando tutti i portatori di interesse pertinenti mediante un processo di consultazione trasparente⁸⁵. Ogni proposta di sistema deve prendere in considerazione gli obiettivi di sicurezza di cui all'Art. 51; deve specificare secondo quali livelli di affidabilità ("di base"; "sostanziale"; "elevato") il prodotto, servizio o processo TIC, o servizio di sicurezza gestito, possa essere certificato, in ragione del rischio associato all'uso⁸⁶; specificare se l'autovalutazione della conformità ad opera del fabbricante/fornitore del prodotto certificato sia consentita⁸⁷; ed infine deve contenere alcuni elementi minimi come, ad esempio, l'oggetto e l'ambito di applicazione del sistema di certificazione, nonché il riferimento agli standard tecnici internazionali od europei su cui il sistema si basa e attraverso cui è possibile conseguire gli obiettivi di sicurezza.

Come risultato del processo di certificazione, i prodotti, servizi o processi certificati sono considerati conformi ai requisiti di tale sistema. Per quanto attiene all'ente certificatore, i certificati europei di cybersicurezza che fanno riferimento a livelli di affidabilità "di base" o "sostanziale" sono rilasciati dagli organismi di valutazione della conformità⁸⁸. Il certificato nell'ambito di un sistema che invece richieda un livello di affidabilità "elevato" deve essere rilasciato

⁸² Art. 46, par. 2, Cybersecurity Act.

⁸³ Art. 51, Cybersecurity Act: gli obiettivi di sicurezza minimi identificati vanno oltre i principi classici della *computer e information security*, ossia la triade CIA, ricomprendendo ulteriori aspetti cruciali della cybersicurezza, quali: la gestione delle vulnerabilità; i principi di base della *digital forensics*; il *disaster recovery*; la *security by design e by default*; gli aggiornamenti di software e hardware.

⁸⁴ Art. 48, Cybersecurity Act.

⁸⁵ Art. 49, Cybersecurity Act.

⁸⁶ Art. 52, Cybersecurity Act.

⁸⁷ Art. 53, Cybersecurity Act.

⁸⁸ Art. 56, par. 4, Cybersecurity Act. Tali enti sono accreditati da organismi nazionali di accreditamento designati ai sensi del regolamento (CE) n. 765/2008 a condizione che l'organismo soddisfi i requisiti di cui all'allegato del regolamento.

dall'autorità nazionale di certificazione della cybersicurezza⁸⁹ oppure, ma solamente in casi tassativi, dagli organismi di valutazione della conformità⁹⁰. La validità di un certificato, che comunque può essere rinnovato, è indicata dal sistema stesso nell'ambito del quale tale certificato è rilasciato⁹¹.

Pur rimanendo in via generale strumento di diritto privato di natura volontaria⁹², le normative dell'Unione o degli Stati membri possono eccezionalmente rendere obbligatoria la certificazione, ad esempio, per alcune categorie di prodotti in determinati settori in considerazione dell'alto grado di criticità. Ed infatti la direttiva NIS2, all'Articolo 24, prevede che gli Stati membri possano imporre ai soggetti essenziali e importanti di utilizzare prodotti, servizi e processi TIC che siano certificati e che la Commissione possa specificare, attraverso atti delegati, quali categorie di soggetti essenziali ed importanti siano tenute ad utilizzare determinate tecnologie TIC certificate ai sensi del Cybersecurity Act.

5. La cybersicurezza dei prodotti con elementi digitali: il Cyber Resilience Act

Al fine di incentivare prodotti e servizi sicuri, parallelamente alla continuazione dell'implementazione del quadro di certificazioni introdotto dal Cybersecurity Act, la Commissione annunciava già nella Strategia del 2020 nuove possibili norme orizzontali in materia di cybersicurezza per tutti i prodotti connessi⁹³. Queste, infatti, avrebbero integrato le misure "verticali", e cioè settoriali, riguardanti categorie specifiche di prodotti.

Così, il 15 settembre 2022, la Commissione pubblica una proposta di "legge sulla ciberresilienza" (*Cyber Resilience Act*, CRA)⁹⁴, ossia un regolamento contenente nuove norme in materia di cybersicurezza per i prodotti con elementi digitali. Il regolamento (UE) 2024/2847 (CRA)⁹⁵ è entrato in vigore il 10 dicem-

⁸⁹ Ad esempio, nel contesto italiano, l'Agenzia per la Cybersicurezza nazionale (ACN) è designata dall'articolo 7, comma 1, lettera e), del decreto-legge 82/2021 quale autorità nazionale di certificazione della cybersicurezza.

⁹⁰ Art. 56, par. 6, Cybersecurity Act.

⁹¹ Art. 56, par. 9, Cybersecurity Act.

⁹² Art. 56, par. 2, Cybersecurity Act.

⁹³ Commissione europea e Alto Rappresentante dell'UE per gli Affari Esteri e la Politica di Sicurezza, *La strategia dell'UE in materia di cybersicurezza per il decennio digitale*, cit., p. 10.

⁹⁴ Commissione europea, *Proposta di regolamento del Parlamento europeo e del Consiglio relativo a requisiti orizzontali di cybersicurezza per i prodotti con elementi digitali e che modifica il regolamento (UE) 2019/1020, 2022/0272(COD)*.

⁹⁵ Regolamento (UE) 2024/2847 del Parlamento europeo e del Consiglio, del 23 ottobre 2024, relativo a requisiti orizzontali di cybersicurezza per i prodotti con elementi digitali e che modifica i regolamenti (UE) n. 168/2013 e (UE) 2019/1020 e la direttiva (UE) 2020/1828 (regolamento sulla ciberresilienza), GU L 2024/2847, 20.11.2024.

bre 2024, ma sarà applicabile solo dall'11 dicembre 2027, eccezion fatta per l'articolo 14 (11 settembre 2026) e il capo IV (11 giugno 2026).

Il CRA mira a risolvere tre ordini di problemi diversi. Primo, un livello insufficiente di cybersicurezza dei prodotti con elementi digitali, testimoniato da vulnerabilità diffuse e dalle forniture inadeguate di aggiornamenti di sicurezza (*patch*). Secondo, un'insufficiente comprensione delle informazioni e un accesso limitato alle stesse da parte degli utilizzatori per quanto concerne le proprietà di cybersicurezza dei prodotti. Terzo, la mancanza di una normativa dell'Unione che disciplini in modo completo gli aspetti di cybersicurezza per tutti i prodotti hardware e software⁹⁶. A tal fine, il CRA pone quattro obiettivi specifici: i) garantire che i fabbricanti migliorino la sicurezza dei prodotti con elementi digitali fin dalla fase di progettazione e durante l'intero ciclo di vita; ii) garantire un quadro coerente in materia di cybersicurezza, facilitando la conformità per i produttori di hardware e software; iii) migliorare la trasparenza delle proprietà di sicurezza dei prodotti con elementi digitali e iv) consentire alle imprese e ai consumatori di utilizzarli in modo sicuro.

Il CRA si applica ai prodotti con elementi digitali messi a disposizione sul mercato la cui finalità prevista o il cui utilizzo ragionevolmente prevedibile include una connessione dati logica o fisica diretta o indiretta a un dispositivo o a una rete⁹⁷. È importante notare che la nozione di prodotto è piuttosto ampia, in quanto comprende non solo qualsiasi prodotto hardware, ma anche software, nonché le relative soluzioni di elaborazione dati da remoto, compresi le componenti software o hardware immessi sul mercato separatamente (c.d. *standalone software*)⁹⁸.

Tuttavia, non tutto il software rientra nell'ambito di applicazione del CRA. Infatti, ai modelli di *Software-as-a-Service* (SaaS), *Platform-as-a-Service* (PaaS) o *Infrastructure-as-a-Service* (IaaS), come il cloud computing, si applicano già le misure della direttiva NIS2. Le disposizioni del CRA si estendono al SaaS solamente nella misura in cui questo costituisca una "soluzione di elaborazione dati da remoto", cioè «qualsiasi elaborazione dati a distanza per la quale il software è stato progettato e sviluppato dal fabbricante del prodotto con elementi digitali in questione o per suo conto, la cui assenza impedirebbe al prodotto con elementi digitali di svolgere una delle sue funzioni»⁹⁹. Sotto altro profilo, un regime di regolamentazione "leggero" (*light-touch*) si applica al software libero e open-

⁹⁶ Commissione europea, *Relazione alla proposta di regolamento relativo a requisiti orizzontali di cybersicurezza per i prodotti con elementi digitali e che modifica il regolamento (UE) 2019/1020*, p. 1.

⁹⁷ Art. 2, par. 1, CRA.

⁹⁸ Art. 3, par. 1, CRA.

⁹⁹ Considerando 11, CRA.

source (c.d. FOSS) che sia destinato ad attività commerciali, al fine di non ostacolare lo sviluppo e la diffusione di tali comunità.

Come molti altri atti legislativi dell'UE sul digitale, il CRA adotta un approccio regolamentativo basato sul rischio. I prodotti con elementi digitali sono suddivisi in categorie in base al livello di rischio di cybersicurezza associato ai prodotti. Oltre ad una categoria "predefinita", i prodotti sono considerati "importanti" se la loro funzionalità principale rientra in una delle categorie elencate nell'Allegato III¹⁰⁰. La categoria "importante" è ulteriormente suddivisa in due sottoclassi, ovvero la classe I e la classe II, dove la seconda ricomprende i prodotti che darebbero luogo ad un impatto negativo maggiore qualora le loro vulnerabilità venissero sfruttate. L'ultima categoria è quella dei prodotti "critici". Questi sono elencati nell'Allegato IV¹⁰¹. Questa tassonomia assume rilevanza soprattutto alla luce della diversa procedura di valutazione della conformità che questi prodotti devono seguire.

Quest'ultima considerazione ci permette di fare luce su un ulteriore approccio regolamentativo alla base del CRA, ossia il modello di legislazione in materia di sicurezza dei prodotti. La normativa UE sulla sicurezza dei prodotti è stata riformata all'inizio degli anni 2000 con il cosiddetto "nuovo quadro legislativo" (*new legislative framework*, NLF). L'NLF è composto dal regolamento (UE) 765/2008, dalla decisione 768/2008 e dal regolamento (UE) 2019/1020 e rappresenta un'evoluzione del cosiddetto "Nuovo Approccio" degli anni '80. Il Nuovo Approccio limitava il contenuto della legislazione armonizzata ai "requisiti essenziali", lasciando alle norme tecniche (standard tecnici) le modalità di attuazione di tali requisiti dal punto di vista operativo. L'NLF ha completato la riforma del Nuovo Approccio rafforzando le procedure di valutazione della conformità (con i cd. "moduli"), l'accreditamento e la sorveglianza del mercato. In breve, i fabbricanti, per poter immettere un prodotto sul mercato interno, devono dimostrare la conformità dei loro prodotti ai requisiti essenziali pertinenti attraverso specifiche procedure di valutazione della conformità stabilite negli atti giuridici rilevanti.

A questo proposito, l'articolo 6 CRA stabilisce due condizioni per rendere i prodotti disponibili sul mercato: i) devono soddisfare i requisiti essenziali (RE) di cui alla parte 1 dell'allegato I¹⁰²; ii) i processi messi in atto dal fabbricante sono conformi ai RE di cui alla parte 2 dell'allegato I¹⁰³.

¹⁰⁰ Art. 7, CRA.

¹⁰¹ Art. 8, CRA.

¹⁰² I prodotti con elementi digitali devono essere progettati, sviluppati e prodotti in modo da garantire un livello adeguato di cybersicurezza in base ai rischi. Sulla base della valutazione dei rischi, il prodotto deve essere reso disponibile senza vulnerabilità note sfruttabili e con una confi-

Il primo obbligo dei fabbricanti, nel processo che mira alla conformità con le due serie di RE, consiste nell'esecuzione di una valutazione dei rischi di cybersicurezza associati a un prodotto per identificare i rischi concreti di cybersicurezza e mappare tali rischi rispetto ai RE pertinenti¹⁰⁴. In linea con la teoria tradizionale della gestione del rischio, tale analisi deve essere contestuale, ossia «basata sulla destinazione d'uso e sull'uso ragionevolmente prevedibile, nonché sulle condizioni d'uso del prodotto con elementi digitali, come l'ambiente operativo o i beni da proteggere, tenendo conto del tempo previsto di utilizzo del prodotto»¹⁰⁵. Il primo obbligo dei fabbricanti indica come l'approccio basato sul rischio e quello sulla sicurezza dei prodotti siano complementari.

Oltre alla valutazione dei rischi di cybersicurezza, i fabbricanti di prodotti con elementi digitali hanno diversi altri obblighi. Questi soggetti devono infatti rispettare obblighi di *due diligence*¹⁰⁶, tra cui gli obblighi di gestione delle vulnerabilità¹⁰⁷, obblighi di documentazione e informazione¹⁰⁸, obblighi di segnalazio-

gurazione sicura per impostazione predefinita (*by default*); deve garantire la protezione da accessi non autorizzati mediante meccanismi di controllo adeguati; deve proteggere la riservatezza dei dati personali o di altro tipo trattati mediante una crittografia all'avanguardia, ecc.

¹⁰³ I fabbricanti dei prodotti con elementi digitali devono: identificare e documentare le vulnerabilità e i componenti contenuti nel prodotto, anche redigendo una distinta base del software in un formato comunemente utilizzato e leggibile, che copra almeno le dipendenze di primo livello del prodotto; ridurre le vulnerabilità senza indugio, anche fornendo aggiornamenti di sicurezza; applicare test e revisioni efficaci e regolari della sicurezza del prodotto; divulgare pubblicamente le informazioni sulle vulnerabilità risolte, una volta reso disponibile un aggiornamento di sicurezza, ecc.

¹⁰⁴ Art. 13, par. 2, CRA.

¹⁰⁵ Art. 13, par. 3, CRA.

¹⁰⁶ I fabbricanti, nel momento in cui integrano componenti di terze parti, compreso il software libero e open source, devono assicurarsi che tali componenti non compromettano la cybersicurezza del prodotto (Art. 13, par. 5, CRA). Inoltre, devono garantire che sui prodotti sia apposto un numero di tipo, di lotto o altro elemento che ne consenta l'identificazione (Art. 13, par. 15, CRA). Ancora, se i fabbricanti hanno motivo di credere che il prodotto o i processi messi in atto non siano conformi ai RE, adottano immediatamente le misure correttive necessarie (Art. 13, par. 21, CRA).

¹⁰⁷ Al momento dell'immissione sul mercato del prodotto e dopo la commercializzazione, per l'intera durata del periodo di supporto, i fabbricanti assicurano che le vulnerabilità siano gestite in modo efficace attraverso piani e procedure appropriate, comprese politiche coordinate di divulgazione delle vulnerabilità (Art. 13, par. 8, CRA).

¹⁰⁸ Quando immettono sul mercato un prodotto, i fabbricanti devono presentare la documentazione tecnica pertinente ai sensi dell'articolo 31 e dell'allegato VII, che deve includere la valutazione del rischio di cybersecurity (Art. 13, par. 4, CRA). Inoltre, devono documentare gli aspetti rilevanti della cybersicurezza relativi al prodotto (ad esempio, le vulnerabilità e le informazioni fornite da terzi). Ancora, devono indicare il proprio nome, la denominazione commerciale o il marchio registrato nonché le modalità di contatto (ad esempio, l'indirizzo postale e l'indirizzo e-mail) sul prodotto o sulla sua confezione (Art. 13, par. 16, CRA). Infine, i prodotti devono essere accompagnati dalle informazioni e dalle istruzioni di cui all'Allegato II, fornite in una lingua facilmente comprensibile, in forma elettronica o fisica (Art. 13, par. 18, CRA).

ne¹⁰⁹ e obblighi di cooperazione¹¹⁰. È opportuno ribadire che prima di immettere sul mercato un prodotto con elementi digitali, i fabbricanti devono dimostrare la conformità ai requisiti essenziali CRA attraverso una procedura di valutazione della conformità. Come ultimo passaggio, i fabbricanti redigono la dichiarazione di conformità UE e appongono la marcatura CE.

La valutazione della conformità è una fase cruciale della legislazione europea sulla sicurezza dei prodotti. Le procedure, *rectius*: i moduli, di valutazione della conformità sono equivalenti dal punto di vista legale, ma non dal punto di vista tecnico. Esistono infatti tre opzioni principali: i) auto-valutazione da parte del fabbricante che culmina con una dichiarazione di conformità; ii) auto-valutazione del fabbricante con il coinvolgimento di un organismo di valutazione della conformità interno accreditato che fa parte dell'organizzazione del soggetto; iii) valutazione eseguita da un organismo di valutazione della conformità esterno¹¹¹.

Nel contesto del CRA, come detto, la tassonomia basata sul rischio dei prodotti con elementi digitali (cioè, predefiniti, importanti di classe I e II, critici e FOSS) è particolarmente rilevante per quanto riguarda le procedure che i fabbricanti possono seguire per dimostrare la conformità ai RE. Mentre per i prodotti “predefiniti” i fabbricanti possono optare per l'autovalutazione o per la valutazione da parte di terzi (esame UE del tipo, garanzia qualità totale e sistema di certificazione di cybersicurezza dell'UE), per i prodotti importanti e critici l'autovalutazione è esclusa¹¹².

Infine, il CRA stabilisce regole dettagliate per la sorveglianza del mercato e l'applicazione delle norme, nonché sanzioni per il mancato rispetto dei molteplici requisiti e obblighi stabiliti dal regolamento. Tuttavia, il regolamento non tratta esplicitamente le questioni relative alla responsabilità, né prevede diritti individuali o mezzi di ricorso per i singoli individui nel caso in cui si verifichino

¹⁰⁹ Se i fabbricanti individuano una vulnerabilità in un componente integrato nel prodotto, devono segnalare alla persona o all'entità che produce o effettua la manutenzione del componente (Art. 13, par. 6, CRA). Sotto diverso profilo, l'articolo 14 del CRA introduce un quadro di segnalazione degli incidenti e delle vulnerabilità. In breve, i fabbricanti devono notificare al CSIRT e all'ENISA qualsiasi vulnerabilità attivamente sfruttata nel prodotto e qualsiasi incidente grave che abbia un impatto sulla sicurezza del prodotto.

¹¹⁰ La documentazione tecnica e la dichiarazione di conformità UE sono tenute a disposizione delle Autorità di Vigilanza del Mercato per almeno 10 anni dall'immissione sul mercato o per il periodo di supporto da parte dei fabbricanti (Art. 13, par. 13, CRA). Su richiesta di un'autorità di vigilanza del mercato, i fabbricanti forniscono a tale autorità tutte le informazioni necessarie per dimostrare la conformità del prodotto e dei processi ai RE (Art. 13, par. 22, CRA).

¹¹¹ Commissione europea, *La guida blu all'attuazione della normativa UE sui prodotti 2022*, COM(2022), 247 final, pp. 66-67.

¹¹² Art. 32, CRA.

danni in conseguenza di una violazione degli obblighi da parte dei destinatari delle disposizioni del CRA.

6. Solidarietà nella cybersicurezza: il Cyber Solidarity Act

Il 18 aprile 2023, la Commissione europea propone un regolamento UE sulla “cyber solidarietà” (c.d. *Cyber Solidarity Act*, CSoA)¹¹³, entrato in vigore ad inizio 2025¹¹⁴. Questo nuovo atto giuridico si basa sui già esistenti quadri di cooperazione operativa e di gestione delle crisi di cybersicurezza (EU-CyCLONe e la rete di CSIRTs), e ha l’obiettivo di rafforzare le capacità dell’UE di individuare e rispondere a minacce e attacchi significativi e su larga scala.

Il CSoA è articolato attorno a tre pilastri: i) una rete paneuropea di poli informatici (c.d., “sistema europeo di allerta per la cybersicurezza”) per potenziare capacità coordinate di rilevamento e conoscenza situazionale; ii) un meccanismo per le emergenze di cybersicurezza al fine di sostenere gli Stati membri ed altri utenti nella preparazione e nella risposta agli incidenti di cybersicurezza significativi e su vasta scala; iii) un meccanismo europeo di riesame degli incidenti di cybersicurezza¹¹⁵.

Il primo pilastro, il sistema europeo di allerta, si compone di una rete di “poli informatici” nazionali e transfrontalieri¹¹⁶, costituita su base volontaria, al fine di migliorare le capacità di gestione delle minacce informatiche dell’UE attraverso la condivisione di informazioni, l’analisi delle minacce, il coordinamento tra soggetti competenti (i CSIRT, la rete di CSIRT, EU-CyCLONe e le autorità competenti designate ai sensi della direttiva NIS2) e lo sviluppo di tecnologie avanzate il miglioramento delle capacità di protezione e risposta dei soggetti rilevanti¹¹⁷. Nel quadro della condivisione di informazioni tra poli informatici

¹¹³ Nella stessa data è stato anche proposto un regolamento che modifica il regolamento (UE) 2019/881 per consentire la futura adozione dei sistemi di certificazione per i “servizi di sicurezza gestiti”, COM(2023), 208 final.

¹¹⁴ Regolamento (UE) 2025/38 del Parlamento europeo e del Consiglio, del 19 dicembre 2024, che stabilisce misure intese a rafforzare la solidarietà e le capacità dell’Unione di rilevamento delle minacce e degli incidenti informatici e di preparazione e risposta agli stessi, e che modifica il regolamento (UE) 2021/694 (regolamento sulla cibersolidarietà), GU L 2025/38, 15.1.2025. È interessante notare come il CSoA trovi la sua base giuridica negli articoli 173 e 322 TFUE, rispettivamente inerenti alla competitività dell’industria dell’Unione e le finanze dell’Unione, anziché nell’art. 114 TFUE, come la quasi totalità degli atti giuridici UE in materia di cybersicurezza.

¹¹⁵ Art. 1, par. 1, CSoA.

¹¹⁶ Il polo informatico transfrontaliero è una «piattaforma multinazionale, istituita mediante un accordo di consorzio scritto, che riunisce in una struttura di rete coordinata i poli informatici nazionali di almeno tre Stati membri» (Art. 2, par. 1, CSoA).

¹¹⁷ Art. 4, par. 2, CSoA.

transfrontalieri, al fine di favorire l'interoperabilità, sono emanati da ENISA orientamenti che specificano i formati e protocolli¹¹⁸.

In virtù della potenziale sovrapposizione tra i poli informatici transfrontalieri e le strutture già esistenti in materia di cybersicurezza a livello UE, quali la rete di CSIRT e EU-CyCLONe, viene assicurato un opportuno raccordo tra le attività di questi *fora* al fine di garantire una piena conoscenza situazionale. Pertanto, i poli informatici transfrontalieri e la rete di CSIRT concordano le modalità procedurali per la cooperazione finalizzata alla condivisione delle informazioni pertinenti; se invece i poli informatici transfrontalieri ottengono informazioni relative ad un incidente su vasta scala, anche potenziale, devono fornire senza ritardo ogni informazione utile ad EU-CyCLONe e alla rete di CSIRT, garantendo pertanto la rilevanza di questi eventi a livello UE e non solo nazionale¹¹⁹. Da un punto di vista operativo, il Centro europeo di competenza per la cibersicurezza (ECCC)¹²⁰ bandisce appalti congiunti di strumenti, infrastrutture e servizi, al fine di istituire poli informatici nazionali e sostenere i consorzi transfrontalieri¹²¹.

Il secondo pilastro concerne invece l'istituzione del meccanismo per le emergenze di cybersicurezza, volto a sostenere tre categorie di azioni: i) azioni di preparazione; ii) azioni a sostegno della risposta agli incidenti di cybersicurezza significativi e su vasta scala; iii) azioni di assistenza reciproca. Tra le azioni di preparazione sostenute dal meccanismo rientrano verifiche coordinate della preparazione dei soggetti operanti in settori ad alta criticità, individuati dalla Commissione, quali i test di penetrazione e la valutazione delle minacce¹²². Gli scenari di rischio e le metodologie per tali esercizi sono elaborati dal gruppo di cooperazione NIS (in collaborazione con la Commissione e l'Alto Rappresentante), l'ENISA e l'EU-CyCLONe¹²³.

Per quanto concerne le azioni a sostegno della risposta agli incidenti, viene istituita la "riserva dell'UE per la cibersicurezza" al fine di assistere, su richiesta, le autorità di gestione delle crisi informatiche e i CSIRT nazionali, nonché il CERT-EU e le autorità competenti dei paesi terzi associati al programma Europa digitale nella gestione degli incidenti di cybersicurezza significativi e su vasta scala¹²⁴. Tale riserva consiste in servizi di risposta erogati da fornitori di fiducia selezionati in base a specifici criteri e la Commissione ha la responsabilità gene-

¹¹⁸ Art. 6, par. 4, CSoA.

¹¹⁹ Art. 7, CSoA.

¹²⁰ Istituito dal Regolamento (UE) 2021/887, con sede a Bucarest.

¹²¹ Art. 9, CSoA.

¹²² Art. 12, par. 2, CSoA.

¹²³ Art. 12, par. 6, CSoA.

¹²⁴ Art. 14, CSoA.

rale della sua attuazione¹²⁵, ancorché funzionamento e amministrazione siano affidati all'ENISA¹²⁶.

Infine, il terzo pilastro consiste nel meccanismo europeo di riesame degli incidenti di cybersicurezza. Dietro richiesta della Commissione o di EU-CyCLONe, ENISA, con il sostegno della rete di CSIRT, con l'approvazione degli Stati membri interessati e con la collaborazione di tutti i portatori di interessi, riesamina e valuta le minacce, le vulnerabilità sfruttabili note e le azioni di attenuazione in relazione a uno specifico incidente significativo o su vasta scala; quindi presenta a EU-CyCLONe, alla rete di CSIRT, agli Stati membri interessati e alla Commissione una relazione finale volta a trarre gli opportuni insegnamenti per evitare o attenuare futuri incidenti¹²⁷. Ovviamente, la relazione finale non include dettagli sulle vulnerabilità sfruttate che rimangono irrisolte e, se richiesto da uno Stato membro, contiene solo dati anonimizzati¹²⁸.

In conclusione, è significativo notare come la causa principale dietro l'adozione di questo ultimo atto giuridico in materia di cybersicurezza a livello UE non sia tanto l'incremento della frequenza e dell'impatto degli incidenti di cybersicurezza e, segnatamente, di incidenti su vasta scala aventi la potenzialità di provocare danni significativi ad infrastrutture critiche – giacché l'Unione aveva già approntato una serie di misure per ridurre le vulnerabilità e accrescere la resilienza delle infrastrutture critiche contro tali rischi (in particolare, la direttiva NIS2) – quanto più, da una parte, la scarsa attitudine cooperativa tra le istituzioni esistenti e, dall'altra, la mancanza di meccanismi appositi di investimento in infrastrutture e servizi per sviluppare capacità e competenze in materia di cybersicurezza, permettendo una migliore gestione della minaccia.

7. Riflessioni conclusive

Il presente capitolo ha mostrato come il c.d. “diritto europeo della cybersicurezza” sia evoluto nel corso dei primi decenni del nuovo millennio, a partire soprattutto dal 2013, anno della prima Strategia UE in materia. In questo contesto, i diversi atti giuridici adottati e, soprattutto, le tre Strategie della Commissione e dell'Alto Rappresentante dell'Unione per gli Affari Esteri e la Politica di Sicurezza, presentate a distanza rispettivamente di tre e quattro anni l'una dall'altra, segnalano come una politica dell'Unione fosse, da una parte, necessaria in un settore lasciato troppo a lungo senza una adeguata regolamentazione e, dall'altra, come il panorama delle minacce e della *governance* delle misure tecni-

¹²⁵ Art. 14, par. 4, CSoA.

¹²⁶ Art. 14, par. 5, CSoA.

¹²⁷ Art. 21, par. 1, CSoA.

¹²⁸ Art. 21, par. 3, CSoA.

che, organizzative ed operative di sicurezza – rispettivamente, la dimensione *offensiva* e *difensiva* della cybersicurezza – sia in continua e rapida evoluzione. Al tempo stesso, questa forte spinta regolamentativa non è solamente caratteristica del diritto della cybersicurezza, bensì più in generale delle politiche dell’Unione in materia digitale. Tale approccio ha tuttavia iniziato a raccogliere critiche¹²⁹.

Il diritto UE della cybersicurezza è andato nel tempo evolvendosi: da una legislazione incentrata sulle reti e sui sistemi informativi, di carattere più marcatamente tecnico-organizzativo, si è gradualmente passati ad un approccio normativo che protegge altri e diversi beni giuridici, con il coinvolgimento maggiore di un ampio ventaglio di portatori di interesse. In tal senso, il diritto UE della cybersicurezza può anche essere considerato come un’interfaccia privilegiata attraverso la quale è possibile analizzare l’adozione sempre più frequente di strategie regolatorie e di approcci normativi ibridi nel “diritto digitale dell’UE”. Come dimostrato nel corso del capitolo, questi approcci non si escludono a vicenda.

L’approccio normativo tradizionale del nuovo quadro legislativo in materia di sicurezza dei prodotti (*new legislative framework*, NLF) è stato sottoposto ad ibridazione con l’approccio basato sui diritti (c.d., *rights-based*)¹³⁰. Il CRA, infatti, introduce alcuni specifici meccanismi di *enforcement* attribuendo alle autorità nazionali competenti o, a determinate condizioni, alla Commissione, i tradizionali poteri correttivi e restrittivi propri del NLF (es., ritiro del prodotto dal mercato) qualora un prodotto con elementi digitali, pur conforme al regolamento, rappresenti un rischio per la conformità con la normativa a protezione dei diritti fondamentali.

Sotto altro profilo, il diritto UE della cybersicurezza è andato componendosi di strumenti giuridici “verticali” e “orizzontali”. Sempre per quanto riguarda la sicurezza dei prodotti (ricomprendendo, in questo contesto, sia la sicurezza intesa come *safety* che come *security*), diversi atti legislativi settoriali (approccio *verti-*

¹²⁹ V. PAPA-KONSTANTINO, P. DE HERT, *The Regulation of Digital Technologies in the EU: Actification, GDPR Mimesis and EU Law Brutality at Play*, cit.; M. DRAGHI, *The Future of European Competitiveness*, 2024, p. 26, https://commission.europa.eu/document/download/97e481fd-2dc3-412d-be4c-f152a8232961_en. Sul punto, la Commissione europea ha presentato a fine 2025 diverse proposte di revisione dei quadri normativi europei sul digitale (ie., Digital Omnibus e Digital Omnibus sull’IA), nonché proposte di emendamenti mirati alla direttiva NIS2 e una revisione più struttura del Cybersecurity Act ad inizio 2026.

¹³⁰ Anche il Regolamento (UE) 2024/1689 (c.d. AI Act) è caratterizzato dal rafforzamento del tradizionale approccio di sicurezza dei prodotti con specifici meccanismi di tutela dei diritti fondamentali. Si veda T. EVAS, *The EU Artificial Intelligence Act: Advancing Innovation for Trustworthy AI*, in *AIRe – Journal of AI Law and Regulation*, 2024 (1/1), p. 100; cfr. M. ALMADA, P. NICOLAS, *The EU AI Act: Between the rock of product safety and the hard place of fundamental rights*, in *Common Market Law Review*, 2025 (62/1).

cale) sono stati revisionati al fine di includere requisiti essenziali di cybersicurezza¹³¹. Allo stesso tempo, la Commissione ha proposto nel 2022 il Cyber Resilience Act, che introduce norme *orizzontali* di cybersicurezza per i prodotti con elementi digitali.

Un'altra tendenza che si può osservare nello sviluppo del diritto UE della cybersicurezza è l'adozione di approcci "multirischio". Le implicazioni sono duplici. Le misure tecniche, organizzative e operative di cybersicurezza non hanno più solamente il compito di fare fronte alle tradizionali minacce alla sicurezza digitale: devono anche tenere conto dell'ambiente fisico in cui si trovano le reti e i sistemi informativi, in un'ottica di protezione "olistica". Alla luce del rapporto complementare che intercorre tra sicurezza fisica e cybersicurezza, non sorprende che la direttiva NIS2 e la direttiva CER, che stabilisce misure per raggiungere la resilienza fisica delle entità critiche, debbano essere attuate in modo coordinato.

La seconda implicazione riguarda l'inclusione di fattori non tecnici come parte delle misure di gestione del rischio di cybersicurezza. Nel contesto delle valutazioni coordinate del rischio per la sicurezza delle catene di approvvigionamento critiche condotte dal gruppo di cooperazione NIS vengono presi in considerazione anche fattori non tecnici (es., geopolitici). Gli stessi fattori sono rilevanti anche nel contesto dell'applicazione del CRA: nel determinare l'importanza di un rischio di cybersicurezza, la Commissione e le autorità di vigilanza del mercato prendono in considerazione anche fattori di rischio non tecnici, in particolare quelli stabiliti a seguito delle summenzionate valutazioni di cui all'articolo 22 della direttiva NIS2.

Se, come abbiamo visto, la cybersicurezza gioca un ruolo sempre più rilevante nell'agenda della Commissione europea, lo stesso si può dire dei governi nazionali. Da una parte, la cybersicurezza è una componente chiave per il piano della ripresa europea *Next Generation EU*¹³². Dall'altra, guardando all'esperienza italiana, il Piano Nazionale di Resilienza e Resistenza (PNRR) ha stanziato 623 milioni di euro da investire nel contesto del recente quadro di governance introdotto dal Perimetro di Sicurezza Nazionale Cibernetica (PSNC)¹³³ nel 2019, poi ridisegnato

¹³¹ È il caso della Direttiva 2014/54/UE sulle apparecchiature radio, attraverso il Regolamento delegato UE 2022/30 volto a specificare a quali categorie di prodotti radio si applicano i requisiti essenziali di cui all'articolo 3, paragrafo 3, lettere d), e) ed f) della direttiva in materia di cybersicurezza; ancora, della Direttiva 2006/42/CE, abrogata dal Regolamento (UE) 2023/1230 che introduce *inter alia* specifici requisiti essenziali di cybersicurezza; infine, la Direttiva generale sulla sicurezza dei prodotti 2001/95/UE abrogata dal Regolamento (UE) 2023/988 che innova la disciplina introducendo aspetti di cybersicurezza per la valutazione della sicurezza di un prodotto.

¹³² COMMISSIONE EUROPEA, *Il momento dell'Europa: riparare i danni e preparare il futuro per la prossima generazione*, COM, 2020, 98 final.

¹³³ Decreto-legge 21 settembre 2019, n. 105.

dal decreto-legge 14 giugno 2021, n. 82 che istituisce l'Agenzia per la Cybersicurezza Nazionale, aderendo pertanto ad un modello centralizzato.

I REATI INFORMATICI E LA VIOLAZIONE DEI DIRITTI DELLA PERSONA IN RETE

Francesco Di Tano

SOMMARIO: 1. I reati informatici. 2. Le fattispecie di reato informatico in senso stretto. 3. Manifestazione del pensiero e condotte antisociali in rete. 4. L'odio online. 5. Cyberstalking, cyberbullismo e diffusione illecita di immagini sessualmente esplicite.

1. I reati informatici

L'evoluzione tecnologica che dal secolo scorso ha progressivamente trasformato la società, conducendo a una digitalizzazione pervasiva delle attività umane, ha inevitabilmente generato, accanto ai numerosi benefici, nuove opportunità di utilizzo distorto delle tecnologie a fini illeciti e criminali¹.

Il legislatore italiano ha progressivamente maturato la consapevolezza della necessità di predisporre strumenti normativi idonei al contrasto delle condotte illecite perpetrate mediante l'uso delle tecnologie informatiche, ma solo nel 1993, con l'emanazione della legge recante «Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica»², si è avuto un avanzamento sistematico in materia. Tale quadro normativo ha, difatti, rappresentato il primo intervento organico volto a introdurre nell'ordinamento penale italiano una disciplina specifica dei reati informatici³.

In tale sede, il codice penale è stato oggetto di un intenso aggiornamento, mediante l'inserimento di nuove figure incriminatrici finalizzate a sanzionare condotte lesive realizzate attraverso l'impiego di strumenti informatici e telematici. Tra le nuove disposizioni, si annoverano: l'accesso non autorizzato a un sistema informatico o telematico (art. 615-ter c.p.), la detenzione e diffusione abusiva di credenziali di accesso (art. 615-quater c.p.), la propagazione di soft-

¹ G. FIANDACA, E. MUSCO, *Diritto penale. Parte speciale*, vol. II, tomo 1, Bologna: Zanichelli, 2024.

² L. n. 547/1993 del 23 dicembre 1993.

³ A. CADOPPI ET AL., *Trattato di Diritto penale – Cybercrime*, Milano: Utet Giuridica, 2023.

ware finalizzati al danneggiamento o all'interruzione dei sistemi informatici (art. 615-*quinqüies* c.p.), l'intercettazione e l'interruzione illecita di comunicazioni informatiche o telematiche (art. 617-*quater* c.p.), nonché l'installazione di dispositivi tecnici volti a tali finalità (art. 617-*quinqüies* c.p.) e la manipolazione del contenuto delle comunicazioni elettroniche (art. 617-*sexies* c.p.).

Parallelamente, talune ipotesi delittuose già presenti nel corpus codicistico sono state opportunamente ampliate o adattate, al fine di contemplare nuove modalità esecutive realizzabili per mezzo delle tecnologie informatiche. È il caso, ad esempio, dei reati di esercizio arbitrario delle proprie ragioni mediante violenza sulle cose (art. 392 c.p.), attentato agli impianti di pubblica utilità (art. 420 c.p.) e violazione, sottrazione o soppressione della corrispondenza (art. 616 c.p.).

Il legislatore, in tale processo evolutivo, ha adottato un approccio fondato sull'invarianza del bene giuridico tutelato e sulla conseguente adeguata rimodulazione delle tecniche di aggressione, rese possibili dall'evoluzione tecnologica. In altre parole, non si è assistito a un mutamento degli interessi protetti, bensì a un aggiornamento degli strumenti repressivi finalizzato a intercettare nuove modalità di offesa.

Il più significativo sviluppo del nostro ordinamento si è registrato, nel 2008, con la ratifica della Convenzione di Budapest sulla criminalità informatica⁴, sottoscritta in ambito internazionale per dare una risposta unitaria e transnazionale al fenomeno, che per sua natura trascende i confini statali. L'adesione alla Convenzione ha comportato un complessivo aggiornamento del diritto penale sostanziale e processuale interno.

In ambito sostanziale, si è assistito, da un lato, all'estensione dell'ambito applicativo dell'art. 615-*quinqüies* c.p., che ha ricompreso non più solo i "programmi" ma anche le "apparecchiature" e i "dispositivi" informatici predisposti a finalità distruttive o interruttive; dall'altro lato, all'introduzione di nuove fattispecie incriminatrici relative al danneggiamento informatico (artt. 635-*bis*, 635-*ter*, 635-*quater* e 635-*quinqüies* c.p.), nonché di reati connessi all'identità digitale, quali la falsa dichiarazione o attestazione al certificatore sull'identità personale (art. 495-*bis* c.p.) e la truffa ai danni del certificatore di firma elettronica (art. 640-*quinqüies* c.p.).

Sul versante processual-penalistico, invece, modificando l'art. 51 c.p.p., la riforma ha previsto la concentrazione della competenza territoriale in capo all'ufficio del pubblico ministero presso il tribunale del capoluogo del distretto nel cui ambito ha sede il giudice competente, e ha inciso su rilevanti disposizio-

⁴ L. n. 48/2008 del 18 marzo 2008.

ni in materia di ispezione, perquisizione e sequestro, introducendo l'obbligo per l'autorità giudiziaria di adottare misure tecniche e prescrizioni idonee a garantire l'integrità e la conservazione dei dati, dei programmi e delle infrastrutture informatiche, nonché a impedirne ogni forma di alterazione, compromissione o dispersione.

In questo quadro generale si inserisce la distinzione definitoria tra reati necessariamente informatici e reati eventualmente informatici⁵. I primi, detti anche propri o in senso stretto, presuppongono necessariamente l'impiego di strumenti informatici o telematici, sia come mezzo attraverso il quale si realizza la condotta criminosa (ad esempio, mediante software o accessi abusivi), sia come oggetto giuridico dell'offesa (come nel caso di un sistema informatico violato o danneggiato). In altri termini, tali reati non sarebbero concepibili al di fuori del contesto digitale.

I secondi, invece, definiti anche impropri, non implicano strutturalmente l'uso di strumenti digitali, ma possono essere commessi anche mediante il ricorso a essi. Si tratta di reati comuni, quali la truffa, la diffamazione o lo *stalking*, che acquisiscono una dimensione informatica solo quando la condotta viene realizzata tramite strumenti telematici, come e-mail, social network o applicazioni di messaggistica.

2. Le fattispecie di reato informatico in senso stretto

Le fattispecie di reato informatico in senso stretto rappresentano il nucleo più tipico e strutturato della criminalità digitale, in quanto delineano ipotesi delittuose che presuppongono l'impiego necessario di strumenti informatici o telematici, sia come mezzo esecutivo della condotta sia come oggetto materiale dell'offesa.

In questo paragrafo saranno analizzate, in chiave sistematica, le principali incriminazioni previste dal codice penale per la tutela del cosiddetto domicilio informatico e dell'integrità dei sistemi e dei dati, individuando per ciascuna di esse il bene giuridico protetto, gli elementi costitutivi e le principali problematiche interpretative.

Tra le fattispecie maggiormente significative rientra, innanzitutto, quella dell'accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.), che prevede la punibilità per chiunque si introduca indebitamente all'interno di un sistema informatico o telematico protetto da misure di sicurezza, ovvero vi

⁵ S. PIETROPAOLI, *Informatica criminale. Diritto e sicurezza nell'era digitale*, Torino: Giappichelli, 2025.

si trattenga contro la manifestazione, anche implicita, della volontà contraria da parte del titolare del diritto di esclusione.

La disposizione contempla due condotte alternative – l'accesso abusivo e la permanenza illecita – che si pongono in violazione della riservatezza e della sfera di controllo del legittimo titolare del sistema. Il bene giuridico protetto è comunemente identificato nel domicilio digitale, concetto giuridico che estende, in chiave evolutiva, la tutela del domicilio individuale anche agli ambienti virtuali, intesi come luoghi di pertinenza personale protetti costituzionalmente. L'equiparazione, sotto il profilo strutturale, con la figura di reato della violazione di domicilio, disciplinata dall'art. 614 c.p., rivela la volontà del legislatore di trasporre nel contesto digitale le medesime garanzie riconosciute agli spazi fisici privati.

In sede interpretativa, la Corte di Cassazione a Sezioni Unite ha ulteriormente chiarito, nel tempo, che la fattispecie è integrata anche qualora il soggetto, pur legittimato all'accesso, utilizzi il sistema per scopi radicalmente difformi rispetto a quelli per cui tale abilitazione era stata concessa⁶.

La detenzione e diffusione abusiva di codici di accesso a sistemi informatici e telematici (art. 615-*quater* c.p.) configura un illecito penale a carattere strumentale rispetto alla precedente figura criminosa. Tale disposizione punisce chiunque, con finalità di lucro o con l'intento di arrecare pregiudizio ad altri, si procuri, riproduca, distribuisca, comunichi o ceda, senza legittimazione, codici di identificazione, parole chiave, strumenti d'accesso o ogni altro mezzo idoneo a consentire l'intrusione in sistemi informatici o telematici protetti, ovvero fornisca istruzioni, indicazioni o procedure utili allo stesso scopo. Anche in questa ipotesi, il bene tutelato è il domicilio informatico, la cui inviolabilità costituisce presupposto fondamentale per la sicurezza e la riservatezza delle comunicazioni digitali. Sotto il profilo soggettivo, la norma richiede dolo specifico, configurato dall'intenzione di conseguire un vantaggio patrimoniale o di cagionare un danno a terzi, elementi che accentuano la pericolosità della condotta anche nella fase meramente preparatoria dell'illecito informatico.

Un ulteriore passo in avanti nella repressione delle condotte informatiche lesive è rappresentato dalla previsione di reati a carattere preparatorio, volti a colpire la diffusione di strumenti informatici dannosi.

La messa a disposizione di strumenti informatici destinati a causare danno o a compromettere la funzionalità dei sistemi (art. 615-*quinqüies* c.p.) sanziona penalmente tutte le condotte, anche meramente preparatorie, consistenti nella produzione, nell'acquisizione, nella riproduzione, nella diffusione, nella comu-

⁶ Cass., Sez. Un., 27 ottobre 2011, n. 4694; Cass., Sez. Un., 8 settembre 2017, n. 41210.

nicazione o nella cessione di dispositivi hardware o software concepiti con lo scopo di compromettere l'integrità, la sicurezza o il corretto funzionamento di un sistema informatico o delle informazioni, dati o programmi in esso contenuti o ad esso collegati. La norma si rivolge a una pluralità di comportamenti che precedono l'attacco vero e proprio, mirando a reprimere la filiera tecnologica dell'offesa informatica. Sono comprese, ad esempio, le attività connesse alla distribuzione di *malware*, *virus*, *worm*, *trojan*, *spyware*, *rootkit*, *keylogger* o altri strumenti digitali potenzialmente distruttivi. L'offesa si realizza nei confronti del domicilio digitale e dell'integrità dei dati, e l'elemento psicologico richiesto è, anche in questo caso, il dolo specifico, ossia la finalità univoca di ledere un sistema informatico o ostacolarne il funzionamento.

Particolarmente delicata è anche la tutela della riservatezza delle comunicazioni digitali, oggetto di specifiche incriminazioni.

L'art. 617-*quater* c.p. («Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche») incrimina chiunque, fraudolentemente, intercetti comunicazioni relative a un sistema informatico o telematico ovvero intercorrenti tra più sistemi collegati, nonché chi ne impedisca o ne interrompa lo svolgimento, anche in assenza di captazione del contenuto. L'introduzione di tale norma, ispirata al parallelo disposto dell'art. 617 c.p. in materia di comunicazioni telefoniche, risponde all'esigenza di offrire protezione penale alla riservatezza delle comunicazioni digitali, quale espressione del diritto alla privacy e della libertà individuale nelle interazioni elettroniche.

Il legislatore configura tre condotte alternative, accomunate dall'elemento soggettivo del dolo generico: (i) l'intercettazione, ossia la captazione non autorizzata del flusso di dati in transito tra sistemi; (ii) l'impedimento, consistente nell'interferenza che ostacola lo svolgimento regolare della comunicazione; (iii) l'interruzione, che implica l'arresto forzoso della trasmissione in corso. Sotto il profilo oggettivo, il reato è integrato anche se la comunicazione non è contenutisticamente significativa, poiché ciò che rileva è l'illecita ingerenza nel flusso comunicativo digitale, indipendentemente dal contenuto intercettato.

Strettamente connesso al precedente, l'art. 617-*quinquies* c.p. («Installazione di apparecchiature atte a intercettare comunicazioni informatiche o telematiche») punisce la condotta di chi installa apparecchiature o strumenti informatici idonei all'intercettazione, all'impedimento o all'interruzione di comunicazioni informatiche o telematiche. Il presupposto di tipicità è l'idoneità tecnica dei dispositivi alla realizzazione dell'attività lesiva: ne consegue che l'integrazione della fattispecie può aversi anche in assenza di un'effettiva intercettazione o interruzione, purché l'installazione sia funzionalmente orientata a tal fine. La norma si configura come reato di pericolo concreto, volto a prevenire la compromissione della segretezza delle comunicazioni digitali già nella fase preparatoria,

mediante la predisposizione degli strumenti tecnici finalizzati all'offesa. La *ratio legis* è evidentemente preventiva e anticipatoria, nella misura in cui mira a reprimere non tanto il risultato lesivo quanto la semplice predisposizione materiale dei mezzi per conseguirlo.

La protezione dell'integrità delle comunicazioni trova ulteriore sviluppo nella norma che incrimina la falsificazione del loro contenuto.

Con l'art. 617-*sexies* c.p. («Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche»), difatti, il legislatore ha introdotto una specifica incriminazione per chi modifica, altera, falsifica o sopprime il contenuto di una comunicazione informatica o telematica durante la trasmissione, rendendola difforme da quella originariamente inviata o ricevuta. Si tratta di una fattispecie che tutela la genuinità e l'affidabilità del contenuto informativo trasmesso, elementi fondamentali per il corretto funzionamento della rete e per la tutela dell'identità digitale.

L'illecito si perfeziona attraverso una manipolazione fraudolenta dei dati in transito, con conseguente alterazione dell'integrità comunicativa, potenzialmente idonea a produrre conseguenze significative, sia patrimoniali sia personali, in ambiti quali la contrattualistica online, la posta elettronica certificata o la trasmissione di documenti elettronici con valore legale. Sotto il profilo soggettivo, è richiesto il dolo generico, consistente nella coscienza e volontà di modificare il contenuto trasmesso, anche in assenza di un fine di lucro o di danno.

Accanto alla tutela del domicilio e della comunicazione informatica, centrale è anche la salvaguardia dell'integrità dei dati e dei sistemi, oggetto di un'articolata disciplina in tema di danneggiamento.

Il danneggiamento informatico (art. 635-*bis* c.p.), modellato sulla figura generale del danneggiamento di cui all'art. 635 c.p., punisce chiunque, salvo che il fatto non costituisca reato più grave e su querela di parte, distrugga, comprometta, alteri, cancelli o renda inservibili dati, programmi o informazioni informatiche altrui. La disposizione configura un reato di evento, la cui tipicità si compie attraverso una condotta che incide materialmente sull'integrità dei dati o dei programmi. La norma prevede un aggravamento della pena se il comportamento è realizzato mediante violenza alla persona, minaccia o abuso della propria qualità di operatore di sistema. In questa prospettiva, il bene giuridico tutelato è il patrimonio digitale, inteso quale estensione del patrimonio tradizionale alla dimensione immateriale dei contenuti informatici.

A partire dalla riforma introdotta con la legge 48/2008, il legislatore ha successivamente articolato una serie di figure di danneggiamento informatico aggravato, che completano il quadro punitivo rispetto alla fattispecie precedente e contemplano casi di maggiore allarme sociale: il danneggiamento di informazioni, dati e programmi informatici pubblici o di interesse pubblico (art. 635-*ter*

c.p.), che colpisce le condotte lesive aventi a oggetto sistemi informatici o telematici di pubblica utilità, la cui compromissione può incidere su servizi essenziali (trasporti, energia, sanità, telecomunicazioni); il danneggiamento di sistemi informatici o telematici (art. 635-*quater* c.p.); la detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 635-*quater* 1 c.p.); il danneggiamento di sistemi informatici o telematici di pubblico interesse (art. 635-*quinquies* c.p.), che punisce la distruzione o l'alterazione di sistemi informatici o telematici appartenenti allo Stato o a enti pubblici, tutelando così l'integrità delle infrastrutture digitali strategiche.

Tutte queste ipotesi sono connotate da un'intensificazione della risposta penale, giustificata dalla particolare rilevanza pubblica del bene giuridico offeso, che viene ad assumere una funzione sistemica nell'organizzazione amministrativa, economica o di sicurezza nazionale.

A chiusura della rassegna delle principali fattispecie informatiche in senso stretto, si colloca il reato di frode informatica (art. 640-*ter* c.p.), che rappresenta una trasposizione tecnologica della truffa (art. 640 c.p.), rispetto alla quale si distingue per l'oggetto e per le modalità di esecuzione. Tale fattispecie prevede la punibilità per chiunque, mediante alterazione del funzionamento di un sistema informatico o telematico, ovvero intervenendo senza diritto su dati, informazioni o programmi ivi contenuti o ad esso connessi, ne modifichi l'elaborazione e ottenga, per sé o per altri, un vantaggio indebito con altrui pregiudizio. La frode informatica si configura come reato di risultato, che si consuma nel momento in cui si verifica l'ingiusto profitto con contestuale danno patrimoniale. Tipico è il caso del phishing, tecnica fraudolenta consistente nell'indurre le vittime a rivelare informazioni riservate, solitamente credenziali bancarie, mediante messaggi ingannevoli apparentemente provenienti da enti affidabili. La specificità della norma risiede nella protezione della fiducia nei sistemi informatici come ambienti sicuri per l'elaborazione e la conservazione dei dati.

3. Manifestazione del pensiero e condotte antisociali in rete

Da sempre, il potere di comunicare e diffondere informazioni ha sempre costituito uno degli strumenti più efficaci di controllo e legittimazione del potere istituzionale. Oggi, nell'era dell'informazione pervasiva e delle reti digitali, tale potere è stato redistribuito, ridefinito e potenziato⁷.

⁷ M. CASTELLS, *Communication, Power and Counter-power in the Network Society*, in *International Journal of Communication*, 2007 (1), pp. 238-266.

Con la propria struttura aperta, interattiva, globale e asincrona, Internet ha rivoluzionato radicalmente il modo in cui gli individui manifestano il proprio pensiero, accedono alla conoscenza, si relazionano e partecipano alla vita democratica. La rete abbattuto, nel tempo, le tradizionali barriere spaziali, temporali ed economiche.

Oggi l'individuo detiene il potere di comunicare pubblicamente – in forma decentralizzata e globale – idee, opinioni, contenuti artistici e rivendicazioni sociali. Si è così affermato un nuovo paradigma comunicativo, in cui la libertà di espressione si intreccia con l'autonomia creativa, l'accesso all'informazione e la partecipazione collettiva alla cultura democratica⁸.

Tuttavia, le stesse tecnologie che hanno democratizzato la comunicazione hanno anche creato nuove asimmetrie e vulnerabilità. La possibilità di esprimersi in maniera (apparentemente) anonima o pseudonima, l'abbattimento delle mediazioni editoriali, la persistenza dei contenuti e l'elevata viralità degli stessi hanno favorito la proliferazione di condotte lesive della dignità, della reputazione e della sicurezza delle persone. Diffamazione online, campagne d'odio, cyberstalking, divulgazione di informazioni personali (*doxing*), incitamento alla violenza e diffusione di fake news rappresentano manifestazioni patologiche del nuovo ecosistema informativo e comunicativo, spesso integrando fattispecie di reato informatico improprio.

La libertà di espressione nell'ambiente online assume così una dimensione profondamente ambivalente: da un lato, strumento di emancipazione, autodefinizione e costruzione identitaria; dall'altro, veicolo di oppressione, discriminazione e lesione dei diritti altrui. Tale ambivalenza è particolarmente evidente nell'uso dell'anonimato, che può essere garanzia di libertà nei regimi oppressivi, protezione della privacy in contesti vulnerabili, oppure strumento di impunità e deresponsabilizzazione per condotte offensive o criminali.

Inoltre, l'ambiente digitale incide profondamente sulla configurazione della responsabilità individuale, introducendo variabili che alterano le ordinarie dinamiche di controllo sociale. L'apparente anonimato offerto dalle interazioni online riduce la percezione di esposizione personale, inducendo l'utente a ritenersi al riparo da conseguenze giuridiche o sociali. Tale condizione, ancorché tecnicamente superabile attraverso strumenti di tracciabilità (quali l'identificazione dell'indirizzo IP o la conservazione dei log da parte dei provider), continua a produrre rilevanti effetti psicologici e comportamentali. In particolare, si assiste a fenomeni di cosiddetta “deindividuazione”⁹, in cui la distanza fi-

⁸ J.M. BALKIN, *Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation*, in *UC Davis Law Review*, 2018 (51), pp. 1149-1210.

⁹ La “deindividuazione” è identificata come un processo psicologico che si manifesta in con-

sica, l'assenza di segnali visivi e la mancanza di feedback diretti disinibiscono l'agente, favorendo condotte impulsive e, talvolta, antisociali. Questo contesto favorisce una percezione attenuata del nesso tra azione e responsabilità: il soggetto non si percepisce come pienamente autore della propria condotta, soprattutto quando essa si inserisce in dinamiche collettive.

A ciò si affianca il fenomeno della *group polarization*, per cui l'aggregazione virtuale tra utenti portatori di opinioni affini amplifica le tendenze iniziali e le estremizza¹⁰. Ne derivano effetti distorsivi anche sul piano della responsabilità penale e civile, specie quando le condotte lesive si manifestano in modo diffuso, reiterato e apparentemente spontaneo, come nei casi di campagne d'odio online, diffamazioni collettive, o molestie digitali.

In tale cornice, la rete si configura come un ambiente comunicativo che, per la sua struttura e per i meccanismi algoritmici che ne regolano la visibilità dei contenuti, può facilitare la normalizzazione del discorso d'odio e la banalizzazione delle offese personali.

Emergono, dunque, forme di responsabilità diffuse, spesso frammentate e difficili da attribuire a un singolo autore, ma che producono effetti reali e profondi sulla dignità, la reputazione e la sicurezza della persona.

In questo scenario, il diritto è chiamato a un compito arduo: garantire la libertà di manifestazione del pensiero e, al contempo, proteggere i diritti fondamentali degli individui. L'ordinamento giuridico è sollecitato a ripensare categorie, strumenti e modelli di tutela¹¹. I reati contro la persona tradizionali – come la diffamazione, la minaccia o la molestia – assumono nuove configurazioni e richiedono interpretazioni adeguate alla specificità dei contesti digitali. Inoltre, emergono nuove figure criminose, spesso prive di corrispettivo nel diritto penale classico, come la diffusione illecita di immagini intime, il *deepfake*, la manipolazione algoritmica di contenuti, la diffusione massiva di dati sensibili o la costruzione di identità fittizie a fini lesivi.

Tutto ciò avviene in un contesto normativo frammentato, dove il diritto fatica ad adattarsi alla mutevolezza delle tecnologie e alla transnazionalità delle condotte. Di qui la necessità di un approccio multilivello, regolatorio e tecnico,

testi collettivi caratterizzati da elevato anonimato e dalla ridotta focalizzazione sull'identità individuale, e che comporta un indebolimento della consapevolezza di sé e delle capacità di giudizio critico, favorendo la conformazione dell'individuo alle norme e ai comportamenti prevalenti nel gruppo, indipendentemente dal loro valore etico o giuridico. Per approfondimenti: P. ZIMBARDO, *The Human Choice: Individuation, Reason, and Order versus Deindividuation, Impulse, and Chaos*, in *Nebraska Symposium on Motivation*, 1969 (15), pp. 237–307.

¹⁰ C.R. SUNSTEIN, *The Law of Group Polarization*, in *Journal of Political Philosophy*, 2002 (10), pp. 175–195.

¹¹ R. COHEN-ALMAGOR, *Speech, Media, and Ethics: The Limits of Free Expression*, London: Palgrave-Macmillan, 2005.

capace di garantire in modo bilanciato la libertà e la responsabilità, la partecipazione e la tutela, l'innovazione e la giustizia.

La protezione della libertà di manifestazione del pensiero nella società digitale non è più soltanto questione di limiti e garanzie giuridiche, ma coinvolge direttamente l'architettura tecnologica, le logiche algoritmiche, il design delle piattaforme e le politiche aziendali.

4. L'odio online

I sentimenti di ostilità, le tensioni sociali e le loro manifestazioni espressive accompagnano l'umanità fin dalle epoche più antiche. L'avvento di Internet e delle tecnologie digitali, più che creare un fenomeno del tutto nuovo, ha contribuito a inasprire problemi già radicati nel tessuto storico-culturale della società umana contemporanea.

Gruppi e singoli individui hanno sfruttato le potenzialità tecniche della rete per commettere azioni antisociali, illecite e offensive, tra cui messaggi intolleranti, ideologie estremiste e atteggiamenti persecutori.

L'odio online si manifesta comunemente contro minoranze etniche e religiose, personalità politiche, oppure contro individui presi di mira per i più disparati motivi, dalla discriminazione razziale o sessuale al semplice desiderio di denigrazione, vendetta o rivalsa¹². Le conseguenze di queste condotte destano crescente preoccupazione nei sistemi democratici, poiché minano la dignità, la sicurezza personale e la reputazione delle persone colpite¹³.

La peculiarità dell'ambiente digitale risiede nel potenziale di amplificazione e persistenza: le azioni offensive possono ripetersi in modo ossessivo, raggiungere un pubblico vastissimo e rimanere accessibili nel tempo, aggravando i danni rispetto alle condotte offline.

Insulti, *trolling*, *doxing*, minacce esplicite, incitamenti all'odio razziale o sessista, campagne di denigrazione pubblica sono solo alcuni esempi di condotte eterogenee non facilmente riconducibili a un'unica fattispecie.

¹² S.A. CASTAÑO-PULGARÍN ET AL., *Internet, social media and online hate speech. Systematic review*, in *Aggression and Violent Behavior*, 2021 (58); A. VERZA, "Mascolinità tossica" sul web: la "cultura" dell'odio antifemminista online, in A. VERZA, S. VIDA (a cura di), *Postfemminismo e neoliberalismo*, Roma: Aracne, 2020, pp. 157-196; L. DE FAZIO, C. SGARBI, *Unwanted Online Attention Among an Italian Students Sample*, in *European Journal on Criminal Policy and Research*, 2016 (22), pp. 219-234.

¹³ B.G. BELLO, L. SCUDIERI, *L'odio online: forme, prevenzione e contrasto*, Torino: Giappichelli, 2022; F. DI TANO, *Hate speech e molestie in rete. Profili giuridici e prospettive de iure condendo*, Roma: Aracne, 2019; G. ZICCARDI, *L'odio online. Violenza verbale e ossessioni in rete*, Milano: Raffaello Cortina, 2016; D.K. CITRON, *Hate Crimes in Cyberspace*, Cambridge, Mass.: Harvard University Press, 2014; J. WALDRON, *The Harm in Hate Speech*, Cambridge, Mass.: Harvard University Press, 2012.

Le aggressioni *online* penetrano nella sfera privata delle vittime, spesso prevedendo altresì l'accesso ai loro dispositivi o account personali allo scopo di raccogliere informazioni riservate o intime. La divulgazione di tali dati può determinare conseguenze immediate, come furti di identità, discriminazioni lavorative, azioni persecutorie dentro e fuori dal web e un persistente senso di insicurezza.

In *altre* circostanze, l'offesa si realizza attraverso la diffusione di contenuti diffamatori, in grado di compromettere la vita relazionale e professionale della persona offesa, oppure attraverso pratiche di esclusione virtuale, come la chiusura forzata di pagine o blog, fino ad arrivare ad attacchi informatici (come, ad esempio, gli attacchi *denial-of-service*, o DDoS) che bloccano l'accesso a piattaforme e servizi.

Si tratta, in generale, di comportamenti reiterati e distruttivi, che incidono profondamente sul benessere psicologico della vittima, con un'ampia gamma di conseguenze emotive: dall'ansia e dal senso di rabbia o tristezza, a forme più gravi di angoscia, depressione e tendenze suicidarie, specialmente se le molestie virtuali si sommano a episodi di violenza o *stalking* nella vita reale.

A fronte di queste dinamiche, gli strumenti normativi tradizionali – come le norme incriminatrici dei reati di diffamazione, minaccia, molestia, nonché propaganda e istigazione a delinquere per motivi di discriminazione razziale etnica e religiosa – si mostrano spesso inadeguati, sia per la varietà delle forme di aggressione digitale sia per l'assenza di una disciplina unitaria a livello sovranazionale.

Le condotte più tradizionali di odio online interpersonale possono rientrare nell'ambito della diffamazione aggravata dal mezzo di pubblicità (art. 595, comma 3 c.p.) o della molestia (art. 660 c.p.), che tuttavia presentano pene editoriali particolarmente basse e non sempre proporzionate rispetto alla gravità delle condotte e dei danni procurati alle vittime. Forme relativamente più recenti e complesse come il *cyberstalking*, il cyberbullismo e la diffusione illecita di immagini sessualmente esplicite hanno invece assunto una fisionomia autonoma, tanto da richiedere un intervento normativo specifico che ne riconoscesse la gravità e l'impatto sociale.

In questo quadro, l'esigenza di regolazione dei contenuti online evidenzia una costante tensione tra libertà di espressione e necessità di tutela da contenuti illeciti o dannosi.

In una prima fase, la governance digitale è stata affidata prevalentemente ai termini contrattuali di utilizzo delle piattaforme: YouTube, con la propria Hate Speech Policy, vieta i contenuti che incitano all'odio verso gruppi protetti; Facebook, attraverso i Community Standards, e Twitter/X, tramite le Rules and Policies, hanno previsto divieti in materia di terrorismo, violenza e hate speech, riservandosi la rimozione discrezionale dei contenuti; Google ha adottato pro-

cedure di *notice and take down* conformi al modello statunitense del Digital Millennium Copyright Act (DMCA)¹⁴. Tali strumenti, pur garantendo un minimo di disciplina, sollevano dubbi sulle garanzie di trasparenza e libertà di manifestazione del pensiero, con il rischio di un'eccessiva privatizzazione della censura.

Per ridurre tali squilibri, le istituzioni europee hanno progressivamente introdotto strumenti di soft law, tra cui in particolare: il Codice di condotta sull'illecito incitamento all'odio online del 2016, poi aggiornato nel gennaio 2025¹⁵, promosso dalla Commissione europea e sottoscritto da Facebook, Twitter, YouTube e Microsoft; il Codice di buone pratiche sulla disinformazione del 2018, aggiornato nel 2022, volto al contrasto delle fake news¹⁶; la Raccomandazione del Consiglio d'Europa CM/Rec(2018)2 sul ruolo e sulla responsabilità degli intermediari della rete. Tali strumenti, tuttavia, hanno mostrato, ad oggi, limiti per la loro natura privatistica e non cogente.

Un passaggio evolutivo, quantomeno sotto il profilo del diritto positivo, si è avuto con il *Digital Services Act* (Regolamento UE 2022/2065), il quale, pur confermando quanto previsto dalla già sancito dalla Direttiva 2000/31/CE sul commercio elettronico sull'assenza di un obbligo generale di sorveglianza e sulla distinzione delle responsabilità degli intermediari in base alla funzione (semplice trasporto e *mere conduit*, memorizzazione temporanea o *caching*, memorizzazione di informazioni o *hosting*), introduce obblighi procedurali di *notice and action* (meccanismo di segnalazione e azione, disciplinato agli artt. 16 e 17), di notifica di sospetti di reati (art. 18), di sistemi di reclamo e ricorso per gli utenti (artt. 20-21), di adozione di misure adeguate per la protezione dei minori, e prevede obblighi rafforzati e supplementari per i fornitori di piattaforme online di dimensioni molto grandi e di motori di ricerca online di dimensioni molto grandi per la gestione dei rischi sistemici¹⁷ (artt. 33-43).

In definitiva, il percorso normativo europeo riflette il passaggio da un modello di autoregolamentazione privata (*policies* e condizioni contrattuali) e di soft law (raccomandazioni, codici di condotta) a un sistema vincolante di diritto po-

¹⁴ Digital Millennium Copyright Act, Pub. L. 105-304, 112 Stat. 2860 (1998), 17 U.S.C. § 512.

¹⁵ Il 20 gennaio 2025, il Codice di condotta è stato revisionato per la sua integrazione nel quadro del Digital Services Act (Regolamento UE 2022/2065), a seguito della valutazione positiva della Commissione UE e del comitato europeo per i servizi digitali.

¹⁶ Il 13 febbraio 2025, la Commissione UE e il comitato europeo per i servizi digitali hanno approvato l'integrazione del Codice di buone pratiche sulla disinformazione del 2022 come codice di condotta nel quadro del Digital Services Act, analogamente al Codice di condotta sull'illecito incitamento all'odio online.

¹⁷ Il DSA classifica le piattaforme o i motori di ricerca che hanno un numero medio mensile di destinatari attivi del servizio nell'Unione Europea pari o superiore a 45 milioni come piattaforme online di dimensioni molto grandi (conosciuti anche con l'acronimo inglese "VLOP", da *very large online platforms*) o motori di ricerca online di dimensioni molto grandi (detti anche "VLOSE", da *very large online search engines*).

sitivo, nel quale gli intermediari cessano di essere meri soggetti tecnici e assumono un ruolo centrale e responsabilizzato nella governance digitale.

5. *Cyberstalking*, cyberbullismo e diffusione illecita di immagini sessualmente esplicite

I fenomeni del *cyberstalking*, del cyberbullismo e della diffusione illecita di immagini sessualmente esplicite costituiscono, attualmente, le declinazioni più insidiose della devianza relazionale e dell'aggressione alla persona nell'era digitale¹⁸. Sebbene eterogenei nelle modalità e nei soggetti coinvolti, condividono una matrice comune: l'utilizzo sistematico delle tecnologie informatiche come strumento di controllo, umiliazione, intimidazione o punizione, con effetti profondamente destabilizzanti sulla vittima e sulla tenuta del tessuto sociale.

Nella cornice criminologica e psichiatrica, lo *stalking* tradizionale è stato a lungo riconosciuto come una forma patologica di relazione, collocabile tra i disturbi del comportamento affettivo e relazionale. Si manifesta attraverso un insieme di comportamenti reiterati – pedinamenti, appostamenti, telefonate insistenti, invio di regali indesiderati o di messaggi minacciosi – volti a interferire nella vita della vittima, compromettendone l'autonomia, generando un clima di costante paura e inducendo gravi alterazioni dell'equilibrio psicologico. L'aggressore, spesso, giustifica le proprie azioni sulla base di un presunto diritto morale o di un sentimento legittimo, pur riconoscendone talvolta l'illiceità giuridica.

Con la capillare diffusione delle reti digitali e la pervasività dei social network, tali condotte hanno assunto nuove forme, dando origine a quella variante nota come *cyberstalking*, ossia l'uso intenzionale e ripetuto di strumenti telematici per molestare, controllare, minacciare o denigrare un'altra persona.

Le modalità operative del *cyberstalker* possono variare notevolmente: dall'invio reiterato di e-mail offensive o intimidatorie alla pubblicazione di immagini private senza consenso, passando per la creazione di profili falsi per la diffusione di contenuti denigratori o l'accesso illecito ai dispositivi elettronici

¹⁸ Per un'analisi più dettagliata delle singole fattispecie, si vedano: G. CASSANO, *Stalking, atti persecutori, cyberbullismo e tutela dell'oblio*, Milano: Ipsoa, 2017; L. DE FAZIO, C. SGARBI, *Nuove prospettive di ricerca in materia di atti persecutori: il fenomeno del cyberstalking*, in *Rassegna Italiana di Criminologia*, 2012 (3), pp. 146-159; A. VERZA, "Quest" identitaria mediata dal web, (cyber)bullismo e stratificazione sociale alla luce di un singolare caso di "devianza" di massa", in *Studi sulla Questione Criminale*, 2015 (2-3), pp. 129-150; M. BIANCHI, *L'incriminazione del "revenge porn": il nuovo delitto di "diffusione illecita di immagini o video sessualmente espliciti"*, in A. CADOPPI ET AL. (a cura di), *Diritto penale, Tomo III*, Milano: Utet Giuridica, 2022, pp. 6568-6569; D.K. CITRON, M.A. FRANKS, *Criminalizing Revenge Porn*, in *Wake Forest Law Review* 2014 (49), pp. 345-391.

della vittima tramite software malevoli (*trojan*, *spyware*, *keylogger*) per sorvegliarne le attività o sottrarre dati sensibili.

L'uso di applicazioni di messaggistica istantanea e strumenti di geolocalizzazione in tempo reale ha ulteriormente accresciuto l'invasività del fenomeno, consentendo al persecutore di monitorare ogni spostamento della vittima, rafforzando la sua percezione di vulnerabilità e il senso di costante minaccia.

In questo contesto, la letteratura criminologica ha sottolineato come la rete digitale abbia intensificato il processo di vittimizzazione, amplificando il rischio legato alla condivisione volontaria di informazioni personali – foto, contatti, preferenze – che possono essere facilmente reperite e strumentalizzate dal molestatore. L'illusione di uno spazio privato si dissolve, e la distinzione tra ciò che è pubblico e ciò che dovrebbe restare riservato si fa sempre più labile.

Le vittime sviluppano spesso stati ansiosi, depressione, disturbi del sonno e dell'alimentazione, crisi di panico e rabbia, fino ad arrivare a comportamenti autolesivi o al ritiro sociale. Il timore che la persecuzione *online* possa sfociare in violenza fisica, soprattutto nei casi in cui il molestatore abbia un legame pregresso con la vittima, alimenta uno stato di allarme permanente. A complicare il quadro vi è la riluttanza di molte vittime a denunciare, per paura di non essere credute, per vergogna o per timore di essere ritenute corresponsabili.

In risposta a tali dinamiche, il legislatore italiano ha introdotto, nel 2009¹⁹, l'art. 612-*bis* c.p., che punisce con la reclusione da uno a sei anni e sei mesi chiunque, con atti reiterati minacciosi o molesti, provochi nella vittima uno stato di grave ansia o timore, o la costringa a modificare radicalmente le proprie abitudini. Nel 2013, con la legge sul contrasto alla violenza di genere²⁰, è stata introdotta un'aggravante specifica nei casi in cui lo stalking sia realizzato tramite strumenti informatici o da parte di coniugi ed ex partner, riconoscendo la crescente pericolosità delle condotte digitali. La giurisprudenza italiana di legittimità ha inoltre stabilito che la competenza territoriale per questi reati si debba radicare nel luogo in cui la vittima subisce l'effetto più rilevante, come l'alterazione delle proprie abitudini di vita o l'insorgere dello stato di prostrazione psicologica.

Nel medesimo panorama giuridico e criminologico, il cyberbullismo rappresenta un'altra forma significativa di violenza relazionale mediata dalla tecnologia. Con questo termine si indica un insieme di comportamenti aggressivi, reiterati e intenzionali, esercitati da uno o più individui tramite strumenti digitali, ai danni di una vittima – generalmente minorenni – che non è in grado di difendersi efficacemente.

¹⁹ D.L. n. 11/2009 del 23 febbraio 2009, convertito in L. n. 38/2009 del 23 aprile 2009.

²⁰ L. n. 119/2013 del 15 ottobre 2013.

Rispetto al bullismo tradizionale, analogamente al cyberstalking, il cyberbullismo si caratterizza per la sua pervasività: le azioni persecutorie possono avvenire in qualsiasi momento e luogo, rendendo la dimensione domestica o personale della vittima vulnerabile quanto quella pubblica.

Le condotte più diffuse includono insulti e minacce sistematiche, diffusione di contenuti umilianti, furto di identità per screditare la vittima, diffusione di dati personali o sensibili, esclusione intenzionale da spazi digitali condivisi, campagne di discredito e pubblicazione di immagini o video lesivi della dignità altrui.

Tali comportamenti trovano terreno fertile in piattaforme sociali come Facebook, Instagram, TikTok, YouTube, WhatsApp e Telegram, dove l'effetto moltiplicatore del danno è amplificato dalla possibilità di raggiungere un pubblico vastissimo in tempi rapidissimi, anche e soprattutto grazie al contributo – più o meno consapevole – degli altri utenti, attraverso un *like* o una condivisione.

Dal punto di vista psicologico, i bulli cibernetici, non percependo spesso la gravità delle proprie azioni, evidenziano la tendenza a minimizzare il danno inflitto, mostrando una bassa empatia e una marcata deresponsabilizzazione, favorita dalla percezione dell'ambiente digitale come uno spazio privo di regole. Le vittime, invece, tendono a sentirsi impotenti, isolate e sopraffatte, manifestando reazioni emotive quali tristezza, vergogna, ansia e paura cronica, con ripercussioni anche gravi sul piano affettivo, relazionale e scolastico, fino a comportamenti autolesionistici o ideazioni suicide. Un ruolo determinante lo giocano gli spettatori passivi, il cui silenzio o la cui indifferenza rafforzano l'azione persecutoria; al contrario, la solidarietà manifestata da coetanei o adulti può contribuire a limitare gli effetti del danno.

Preso atto della crescente rilevanza del fenomeno, il legislatore italiano, seppur non introducendo una norma incriminatrice all'interno dell'ordinamento giuridico italiano, ha colmato un vuoto normativo nel 2017, fornendo la prima definizione legislativa e previsto alcuni strumenti di difesa²¹. L'art. 1 della legge, difatti, qualifica il cyberbullismo come «qualunque forma di pressione, aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione, furto d'identità, alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati personali in danno di minorenni, realizzata per via telematica, nonché la diffusione di contenuti on line aventi ad oggetto anche uno o più componenti della famiglia del minore il cui scopo intenzionale e predominante sia quello di isolare un minore o un gruppo di minori ponendo in atto un serio abuso, un attacco dannoso, o la loro messa in ridicolo». Tra le misure previste figurano la possibilità per il minore ultraquattordicenne (o i suoi genitori o legali rappresentanti) di richie-

²¹ L. n. 71/2017 del 17 maggio 2017.

dere la rimozione di contenuti offensivi, e l'intervento del Garante Privacy in caso di inadempienza da parte dei gestori. Inoltre, è stata estesa ai casi di cyberbullismo la procedura di ammonimento da parte del questore, già prevista per lo stalking, con l'obiettivo di prevenire la reiterazione delle condotte.

In stretto collegamento con le dinamiche del cyberstalking e del cyberbullismo si colloca il fenomeno della diffusione illecita di immagini o video sessualmente espliciti, comunemente noto, nella sua origine mediatica anglosassone, come *revenge porn*. Nel sistema giuridico statunitense, dove questa locuzione ha avuto origine, il termine – letteralmente traducibile in “pornografia di vendetta” – si riferiva alla diffusione non consensuale di immagini intime appartenenti a una persona, con l'obiettivo di danneggiarla, spesso come atto ritorsivo dopo la conclusione di una relazione sentimentale.

Storicamente, la facilità di produzione e condivisione di contenuti multimediali, soprattutto con l'avvento del digitale e di internet, ha reso questo tipo di abuso particolarmente insidioso. La rimozione dei contenuti dal web si presenta difatti estremamente difficile, se non impossibile, per via della loro replicabilità, della diffusione su server esteri e dell'insufficienza degli strumenti tecnici e giuridici attualmente disponibili.

Il materiale, acquisito con o senza il consenso della persona ritratta, viene poi diffuso sempre in assenza di autorizzazione, ledendo profondamente la riservatezza e l'autodeterminazione sessuale della vittima. La condivisione di immagini intime, anche se avvenuta consensualmente nel corso di una relazione, non implica alcuna autorizzazione alla loro divulgazione, sebbene persistano ancora radicate convinzioni culturali di colpevolizzazione della vittima, soprattutto se donna, rafforzando stereotipi sessisti e negando la piena titolarità della donna sul proprio corpo e sulla propria sessualità. Oltre al danno individuale – umiliazione, emarginazione, traumi psicologici – la diffusione illecita di contenuti sessuali agisce come una forma di discriminazione strutturale, incidendo sull'eguaglianza sociale e di genere.

Prima del c.d. Codice Rosso, che ha introdotto disposizioni a tutela delle vittime di violenza domestica e di genere²², la giurisprudenza tentava di incasellare questi episodi in fattispecie esistenti – atti persecutori, molestia, diffamazione aggravata, trattamento illecito di dati – ma nessuna di queste si rivelava pienamente adeguata alla gravità dei danni cagionati alle vittime o a cogliere la specificità delle condotte.

Solo con l'introduzione dell'art. 612-ter c.p., mediante il Codice Rosso, è stata definita in modo autonomo, nel nostro ordinamento, la fattispecie della dif-

²² L. n. 69/2019 del 19 luglio 2019.

fusione illecita di immagini o video sessualmente espliciti, con pene fino a sei anni di reclusione e sanzioni pecuniarie.

La norma punisce sia chi produce e diffonde il materiale, sia chi, diverso dall'autore della registrazione, lo riceve e lo condivide con l'intento specifico di arrecare danno. Sono previste aggravanti se l'azione è commessa con strumenti informatici, da persone legate affettivamente alla vittima o nei confronti di soggetti vulnerabili.

La Corte di Cassazione ha recentemente chiarito che si tratta di reato istantaneo, che si perfeziona con la prima trasmissione a terzi, e che la nozione di "contenuto sessualmente esplicito" comprende anche immagini che, pur non mostrando atti sessuali espliciti, evocano chiaramente la sfera sessuale o che sono state acquisite da un sito web di incontri ad accesso limitato²³.

Queste pronunce dimostrano come l'ordinamento giuridico stia progressivamente affinando gli strumenti interpretativi per fronteggiare una fenomenologia in costante evoluzione, che impone risposte non solo punitive, ma anche culturali e formative, capaci di incidere sulle rappresentazioni sociali della sessualità, del consenso e del rispetto della persona nel contesto digitale.

Nella medesima direzione si colloca la recente legge intitolata «Disposizioni e deleghe al Governo in materia di intelligenza artificiale»²⁴, che ha previsto, all'articolo 26, l'introduzione dell'art. 612-*quater* nel codice penale, configurando una nuova ipotesi di reato finalizzata al contrasto della diffusione illecita dei cosiddetti *deepfake*. Tale disposizione incriminatrice, rubricata «Illecita diffusione di contenuti generati o alterati con sistemi di intelligenza artificiale», prevede la pena della reclusione da uno a cinque anni per chiunque cagioni un danno ingiusto ad una persona, cedendo, pubblicando o altrimenti diffondendo, senza il suo consenso, immagini, video o voci falsificati o alterati mediante l'impiego di sistemi di intelligenza artificiale e idonei a indurre in inganno sulla loro genuinità.

L'intervento normativo del legislatore si configura come una risposta mirata e sistemica alle trasformazioni indotte dall'innovazione tecnologica nel settore dell'intelligenza artificiale, che ha reso possibile – con livelli di realismo sempre più elevati – la creazione, alterazione e diffusione di contenuti audiovisivi manipolati digitalmente. I *deepfake*, generati mediante sofisticati algoritmi di *machine learning* e *deep learning*, pongono nuove e complesse sfide sotto il profilo giuridico, incidendo in maniera significativa sui diritti fondamentali della persona, sulla

²³ Cass., sez. I, 28 marzo 2024, n. 33230; Cass., sez. V, 26 luglio 2023, n. 32602; Cass., sez. V, 5 marzo 2024, n. 25516; Cass., sez. V, 22 febbraio 2023, n. 14927. Si veda, altresì, nota a sentenza di G.M. Caletti, *La prima pronuncia di legittimità sull'art. 612-ter c.p.*, in *Sistema Penale*, 2023 (10), pp. 163-176.

²⁴ L. n. 132/2025 del 23 settembre 2025.

veridicità delle informazioni in circolazione e sull'affidabilità dell'ecosistema digitale.

In tale contesto, il legislatore ha inteso colmare una rilevante lacuna del sistema penale, che non contemplava esplicitamente condotte lesive riconducibili alla produzione e diffusione non consensuale di tali materiali. Si tratta di un fenomeno emergente, ma già ampiamente sfruttato per finalità pregiudizievoli, come nel caso di pratiche riconducibili al cyberbullismo, alla diffusione intenzionale di fake news, a vendette personali (ad esempio, in ambito affettivo o relazionale), nonché a manipolazioni della reputazione digitale di individui esposti.

L'impianto sanzionatorio subordina la punibilità della condotta non solo alla mancanza di consenso da parte del soggetto rappresentato nei contenuti, ma richiede altresì la configurazione di un danno ingiusto, quale elemento qualificante della fattispecie. In tal modo, analogamente a quanto previsto con le fattispecie precedentemente analizzate, la norma mira a garantire un equilibrio tra la tutela dei diritti della personalità e la libertà di espressione, tenendo conto delle peculiarità del contesto digitale e della potenziale lesività delle condotte automatizzate.

La disposizione si pone altresì in coerenza e continuità sistematica con le menzionate misure più stringenti introdotte dal Digital Services Act in capo agli intermediari digitali e alle piattaforme online, con particolare attenzione ai contenuti potenzialmente ingannevoli.

IL DATA BREACH E L'INCIDENTE DI SICUREZZA

Juri Monducci

SOMMARIO: 1. Introduzione: la crescente esposizione ai rischi digitali. – 2. Il concetto di data breach e la differenza rispetto all'incidente di sicurezza. – 3. Gli obblighi giuridici. – 3.1 Gli obblighi derivanti in caso di incidente di sicurezza. – 3.2 L'intersezione con il RGPD e l'obbligo di notifica all'autorità di controllo derivante dal data breach. 3.3. La comunicazione del data breach agli interessati – 4. L'importanza della prevenzione, gli obblighi di accountability e le attività successive all'incidente.

1. Introduzione: la crescente esposizione ai rischi digitali

Negli anni Ottanta del secolo scorso si iniziò a parlare del concetto di «società della sorveglianza», inizialmente fatto proprio solo da alcuni autori statunitensi¹.

La “sorveglianza” a cui facevano riferimento tali autori consisteva, in particolare, nella constatazione della capacità di raccolta, memorizzazione ed elaborazione dei più minuti dettagli della vita privata dei cittadini da parte di *database* elettronici².

Mentre, infatti, in precedenza, fino alla Seconda Guerra Mondiale, la sorveglianza era effettuata per mezzo di strumenti cartacei, dall'avvento delle nuove tecnologie digitali ha iniziato ad essere assolta da elaboratori elettronici, capaci di raccogliere dati di ogni specie, e quindi di ogni movimento quotidiano dell'essere umano: ritirare denaro dagli sportelli bancari automatici, utilizzare tessere magnetiche per il pagamento della merce acquistata (carta di credito, carte di debito, chip), fare una telefonata, presentare domande alla pubblica

¹ Il primo ad utilizzare questa terminologia fu G. MARX, *The Surveillance Society: the Threat of the 1984 – Style Techniques*, in *The Futurist*, 1985, https://web.mit.edu/gtmarx/www/futurist_surv_soc.pdf; tale concetto viene poi ripreso da D. FLAHERTY, *Protecting Privacy in Surveillance Societies*, Chapel Hill: University of North Carolina Press, 1989, e da L. DAVID, *The Electronic Eye. The Rise of Surveillance Society*, Minneapolis: University of Minnesota Press, 1994 (trad. it. 1997).

² Si rammenta che, mentre la banca dati (*databank*) consiste semplicemente in un sistema diretto alla semplice raccolta di dati (come può essere una rubrica telefonica), la base di dati (*database*) consiste in un sistema automatico unico con la funzione di integrare i dati contenuti in più *databanks* distinti che li organizza in modo da renderli collegabili tra loro (definizioni tratte da A. CAPELLI, *Introduzione alle banche dati giuridiche*, Bologna: Clueb, 1991).

amministrazione, ricevere in comodato libri o videocassette, muoversi e spostarsi nelle vie cittadine, etc.

Ci si rese quindi conto della particolare “prepotenza” della raccolta ma, soprattutto, dell’elaborazione di tali informazioni, comprendendo come la capacità degli “elaboratori elettronici” non era tanto quella di raccogliere, quanto di interagire con altri omologhi, confrontando così dati provenienti da diverse fonti tra di loro non omogenee.

Il punto nasceva dalla constatazione che non sempre i soggetti i cui dati venivano raccolti ne erano a conoscenza, così da non permettere loro di sapere quanto gli altri conoscevano sulla loro vita privata. E, quindi, nemmeno sapevano *chi* aveva informazioni che li riguardavano.

In linea generale, quindi, ancora oggi le informazioni collazionate sono capaci di svelare ogni segreto sulla vita della persona, e risultano particolarmente pericolose se si considera che i database o i sistemi informativi e informatici possono essere usati da persone diverse, in taluni casi anche in via incidentale o, addirittura da soggetti terzi non autorizzati.

In questo contesto di “iperconnessione”, di utilizzo massivo degli strumenti digitali, le tecnologie digitali pervadono ogni ambito della vita sociale, economica e amministrativa, così che la principale criticità, sia dal punto di vista giuridico, sia dal punto di vista tecnico, è l’esposizione ai rischi informatici.

L’incremento del numero e della sensibilità dei dati trattati e, comunque, l’uso quotidiano e, anzi, persistente, degli strumenti digitali, dell’intelligenza artificiale, dei servizi cloud, delle comunicazioni elettroniche e a distanza, spesso anche da parte di persone prive di competenze tecniche o con competenze tecniche insufficienti, stanno rendendo gli enti pubblici e privati particolarmente vulnerabili alle più moderne minacce digitali, dal puro attacco informatico, all’incidente digitale causato da errore, o ignoranza umana³.

In questo scenario, la sicurezza delle informazioni, quale corollario della protezione dei dati personali, assume un ruolo centrale, non solo per la salvaguardia dei diritti fondamentali degli interessati, ma anche per la tenuta del tessuto economico e istituzionale.

Le conseguenze di un incidente informatico possono tradursi in blocchi operativi, danni reputazionali, esposizione a responsabilità contrattuali e legali, oltre a possibili sanzioni da parte delle autorità di controllo⁴, ma soprattutto rischia di violare i diritti fondamentali dell’essere umano che, in taluni casi, po-

³ Enisa, *Threat Landscape 2023*, <https://www.enisa.europa.eu/sites/default/files/publications-/ENISA%20Threat%20Landscape%202023.pdf>.

⁴ GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Linee guida in materia di violazioni di dati personali*, 18 ottobre 2018.

trebbe essere portato, come occasionalmente effettivamente accaduto, a porre in essere gesti estremi.

È ormai sotto l'occhio di tutti come la violazione dei dati può pregiudicare gravemente la vita privata e la protezione dei dati delle persone che, a seguito della violazione, potrebbero subire furto o usurpazione d'identità, danni patrimoniali (es. perdite finanziarie) o non patrimoniali, da perdita della riservatezza a pregiudizio alla reputazione.

L'evoluzione tecnologica, dagli anni Ottanta, ha fatto passi da gigante, così come li ha dovuti fare il diritto, che si è reso conto che non poteva più continuare a disciplinare il settore informatico con la stessa tecnica legislativa che aveva utilizzato negli ultimi Secoli.

In parallelo all'evoluzione digitale, quindi, la normativa eurounitaria ha spinto ad adottare un approccio basato sulla responsabilizzazione (c.d. *accountability*), imponendo ai titolari e ai responsabili del trattamento una valutazione e una gestione del rischio legato alla sicurezza dei dati.

Il Regolamento (UE) 2016/679 (di seguito, RGPD) disciplina in modo puntuale le ipotesi di violazione dei dati personali (*data breach*) e gli obblighi giuridici che ne derivano, riconoscendo espressamente la centralità della sicurezza nel trattamento dei dati (cfr., in particolare, gli artt. 5, 24, 25, 32; 33; 34, del RGPD).

V'è però da aggiungere come, in realtà, l'espressione *data breach* non esaurisce tutte le possibili situazioni di rischio informatico. Vi sono numerose ipotesi (interruzioni di sistema, malfunzionamenti tecnici, attacchi informatici) che, pur mettendo a rischio il sistema informatico e/o il sistema informativo, non coinvolgono dati personali, e che quindi rientrano nell'ambito più ampio degli *incidenti di sicurezza*⁵.

Distinguere correttamente tra queste due categorie – incidente di sicurezza e violazione dei dati personali – è il presupposto essenziale per una corretta valutazione delle misure da adottare e degli obblighi da assolvere, sia in termini tecnici, sia in termini giuridici.

A ciò si aggiunga che il panorama normativo eurounitario è in continua evoluzione: strumenti come la Direttiva NIS⁶, il *Cyber Resilience Act*⁷ o il *Data Act*⁸

⁵ Enisa, *Good practices for incident management and incident response teams*, 2021; per una disamina della vulnerabilità informatica come «tratto distintivo dell'essere umano del ventesimo secolo» vedi anche G. MALGIERI, *Vulnerability and Data Protection Law*, Oxford: Oxford University Press, 2023.

⁶ La Direttiva (UE) 2022/2555 del 14 dicembre 2022 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del Regolamento (UE) n. 910/2014 e della Direttiva (UE) 2018/1972 e che abroga la Direttiva (UE) 2016/1148 (direttiva NIS 2).

⁷ Il Regolamento (UE) 2024/2847 del 23 ottobre 2024 relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali e che modifica i Regolamenti (UE) n. 168/2013 e (UE)

tendono a rafforzare l'obbligo di adozione di misure di sicurezza in ambito digitale, anche al di là del perimetro della protezione dei dati personali, delineando un quadro sempre più integrato tra cybersicurezza, responsabilità organizzativa e tutela delle informazioni.

L'obiettivo di questo contributo è quindi quello di offrire una ricostruzione sistematica del concetto di *data breach*, chiarirne la distinzione rispetto agli altri incidenti di sicurezza, analizzarne la disciplina giuridica applicabile e fornire un quadro operativo essenziale per affrontare correttamente gli obblighi e le attività successive a una eventuale violazione ma, soprattutto, per tentare di comprendere le modalità che il legislatore eurolunitario ha implementato per evitare che i *data breach* si verifichino, o per evitare che si verifichino di nuovo.

2. Il concetto di *data breach* e la differenza rispetto all'incidente di sicurezza.

La *violazione dei dati personali*, più comunemente chiamata con il nome inglese *data breach*, è espressamente definita dall'art. 4, par. 12, del RGPD come «la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati».

L'istituto del *data breach* e, comunque, la logica per la quale sono state introdotte nell'ordinamento specifiche disposizioni finalizzate a stabilire come devono comportarsi i titolari e i responsabili del trattamento laddove si verifichi un incidente di tale natura, parte dal presupposto che le singole autorità di controllo, gli interessati e, in taluni casi, addirittura i titolari stessi del trattamento, sono spesso inconsapevoli del fatto che si è verificato un incidente che ha messo a rischio i dati personali.

Lo scopo della norma, quindi, è quello di imporre l'intervento di colui che si "accorge" del *data breach*, affinché ne porti a conoscenza il titolare e l'autorità di controllo che, poi, potranno e dovranno esercitare quei doveri di controllo e di intervento finalizzati a ridurre al minimo il rischio che l'incidente possa avere delle conseguenze sui diritti fondamentali dell'essere umano, sia con riferimento allo specifico incidente, già verificatosi, sia per evitare che l'incidente si verifichi nuovamente.

La definizione che la normativa fornisce del *data breach* è poi ripresa, ed esplicitata, nelle «Linee guida sulla notifica delle violazioni dei dati personali ai

2019/1020 e la Direttiva (UE) 2020/1828 (Regolamento sulla ciberresilienza).

⁸ Il Regolamento (UE) 2023/2854 del 13 dicembre 2023 riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo e che modifica il Regolamento (UE) 2017/2394 e la Direttiva (UE) 2020/1828 (regolamento sui dati).

sensi del regolamento (UE) 2016/679» adottate, in prima battuta, il 3/10/2017 dall'allora Gruppo di Lavoro Articolo 29 per la Protezione dei Dati, che, in esito all'entrata in vigore del RGPD, è poi diventato il Comitato Europeo per la Protezione dei Dati (di seguito, EDPB), poi rielaborate, dopo i primi anni di esperienza sul campo, nelle «Linee guida 9/2022 sulla notifica delle violazioni dei dati personali ai sensi del regolamento generale sulla protezione dei dati (GDPR)» (di seguito, Linee Guida 9/2022), adottate il 28/03/2023 dall'EDPB.

La consapevolezza della necessità di gestire le violazioni di dati, del resto, non è solo della normativa eurounitaria in materia di protezione dei dati, ma deriva anche dalla «Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale», fatta a Strasburgo il 28 gennaio 1981, così come emendata dal Protocollo di emendamento fatto a Strasburgo il 10 ottobre 2018⁹, il cui articolo 7 prevede (ora) che «[c]iascuna Parte dispone che il titolare del trattamento notifichi, senza indugio, almeno all'autorità di controllo competente ai sensi dell'articolo 15 della presente Convenzione, le violazioni dei dati che possono seriamente interferire con i diritti e le libertà fondamentali delle persone interessate».

L'obbligo di gestione del *data breach*, peraltro, non è un istituto introdotto per la prima volta con il RGPD, perché già in precedenza taluni soggetti erano tenuti a gestire tale tipologia di incidenti. Si pensi, infatti, ai fornitori di servizi di comunicazione elettronica accessibili al pubblico, per i quali la Direttiva 2009/136/CE e il Reg (UE) n. 611/2013, già prevedevano l'obbligo di notifica e di comunicazione; ma si pensi anche, in Italia, agli organismi sanitari pubblici e privati che, con provvedimento del Garante del 4 giugno 2015, erano stati obbligati a notificare al Garante, e a comunicare agli interessati, ogni ipotesi di violazione dei dati che avesse colpito i dossier sanitari elettronici¹⁰.

Al di là della definizione normativa, il *data breach* è un particolare tipo di incidente di sicurezza che ha “colpito” i dati personali, e che impedisce al titolare del trattamento di essere in grado di garantire l'osservanza dei principi relativi al trattamento dei dati personali di cui all'art. 5 del RGPD.

Deve quindi evidenziarsi sin da ora la fondamentale distinzione tra incidente di sicurezza e violazione dei dati personali: mentre tutte le violazioni dei dati personali sono incidenti di sicurezza, non tutti gli incidenti di sicurezza sono necessariamente violazioni dei dati personali¹¹.

⁹ Il Protocollo è stato ratificato dall'Italia con legge 22 aprile 2021, n. 60.

¹⁰ Linee Guida in materia di Dossier sanitario del 4 giugno 2015 [doc. web 4084632], in particolare par. 7.

¹¹ Cfr. par. 15 delle Linee Guida 9/2022, che a sua volta evidenziano come l'incidente di sicurezza «non si limita ai modelli di minacce nei quali un attacco viene effettuato ai danni di un'organizzazione dall'esterno della stessa, bensì include anche incidenti derivanti dal trattamento interno che

Il *data breach*, quindi, come «evento», e come evento che può avere la sua genesi sia in un atto volontario, da parte di soggetti interni all'organizzazione, così come da parte di soggetti esterni alla stessa, sia in un atto non volontario, che sia generato dall'azione umana (ad es. da un dipendente che per mera distrazione invia una email contenente dati personali a un destinatario errato), così come dalla natura (ad es. un'alluvione o un incendio che causano la perdita o la distruzione dei documenti o dei sistemi informatici contenenti dati personali).

Ciò che, in realtà, bisogna tenere in considerazione per delineare il *data breach*, non è tanto la fonte dello stesso, o le ragioni che lo hanno determinato (banalmente anche solo perché le ragioni, in molti casi, soprattutto nel momento in cui il *data breach* viene ad evidenza, potrebbero essere sconosciute), quanto le «conseguenze» sui dati personali.

Il *data breach*, in sostanza, è tale laddove vi sia stato, appunto, un «evento», magari ancora nemmeno individuato, che ha causato, o può aver causato, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali.

La «distruzione» dei dati è, evidentemente, da individuarsi nell'ipotesi in cui gli stessi, a causa dell'evento, non esistono più¹² o non esistono più nella forma che sia utile al titolare o al responsabile del trattamento mentre, la «perdita» dei dati consiste nell'ipotesi in cui i dati, in astratto, esistono, ma il titolare potrebbe averne perso il controllo o l'accesso, oppure potrebbe non averli più in suo possesso¹³.

Le altre ipotesi che costituiscono un *data breach* sono individuate nella «modifica» dei dati, che consiste in una loro alterazione (e, quindi, «quando i dati personali sono stati modificati, corrotti o non sono più completi»)¹⁴ e nella «divulgazione non autorizzata o l'accesso ai dati personali», che configurano tutte quelle ipotesi in cui i dati personali sono venuti a conoscenza di soggetti che non avrebbero titolo a conoscerli (o perché trasmessi a tali soggetti, o perché taluno non autorizzato vi ha fatto accesso), così come tutte quelle ipotesi in cui

violano i principi di sicurezza».

¹² Si pensi, come già evidenziato, all'ipotesi di un incendio che causa la distruzione dei registri contenenti dati personali non inclusi anche in altri archivi, cartacei o elettronici, così come ad una alluvione che causa il danneggiamento irreversibile del server contenente i dati.

¹³ Nelle Linee Guida 9/2022 l'EDPB, anche alla luce dell'esperienza maturata dall'entrata in vigore del RGPD, si spinge ad evidenziare come «[u]n esempio di perdita di dati personali può essere la perdita o il furto di un dispositivo contenente una copia della banca dati dei clienti del titolare del trattamento. Un altro esempio può essere il caso in cui l'unica copia di un insieme di dati personali sia stata crittografata da un ransomware (malware del riscatto) oppure dal titolare del trattamento mediante una chiave non più in suo possesso».

¹⁴ Cfr. Linee Guida 9/2022, par. 14.

terzi non autorizzati, oltre ad accedere ai dati, hanno anche proceduto al loro trattamento.

Nella sostanza, il *data breach* può essere classificato sulla base di tre, distinti, principi, che sono stati fatti propri dall'EDBP ma che, di fatto, derivano dai principi basilari della scienza della sicurezza delle informazioni:

1. «violazione della riservatezza», che si configura in ipotesi di divulgazione accidentale a soggetti non autorizzati, sia interni sia esterni, così come in caso di accesso ai dati da parte di tali soggetti, e deve considerarsi particolarmente rilevante per il rischio di pregiudizio alla vita privata, all'onore e alla reputazione dell'interessato, con evidenza che il rischio deve considerarsi aumentare quanto più aumenta la sensibilità dei dati¹⁵.
2. «violazione dell'integrità», che si configura in caso di modifica non autorizzata o accidentale dei dati o corruzione degli stessi, ed è da considerarsi particolarmente rilevante quando l'alterazione può produrre effetti negativi sui diritti dell'interessato, ad esempio determinando decisioni automatizzate basate su dati errati¹⁶. Anche in questo caso, quanto più è sensibile il dato violato, tanto più grave può essere il rischio e/o la conseguenza¹⁷.
3. «violazione della disponibilità», che invece si configura in caso di perdita, accesso o distruzione accidentali o non autorizzati dei dati¹⁸ e può configurarsi anche solo nel caso in cui i dati diventino inaccessibili, vengano cancellati o persi, in modo accidentale o illecito¹⁹.

Ciascun *data breach* deve quindi essere necessariamente classificato in almeno una di queste tre macrocategorie, con evidenza che ciascuna ipotesi di violazione potrebbe essere classificato anche in più categorie (si pensi, a mero titolo esemplificativo, all'ipotesi del furto dei dati personali, che verrebbe classificato

¹⁵ A titolo esemplificativo rientrano nell'ipotesi della violazione di riservatezza gli incidenti che causano una intrusione informatica con esfiltrazione di dati (*data exfiltration*), l'inoltro di Email contenenti dati personali a destinatari errati, la pubblicazione accidentale di documenti su canali accessibili al pubblico, ecc.

¹⁶ A titolo esemplificativo, rientrano in tale ipotesi l'attacco informatico volto a manipolare i dati (es. alterazione di registri contabili), l'errore umano nella gestione di archivi o database, il malfunzionamento software che produce cambiamenti non intenzionali.

¹⁷ Si pensi, a mero titolo esemplificativo, all'ipotesi di un intervento chirurgico effettuato su un soggetto che non ne aveva necessità a causa dello "scambio" di referti istologici.

¹⁸ Sul punto giova osservare che la violazione della disponibilità è tale sia nell'ipotesi in cui la perdita sia solo temporanea (perché gli stessi possono essere integralmente recuperati *alimunde*, oppure tramite il sistema di back up) sia nell'ipotesi in cui, invece, sia permanente. Ciò che cambia, in questo caso, è la conseguenza, nel senso che, nell'ipotesi in cui la violazione sia solo temporanea, potrebbe non essere necessario procedere alla notifica all'autorità di controllo, laddove sia permanente è altamente probabile che detta notifica sia da eseguire. Ma, sul punto, vedi *infra*, sub 3.

¹⁹ A titolo esemplificativo, rientrano nella violazione della disponibilità le ipotesi di cancellazione accidentale di un archivio, l'attacco ransomware che blocca l'accesso ai dati o il guasto hardware.

sia nell'ipotesi della violazione della disponibilità – dato che il titolare potrebbe non avere più la possibilità di recuperarli – sia nella violazione della riservatezza – dato che gli stessi sarebbero venuti a conoscenza di coloro che li hanno sottratti).

Alla luce di quanto *supra* evidenziato, quindi, il *data breach* non si esaurisce nella mera compromissione dei dati, ma include qualsiasi evento suscettibile di produrre danni (fisici, materiali o immateriali) agli interessati, quali, appunto, la discriminazione, il furto di identità, la perdita finanziaria, il danneggiamento della reputazione, l'accesso non autorizzato o divulgazione di dati sensibili, etc.

Ciascun *data breach*, pertanto, al di là della sua rilevanza nell'ambito dell'organizzazione del titolare o, comunque, al di là delle conseguenze che comporta o che può comportare, costringe l'intervento del titolare del trattamento, imponendogli l'attivazione degli obblighi di notifica e di comunicazione, così come l'adozione di misure correttive e preventive.

Diverso, invece, è il caso del mero «incidente di sicurezza» che, come si è visto, non è detto che configuri anche una ipotesi di violazione dei dati personali.

L'incidente di sicurezza rappresenta un concetto molto più ampio del *data breach*, perché non è limitato ai casi in cui siano coinvolti dati personali. A mero titolo di esempio, un'interruzione temporanea del servizio dovuta a un guasto hardware può costituire un incidente di sicurezza rilevante per la continuità operativa, ma può non configurare *data breach* se non coinvolge dati personali mentre, al contrario, la cancellazione accidentale di dati personali anche temporanea rientra nell'ambito del *data breach*, dato il diretto nesso con i diritti degli interessati.

In proposito, per quanto l'EDPB evidenzia che la distinzione tra incidente di sicurezza e *data breach* è cruciale dal punto di vista operativo e giuridico, in quanto solo nel secondo caso scattano obblighi specifici di notifica (art. 33 del RGPD) e di comunicazione ai soggetti coinvolti (art. 34 RGPD), tale conclusione riguarda solo il contesto della normativa in materia di protezione dei dati personali perché, in realtà, a seguito dell'adeguamento dell'ordinamento nazionale alla Direttiva NIS2, operato con il d.lgs. 4 settembre 2024, n. 138, anche «un evento che compromette la disponibilità, l'autenticità, l'integrità o la riservatezza di dati conservati, trasmessi o elaborati o dei servizi offerti dai sistemi informativi e di rete o accessibili attraverso di essi» (art. 2, comma 1, lett. t) impone, ora, l'intervento dei soggetti pubblici e privati sottoposti, appunto, agli obblighi della normativa NIS2 (che, però, sono molti meno dei soggetti tenuti all'applicazione del RGPD, essendo solo quelli «di cui allegati I, II, III e IV»).

Come è evidente, l'incidente definito dalla normativa NIS2 non è solo quell'incidente che rischia di compromettere i dati (che, attenzione, potrebbero essere anche «dati non personali»), ma è anche quell'evento che compromette la disponibilità, l'autenticità e l'integrità dei «servizi offerti dai sistemi informativi o di rete» indipendentemente, appunto, dal fatto che tale incidente si estenda ai dati di natura personale.

3. Gli obblighi giuridici

La gestione di un incidente di sicurezza o di un *data breach* non si esaurisce nell'adozione di misure tecniche per contenerne gli effetti: essa comporta anche il rispetto di obblighi giuridici ben precisi, che variano a seconda della natura dell'evento.

Il RGPD, nelle disposizioni centrali degli artt. 33 e 34, prevede obblighi specifici in caso di violazione dei dati personali, mentre per gli incidenti di sicurezza (che coinvolgano, o meno, dati personali) si applicano altre normative di settore, come la Direttiva (UE) 2022/2555 (c.d. Direttiva NIS2), che, come si è visto, si applica solo a determinati soggetti pubblici e privati, ed è stata attuata, in Italia, dal d.lgs. 138/2024.

3.1. Gli obblighi derivanti dall'incidente di sicurezza

Come si è visto, la Direttiva (UE) 2022/2555 del 14 dicembre 2022, meglio nota come Direttiva NIS2, costituisce la principale risposta normativa dell'Unione Europea all'evoluzione crescente delle minacce cibernetiche e delle sfide legate alla resilienza delle infrastrutture digitali. Essa sostituisce la precedente Direttiva (UE) 2016/1148 (ora generalmente chiamata *Direttiva NIS1*), ampliandone l'ambito soggettivo e oggettivo di applicazione, e rafforzando gli obblighi in capo agli operatori economici e alle pubbliche amministrazioni.

La ragione giustificatrice della Direttiva NIS2, quindi, è da individuarsi nella necessità di assicurare un livello comune elevato di cybersecurity all'interno del mercato unico, prevenendo o, comunque, mitigando gli effetti negativi di incidenti che possano compromettere la fornitura di servizi essenziali e la fiducia degli utenti. Il tema degli obblighi derivanti a seguito del verificarsi di un incidente di sicurezza riveste un ruolo centrale, in quanto rappresenta il banco di prova della capacità normativa di coniugare prevenzione, reazione tempestiva e accountability degli operatori.

La disciplina sulle conseguenze di un incidente di sicurezza è stata attuata, in Italia, con le disposizioni contenute nel Capo IV del d.lgs. 138/2024, il cui arti-

colo 25 impone agli operatori designati come «essenziali» o «importanti»²⁰ di trasmettere, entro 24 ore dal momento in cui vengono a conoscenza di un incidente, un avviso preliminare (*early warning*) al «Computer Security Incident Response Team» (CSIRT)²¹. L'obiettivo è quello di fornire un'informazione tempestiva che consenta l'attivazione immediata di misure di contenimento e coordinamento, anche alla luce dell'impatto e/o alle conseguenze, in taluni casi anche di rilievo nazionale e/o eurounitario, che potrebbe avere l'incidente di sicurezza.

L'art. 25 prevede poi che, senza ingiustificato ritardo, e comunque entro le successive 72 ore (anche queste decorrenti dalla conoscenza dell'incidente, e non dalla pre-notifica), l'operatore deve fornire una «notifica dell'incidente», contenente un aggiornamento delle informazioni già fornite con la pre-notifica, e comunque fornendo una valutazione iniziale dell'incidente che comprenda notizie più dettagliate sulla sua gravità e sul suo impatto e, ove disponibili, gli indicatori di compromissione. Questa fase, come evidente, e come si vedrà *infra* nel par. 3.2., si ispira chiaramente all'obbligo di notifica previsto dal RGPD in caso di *data breach*, pur con le più ampie finalità connaturate all'incidente di sicurezza, quindi finalizzate alla più ampia protezione della sicurezza dei sistemi e dei servizi.

Successivamente, e fermo restando che l'operatore è tenuto a fornire, ma solo su richiesta del CSIRT, una relazione intermedia sui pertinenti aggiornamenti della situazione, entro un mese dall'invio della «notifica dell'incidente», l'operatore è tenuto all'invio allo stesso Gruppo di intervento di una «relazione finale» che contenga la descrizione dettagliata dell'incidente, ivi inclusi la sua gravità e il suo impatto, il tipo di minaccia o la causa originale (*root cause*) che ha probabilmente innescato l'incidente, le misure di attenuazione adottate e in corso nonché, ove noto, l'impatto transfrontaliero dell'incidente.

In considerazione del fatto che, spesso, gli incidenti di sicurezza, soprattutto i più rilevanti e i più impattanti, hanno un effetto che prosegue nel tempo, nel caso al momento dell'invio della prima «relazione finale» l'incidente sia ancora in corso, l'art. 25 impone la trasmissione di una «relazione mensile» sui progressi, e di una «relazione finale» entro un mese dalla conclusione della gestione dell'incidente.

²⁰ L'individuazione dei soggetti tenuti all'applicazione delle disposizioni di cui al d.lgs. 137/2024 sono indicati nell'art. 3, ma poi l'art. 6, ponendosi in relazione con gli Allegati I, II, III e IV al medesimo Decreto, definisce una particolare categoria di soggetti (definiti, appunto, «essenziali» o «importanti»), ai quali competono obblighi più stringenti.

²¹ Il CSIRT, ai sensi dell'art. 1, comma 2, del d.lgs. 138/2024, è il «Gruppo di intervento nazionale per la sicurezza informatica in caso di incidente in ambito nazionale» istituito presso l'Autorità per la Cybersicurezza Nazionale (ANC).

È evidente, dalla disamina degli obblighi derivanti dall'art. 25, che la scansione temporale consente di combinare le esigenze di tempestività connaturate alla *ratio* della notifica con l'approfondimento successivo necessario per un'analisi retrospettiva.

La normativa NIS2 non si limita, poi, agli aspetti comunicativi, ma impone agli operatori l'obbligo di adottare misure organizzative e tecniche di gestione dell'incidente.

L'art. 23 del d.lgs. 138/2024, infatti, prevede, tra gli altri, l'obbligo di implementare un quadro strutturato di *risk management*, che includa procedure di *incident response* e *business continuity*, piani di gestione delle crisi e comunicazione interna ed esterna, sistemi di monitoraggio e registrazione degli incidenti, cooperazione attiva con il CSIRT nazionale e con altri operatori di settore.

Tali obblighi, evidentemente, si saldano proprio con quella logica di resilienza operativa integrata, propria della normativa NIS2, che, oltre alla reazione, impone la capacità di apprendimento organizzativo attraverso l'analisi degli incidenti e la revisione delle misure di sicurezza adottate.

3.2. L'intersezione con il RGPD e l'obbligo di notifica all'autorità di controllo derivante dal data breach

Un profilo di particolare rilievo è, quindi, l'interazione tra Direttiva NIS2 e Reg (UE) 2016/679.

Nel caso in cui un incidente di sicurezza comporti anche una violazione di dati personali, l'operatore (che, come noto, nel contesto del RGPD si definisce *titolare* o *responsabile*), laddove tenuto, deve rispettare, oltre agli obblighi previsti dall'art. 25 *supra* descritti, anche gli altri obblighi derivanti dagli articoli 33 e 34 del RGPD.

Si potrebbe pertanto profilare un regime di doppia notifica, che richiede un attento coordinamento al fine di evitare duplicazione od omissioni, per cui la via maestra per garantire efficienza e conformità multilivello, come si vedrà *infra*, sub par. 4, potrebbe essere quella di adottare modelli integrati di gestione degli incidenti.

L'operatore soggetto all'applicazione del d.lgs. 138/2024 che tratta dati personali (e che è quindi soggetto anche all'applicazione del RGPD²²) sarà infatti tenuto sia agli obblighi di notifica previsti dalla normativa NIS2 sia all'obbligo di notifica (e comunicazione) previsto dal RGPD, mentre l'operatore soggetto

²² Anche in questo caso giova osservare come colui che è soggetto alla Direttiva NIS2 è necessariamente soggetto anche agli obblighi di cui al RGPD, mentre colui che è soggetto a tale ultima normativa, non è necessariamente tenuto all'applicazione della Direttiva NIS2.

alla (sola) applicazione del RGPD sarà tenuto ai soli obblighi di notifica (e comunicazione) previsti dalla normativa eurounitaria in materia di protezione dei dati.

Quando l'incidente integra un *data breach*, si applicano gli obblighi di cui agli artt. 33 e 34 RGPD.

L'art. 33 del RGPD, in particolare, prevede che «il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche».

Lo scopo dell'obbligo di notifica, già evidenziato *supra*, è espressamente delineato dal Considerando n. 87 del RGPD, laddove prevede che è «opportuno verificare se siano state messe in atto tutte le misure tecnologiche e organizzative adeguate di protezione per stabilire immediatamente se c'è stata violazione dei dati personali e informare tempestivamente l'autorità di controllo e l'interessato. [...] Siffatta notifica può dar luogo a un intervento dell'autorità di controllo nell'ambito dei suoi compiti e poteri previsti dal presente regolamento».

Lo scopo, quindi, è quello di consentire l'intervento dell'autorità di controllo (che, in Italia, è il Garante per la Protezione dei Dati Personali, di seguito *Garante*), sia con finalità repressiva, quindi allo scopo di verificare che il titolare, prima dell'incidente, avesse messo in atto tutte le misure di sicurezza adeguate, sia con finalità preventiva, e quindi per verificare che, a fronte di quanto accaduto, il titolare metta in atto le misure di sicurezza necessarie per evitare che quel *data breach* possa ripetersi.

Il titolare, quindi, ha l'obbligo di procedere alla notifica al Garante (o ad altra autorità di controllo competente a seconda del caso ai sensi dell'art. 55 del RGPD), senza ingiustificato ritardo o, comunque, entro 72 ore da quando è venuto a conoscenza dell'incidente.

Il primo punto che si pone all'attenzione dell'interprete è quello di stabilire il momento in cui il titolare è venuto a conoscenza del *data breach* e, in proposito, soccorrono le Linee Guida 9/2022, a mente delle quali il titolare deve considerarsi a conoscenza nel momento in cui «è ragionevolmente certo che si è verificato un incidente di sicurezza che ha portato alla compromissione dei dati personali». Non è sufficiente, quindi, che il titolare sappia che si è verificato un incidente di sicurezza (per cui, in realtà, laddove sia soggetto alla normativa NIS2, per lui potrebbe già essere iniziato a decorrere l'obbligo di notifica previsto da

tale normativa), ma è necessario che sappia, con ragionevole grado di certezza, che l'incidente abbia compromesso i dati personali²³.

Come noto, poi, il *data breach* potrebbe essersi verificato presso il responsabile del trattamento al quale, invece, non compete in via diretta l'obbligo di notifica all'Autorità e di comunicazione agli interessati. L'art. 33, par. 2, infatti, impone al responsabile il solo obbligo di informare della violazione il titolare, così che, per quest'ultimo, la vera conoscenza del *data breach*, dal quale decorrerà il termine per la notifica, sarà da individuarsi, appunto, nella ricezione della informativa del responsabile che dovrà avere un contenuto sufficiente per consentire al titolare di procedere, quantomeno, ad una prima notifica preliminare²⁴.

All'esito della conoscenza del *data breach*, il titolare è tenuto a procedere alla notifica, come si è visto, senza ingiustificato ritardo o, al più, entro 72 ore da tale conoscenza.

Il titolare, acquisita certezza del verificarsi del *data breach*, è quindi tenuto a compiere una istruttoria finalizzata sia a determinare le natura, le cause e l'impatto dell'incidente, ma soprattutto a valutare se sussiste l'obbligo di procedere alla notifica stessa.

L'art. 33, infatti, esclude tale obbligo nel caso in cui «sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche» ma la valutazione di tale *improbabilità* è una valutazione, in questa fase, di stretta competenza del titolare del trattamento, che dovrà basarsi sul principio di *responsabilizzazione* di cui all'art. 5 del RGPD²⁵.

Laddove il titolare concluda ritenendo l'insussistenza della *improbabilità* (e, quindi, ritenendo che sia *probabile* che il *data breach* presenti «un rischio per i diritti e le libertà delle persone fisiche»), allora sarà tenuto ad effettuare la notifica

²³ Sul punto le Linee Guida 2/2022, alla luce dell'esperienza maturata dal Comitato Europeo, esemplificano, evidenziando che in «caso di perdita di una chiave USB contenente dati personali non crittografati spesso non è possibile accertare se persone non autorizzate abbiano avuto accesso ai dati. Tuttavia, anche se il titolare del trattamento non è in grado di stabilire se si è verificata una violazione della riservatezza, tale caso deve essere notificato, in quanto sussiste una ragionevole certezza del fatto che si è verificata una violazione della disponibilità; il titolare del trattamento si considera venuto "a conoscenza" della violazione nel momento in cui si è accorto di aver perso la chiave USB».

²⁴ Poi, chiaramente, resta fermo che il responsabile, ai sensi dell'art. 28, par. 3, del RGPD, sarà tenuto ad assistere «il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento».

²⁵ Per tale valutazione, tuttavia, il titolare può avvalersi degli *esempi* fatti dall'EDPB che, nelle Linee Guida 2/2022, ha evidenziato come potrebbe non essere necessaria la notifica nel caso in cui i dati personali siano «già disponibili pubblicamente, la cui divulgazione non costituirebbe un rischio probabile per la persona fisica». Altri esempi potrebbero essere poi tratti dalle Linee-guida 01/2021 dello stesso Comitato, aventi ad oggetto «esempi riguardanti la notifica di una violazione dei dati personali».

all'autorità di controllo, avvalendosi della procedura prevista dall'autorità competente²⁶.

Nell'atto di notifica, in particolare, il titolare deve necessariamente inserire, almeno:

- a) la descrizione della natura della violazione compresi, ove possibile, le categorie e il numero approssimativo di interessati nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
- b) il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
- c) la descrizione delle probabili conseguenze della violazione dei dati personali;
- d) la descrizione delle misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Al legislatore eurounitario era ben chiaro che, nel brevissimo lasso temporale consentito per l'esecuzione della notifica, il titolare potrebbe non conoscere ancora tutti gli elementi richiesti dalla notifica (in particolare, ad esempio, il numero degli interessati, i dati coinvolti, la causa dell'incidente, l'impatto dello stesso, *etc.*).

Tale mancanza di conoscenza, tuttavia, non si traduce in una causa che consenta di non fare la notifica, o di farla in ritardo, perché l'art. 33, par. 4, consente proprio la c.d. notifica per fasi. Nei casi in cui il titolare non conosca tutti gli elementi da includere nella notifica, egli è tenuto ad effettuare una prima notifica, c.d. notifica preliminare, alla quale può poi far seguire la notifica *completa* non appena sarà a conoscenza degli elementi mancanti. Sul punto, peraltro, nella prassi, anche alla luce dei solleciti che, generalmente, l'Ufficio del Garante inoltra laddove abbia ricevuto una notifica preliminare, ed in considerazione del tempo spesso necessario per ottenere e/o raccogliere tutte le informazioni richieste dalla norma, il titolare compie una moltitudine di notifiche preliminari, alle quali potrebbe seguire una notifica definitiva anche a distanza di molto tempo dalla prima segnalazione²⁷.

²⁶ Il Garante italiano, in particolare, ha predisposto una procedura di notifica telematica, con la quale può procedersi, al momento, solo avvalendosi della firma digitale: <https://servizi.gpdp.it/databreach/s/>.

²⁷ Si pensi che, invece, nella normativa NIS2 l'ipotesi della moltitudine di *relazioni*, prima di quella finale, è espressamente prevista proprio dall'art. 25 del d.lgs. 138/2024.

L'art. 33, paragrafo 1, ultimo periodo, del RGPD, prevede, poi, l'ipotesi (per quanto vietata, da non escludere), in cui il titolare proceda a notifica tardiva (quindi oltre le 72 ore da quando è venuto a conoscenza del *data breach*).

In tale caso egli è tenuto ad esporre al Garante i «motivi del ritardo», in base ai quali, evidentemente, l'autorità valuterà la necessità o meno di adottare, nei confronti del titolare ritardatario, eventuali provvedimenti.

3.3. Segue: la comunicazione del data breach agli interessati

Il successivo art. 34 del RGPD prevede poi che «[q]uando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo».

Come è evidente dalla lettera della disposizione, la soglia che impone la *comunicazione* delle violazioni agli interessati è senz'altro più elevata rispetto a quella della *notifica* all'autorità di controllo; mentre, quindi, l'art. 33, in linea di principio, prevede l'obbligo di procedere a *notifica*, salvo l'eccezione ivi considerata (*improbabilità* del rischio), l'art. 34 prevede l'obbligo di procedere alla *comunicazione* nel solo caso, invece, in cui si ritenga sussistente un rischio *elevato*. Quindi: non tutti i *data breach* per i quali sussiste l'obbligo di *notifica* sono soggetti all'obbligo di *comunicazione*, ma senza dubbio ogni *data breach* per cui sussiste obbligo di *comunicazione*, è senz'altro soggetto a obbligo di *notifica*.

Ovviamente, sempre sulla scorta del principio di *accountability* che governa l'intera normativa in materia di protezione dei dati, l'onere di valutare la sussistenza del *rischio elevato* compete al titolare del trattamento che, nel caso, sarà tenuto a «comprovarlo» (art. 5, par. 2, RGPD).

Alla luce dei rischi che comporta ciascuna ipotesi di violazione dei dati personali, come noto capace di «provocare danni fisici, materiali o immateriali alle persone fisiche, ad esempio perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo» (vedi Considerando n. 85), la *comunicazione* è finalizzata a consentire all'interessato di «*prendere le precauzioni necessarie*» (Considerando n. 86, primo periodo) ragione per cui, laddove prevista, deve essere inviata «*senza ingiustificato ritardo*». A seconda della particolare natura della violazione, quindi, la *comunicazione* consentirà ai singoli interessati di prendere provvedimenti per proteggersi da eventuali conseguenze negative della violazione.

Nel caso in cui, quindi, sussista l'obbligo di procedere alla *comunicazione*, il titolare sarà tenuto a fornire all'interessato (almeno):

- a) una descrizione della natura della violazione;
- b) il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto del titolare;
- c) una descrizione delle probabili conseguenze della violazione;
- d) una descrizione delle misure adottate o di cui si propone l'adozione da parte del titolare per porre rimedio alla violazione e anche, se del caso, per attenuarne i possibili effetti negativi.

Evidentemente, quindi, lo scopo è veramente quello di consentire all'interessato di rendersi conto di cosa è concretamente accaduto e di valutare nel miglior modo possibile cosa può fare per ridurre il più possibile l'impatto che tale incidente può provocargli, eventualmente anche consultandosi con il titolare stesso. Le Linee Guida 9/2022, infatti, prevedono addirittura che «il titolare del trattamento dovrebbe anche fornire consulenza specifica alle persone fisiche sul modo in cui proteggersi dalle possibili conseguenze negative della violazione, ad esempio reimpostando le password in caso di compromissione delle credenziali di accesso».

In linea con le altre disposizioni del RGPD che prevedono lo svolgimento di attività informativa verso l'interessato (vedi, a titolo esemplificativo, l'art. 12 in materia di «[i]nformazioni, comunicazioni e modalità trasparenti per l'esercizio dei diritti dell'interessato»), l'art. 34, par. 2, prevede la necessità che la *comunicazione* contenga un linguaggio «*semplice e chiaro*» dato che la logica dell'istituto non è quella formale, bensì sostanziale, e quindi viene imposto l'utilizzo di un linguaggio poco tecnico, e maggiormente comprensibile all'interessato, se pur rispettoso dei requisiti minimi previsti dalla norma.

La *comunicazione*, tendenzialmente, deve essere resa direttamente agli interessati coinvolti, a meno che ciò richieda uno sforzo sproporzionato (anche questo da valutare secondo il principio di *responsabilizzazione* di cui all'art. 5, par. 2 del RGPD).

L'EDPB, nelle Linee Guida 9/2022, evidenzia che la *comunicazione* deve essere di tipo *dedicato*, quindi non può essere inviata unitamente ad altre informazioni, «quali aggiornamenti regolari, newsletter o messaggi standard». La logica, evidentemente, anche in questo caso, è quella di garantire la massima trasparenza della comunicazione ma, soprattutto, la maggiore diffusività della stessa²⁸,

²⁸ In materia l'EDPB si spinge all'esemplificazione, come di consueto: «[e]sempi di metodi trasparenti di comunicazione sono: la messaggistica diretta (ad esempio messaggi di posta elettronica, SMS, messaggio diretto), banner o notifiche su siti web di primo piano, comunicazioni postali e pubblicità di rilievo sulla stampa. Una semplice comunicazione all'interno di un comunicato stampa

ragione per cui il titolare sarà tenuto a valutare anche la *lingua* da utilizzare nella comunicazione perché, nel caso in cui con gli interessati, alla luce della particolare tipologia di attività svolta, il titolare abbia sempre interagito con una lingua diversa da quella del Paese in cui opera, potrebbe essere opportuno, anzi dovuto, che il titolare invii la comunicazione in tale lingua (o, quantomeno, *anche*, in tale lingua)²⁹.

In proposito, del resto, la modulistica italiana predisposta dal Garante per la notifica richiede che il titolare indichi se ha proceduto, o meno, alla *comunicazione* (o se intende procedervi), le ragioni per cui ha ritenuto non sia necessaria, e, soprattutto, il testo della *comunicazione* e le modalità con le quali vi ha proceduto.

La finalità è proprio quella di consentire al Garante di sindacare la decisione presa dal titolare secondo il principio di *accountability* e, quindi, di intervenire con i provvedimenti prescrittivi di cui all'art. 34, par. 4 e 58, par. 2, lett. e) del RGPD che, in materia, consentono al Garante di imporre al titolare di comunicare agli interessati (o anche a un interessato specifico) la violazione dei dati personali.

Resta poi fermo che il Garante, laddove ritenga, può adottare nei confronti del titolare qualsivoglia altro provvedimento per cui, a titolo esemplificativo, laddove ritenga che il testo della comunicazione non sia conforme alla normativa – perché, ad esempio, non chiaro – può imporgli di effettuare una nuova comunicazione, sia in virtù delle norme appena citate, sia in virtù dell'art. 58, par. 2, lett. d), a mente del quale il Garante può «*ingiungere al titolare del trattamento o al responsabile del trattamento di conformare i trattamenti alle disposizioni del presente regolamento, se del caso, in una determinata maniera ed entro un determinato termine*».

Come si è visto, la *comunicazione* è dovuta ogni qualvolta il titolare ritenga che il *data breach* presenti un rischio elevato per i diritti e le libertà dell'interessato. Si badi che, anche laddove il titolare ritenga sussistente tale rischio, sarà comunque esentato dall'obbligo di procedere all'adempimento in analisi in tre casi, espressamente previsti dall'art. 34, par. 3 del RGPD:

o di un blog aziendale non costituirebbe un mezzo efficace per comunicare una violazione all'interessato. L'EDPB raccomanda al titolare del trattamento di scegliere un mezzo che massimizzi la possibilità di comunicare correttamente le informazioni a tutte le persone interessate. A seconda delle circostanze, ciò potrebbe significare che il titolare del trattamento dovrebbe utilizzare diversi metodi di comunicazione, anziché un singolo canale di contatto».

²⁹ L'EDPB, infatti, evidenzia che «se la violazione riguarda interessati con i quali il titolare del trattamento non ha precedentemente interagito o, in particolare, interessati che risiedono in un altro Stato membro o in un altro paese al di fuori dell'UE diverso da quello nel quale è stabilito il titolare del trattamento, la comunicazione nella lingua nazionale locale potrebbe essere accettabile, tenendo conto della risorsa richiesta» dato che, rammenta, «[l']obiettivo principale è aiutare gli interessati a comprendere la natura della violazione e le misure che possono adottare per proteggersi» e non, quindi, limitarsi all'applicazione formale della normativa in analisi.

- a) quando ha applicato misure tecniche e organizzative adeguate per proteggere i dati personali prima della violazione, in particolare misure atte a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi³⁰;
- b) quando, immediatamente dopo una violazione, il titolare ha adottato misure destinate a garantire che non sia più probabile che si concretizzi l'elevato rischio posto ai diritti e alle libertà delle persone fisiche³¹;
- c) quando il contatto con gli interessati richiederebbe uno sforzo sproporzionato, ad esempio nel caso in cui i dati di contatto siano stati persi a causa della violazione o non siano mai stati noti.

In tale ultimo caso, la *comunicazione* sarà comunque necessaria ma il titolare può limitarsi a procedere a una comunicazione pubblica o a una misura simile che permetta di informare gli interessati con analoga efficacia (articolo 34, paragrafo 3, lettera c), RGPD³².

Il titolare dovrà quindi valutare (e, in caso negativo, lo si rammenta, l'imposizione potrebbe essere disposta dal Garante nell'esercizio dei poteri correttivi di cui all'art. 58, par. 2, del RGPD), l'adozione di disposizioni tecniche per rendere le informazioni sulla violazione disponibili su richiesta, magari fornendo le indicazioni necessarie (e semplici) per effettuare tale richiesta.

Ciò che conta, tuttavia, è un'altra considerazione: per quanto non vi sia obbligo di *comunicazione*, il titolare può sempre valutare di procedervi, anche solo per ragioni di attenzione commerciale, fermo restando che laddove detta *comunicazione* sia di natura volontaria, il titolare potrà valutare di procedervi nelle forme e con il contenuto che ritenga più utile.

3.4. Segue: la registrazione interna del data breach

In caso di violazione dei dati, l'art. 33 del RGPD ha poi introdotto anche un sistema articolato di documentazione delle violazioni verificatesi.

L'ultimo paragrafo di tale norma, infatti, prevede che il «titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rime-

³⁰ Ci si riferisce, quindi, al caso, anch'esso esemplificato dall'EDBP, in cui i dati erano stati protetti da cifratura allo stato dell'arte oppure mediante tokenizzazione.

³¹ In questo caso, a seconda delle circostanze del caso, ci si riferisce all'ipotesi in cui il titolare abbia immediatamente individuato e intrapreso un'azione contro il soggetto che ha avuto accesso ai dati personali prima che questi fosse in grado di utilizzarli in qualsiasi modo.

³² A mero titolo esemplificativo, mediante avviso da inserire nella *home page* del sito internet del titolare.

dio. Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo».

L'obbligo di *documentazione* al quale fa riferimento l'art. 33 prescinde dal fatto che si sia proceduto a *notifica* e/o a *comunicazione*, perché sorge per il solo fatto che si sia verificato un *data breach*.

Per quanto i *data breach* non siano necessariamente soggetti a *notifica* e *comunicazione*, quindi, sono comunque soggetti all'obbligo di *documentazione*, a prescindere dalla natura, dal rischio e dall'impatto che hanno provocato o che potrebbero aver provocato.

L'obbligo di *documentazione* è, in verità, spesso sottovalutato nella prassi organizzativa, ma, invece, rappresenta un cardine del principio di *responsabilizzazione*, dato che garantisce tracciabilità, trasparenza e capacità dimostrativa nei confronti delle autorità di controllo e, soprattutto, dato che consente al titolare (o al suo responsabile della protezione dei dati) di esercitare i poteri di vigilanza e controllo che, secondo le rispettive competenze, sono loro propri.

Dall'art. 33, par. 5, quindi, emerge un duplice livello di obblighi:

- documentazione interna sistematica di ogni violazione, anche quando non vi sia obbligo di *notifica* e/o *comunicazione*;
- finalità dimostrativa verso l'autorità, che deve poter verificare *ex post* la correttezza delle decisioni del titolare.

L'obbligo di *documentazione*, quindi, non coincide con un mero adempimento formale, ma si configura come strumento di *accountability*: il legislatore eurounitario ha voluto garantire che il titolare sia in grado di motivare e dimostrare le proprie scelte, specie nei casi in cui decida di non notificare la violazione dato che, in tale caso, è, se pur legittimamente, impedita la verifica diretta da parte dell'autorità di controllo di tutti i presupposti, le cause, le conseguenze e le decisioni assunte per effetto del *data breach* verificatosi.

La *documentazione* del *data breach*, quindi, non ha una funzione meramente difensiva, ma assume la forma di obbligo positivo e permanente di registrazione, volto a consolidare la capacità organizzativa e preventiva del titolare.

La norma in analisi individua tre elementi fondamentali che devono essere oggetto di registrazione:

- a) le circostanze della violazione: descrizione del contesto, data di rilevazione, sistemi coinvolti, natura dell'incidente (es. perdita di disponibilità, accesso non autorizzato, alterazione dei dati);
- b) le conseguenze: valutazione dell'impatto sui diritti e le libertà degli interessati, distinguendo tra violazioni di riservatezza, integrità e disponibilità;
- c) le misure adottate: azioni correttive immediate, interventi di mitigazione e misure preventive adottate successivamente.

La dottrina, le Linee Guida 9/2022 ma, soprattutto, la prassi applicativa hanno trasformato l'obbligo di *documentazione* in un obbligo di conservazione di un vero e proprio *registro*, strutturato nella modalità ritenuta opportuna dal titolare³³ nel quale inserire, oltre alle informazioni richieste dalla norma, anche informazioni aggiuntive, quali il processo decisionale relativo alla notifica, le valutazioni di rischio effettuate, le evidenze documentali a supporto e, soprattutto, anche a futura memoria, le motivazioni che hanno consentito al titolare di valutare se e perché procedere (o, meglio, a non procedere) alla *notifica* e/o alla *comunicazione*³⁴.

La tenuta del *registro dei data breach* svolge, quindi, una funzione probatoria (anche) a favore del titolare, dimostrando la diligenza nell'affrontare l'incidente, e rappresenta uno strumento di trasparenza organizzativa, utile per ricostruire nel tempo i casi occorsi, analizzarne le cause ricorrenti e individuare *pattern* di rischio che, poi, potranno essere utili allo stesso titolare per valutare, periodicamente, quali siano le attività di trattamento più a rischio e sulle quali abbia senso intervenire per mitigare il rischio e/o modificare le misure di sicurezza tecniche od organizzative già adottate.

Il *registro*, poi, è senz'altro un documento utile e necessario al responsabile della protezione dei dati per svolgere la sua attività di *sorveglianza* dato che, a fronte di uno o più incidenti verificatisi, egli può trarre informazioni a fronte delle quali suggerire al titolare l'adozione di particolari misure di sicurezza tecnica od organizzate.

Tale documentazione, peraltro, consente all'autorità di controllo di verificare la conformità senza dover necessariamente ricevere una notifica preventiva per ogni violazione minore, bilanciando così l'esigenza di vigilanza con l'efficienza del sistema.

³³ Nella prassi v'è chi conserva un *registro* cartaceo, chi ha elaborato un file di calcolo che contiene le informazioni rilevanti, chi ha elaborato o acquistato un apposito e complesso *software* in grado di registrare, catalogare ed elaborare le informazioni inserite.

³⁴ L'EDPB, in particolare, raccomanda al titolare di documentare anche il ragionamento alla base delle decisioni prese in caso di violazione: «[i]n particolare, se una violazione non viene notificata, è opportuno documentare una giustificazione di tale decisione. La giustificazione dovrebbe includere i motivi per cui il titolare del trattamento ritiene improbabile che la violazione possa presentare un rischio per i diritti e le libertà delle persone fisiche. In alternativa, se ritiene che una delle condizioni di cui all'articolo 34, paragrafo 3, GDPR sia soddisfatta, il titolare del trattamento dovrebbe essere in grado di fornire prove adeguate della circostanza che ricorre nel caso di specie».

4. L'importanza della prevenzione, gli obblighi di accountability, e le attività successive all'incidente

Alla luce di quanto evidenziato, è chiaro ed evidente come la prevenzione costituisca il primo presidio di tutela che governa l'intero RGPD, ivi compreso l'istituto del *data breach*, che non è stato introdotto per fini sanzionatori, bensì per consentire al titolare di verificare la tenuta della *governance* che ha predisposto per la gestione dei dati e, quindi, per apprestare le opportune modifiche alla stessa.

L'art. 25 RGPD, recepito e rafforzato dall'art. 25 del d.lgs. 138/2024 (per i soggetti tenuti alla NIS2), impone ai titolari di adottare misure tecniche e organizzative adeguate sin dalla fase di progettazione (*by design*) e per impostazione predefinita (*by default*).

Le Linee guida 4/2019 del Comitato Europeo sul principio di protezione dei dati fin dalla progettazione e per impostazione predefinita sottolineano che la prevenzione deve concretizzarsi in controlli di accesso, cifratura, segregazione dei dati, politiche di minimizzazione, ma anche in misure di carattere organizzativo, quali la formazione continua del personale e le simulazioni di *incident response*.

La mancata predisposizione di misure preventive, infatti, non solo espone l'organizzazione a rischi operativi, ma integra un inadempimento giuridico, così che la prevenzione costituisce un obbligo di diligenza qualificata (propria dei soggetti ai quali si applicano le normative in analisi) da valutarsi, appunto, in relazione allo stato dell'arte tecnologico e alla natura dei dati trattati.

Il principio di *accountability*, quindi, è un principio cardine sia della normativa in materia di protezione dei dati personali, essendo ivi codificato nell'art. 5, par. 2, sia della normativa NIS2, contenuto nell'art. 24 del d.lgs. 138/2024: il titolare non deve solo conformarsi alla norma, ma deve poter dimostrare l'adeguatezza delle misure adottate.

Il principio di *accountability* viene poi trasposto in ogni istituto del RGPD, ivi compreso quello del *data breach*, nell'ambito del quale, quindi, il titolare è tenuto ad adottare ogni misura di sicurezza tecnica od organizzativa necessaria per la sua gestione, e quindi, sia per acquisirne la conoscenza, sia per svolgere l'istruttoria, sia per valutare se sussiste l'obbligo di notifica e/o di comunicazione, sia per determinare come stabilire eventuali adempimenti e/o interventi successivi.

Le stesse Linee Guida 9/2022, del resto, evidenziano in più punti la necessità di "organizzare" la gestione dei *data breach*, ad esempio laddove:

- evidenziano che i «titolari e i responsabili del trattamento sono pertanto incoraggiati a pianificare anticipatamente e a mettere in atto processi per poter rilevare e limitare tempestivamente gli effetti di una violazione, va-

- lutare il rischio per le persone fisiche e stabilire se sia necessario notificare la violazione all'autorità di controllo competente e comunicarla alle persone fisiche interessate, ove necessario»³⁵;
- impongono al titolare del trattamento «di prendere le misure necessarie per assicurarsi di venire “a conoscenza” di eventuali violazioni in maniera tempestiva in modo da poter adottare le misure appropriate», fino a suggerirgli di «disporre di procedure interne per poter rilevare una violazione e porvi rimedio»³⁶;
 - prevedono che il «titolare del trattamento dovrebbe inoltre disporre di accordi con i responsabili del trattamento ai quali fa ricorso, i quali hanno a loro volta l'obbligo di notificare al titolare del trattamento eventuali violazioni»³⁷.

Nella sostanza, e nella prassi applicativa, è quindi evidente come il titolare, al fine di dimostrare il rispetto del principio di *accountability* anche al *data breach*, è tenuto ad adottare una *policy* interna, finalizzata a regolamentare come si dovrà comportare lui stesso e/o i suoi soggetti autorizzati, nel caso si verifichi un incidente di tale natura e, soprattutto, come dovrà comportarsi per mettere in campo quelle azioni di miglioramento che dovranno necessariamente conseguire al verificarsi di un *data breach*.

L'attività successiva all'incidente implica infatti l'attivazione di un *incident response plan*, con azioni immediate di contenimento e analisi tecnica, parte delle quali sono anche suggerite dalle Linee guida ENISA³⁸, nelle quali vengono forniti criteri per valutare gravità e impatto della violazione e alle quali, quindi, potrebbe fare rinvio la *policy* aziendale (dato che, comunque, i documenti ENISA non hanno valore cogente).

Al di là dell'adempimento degli obblighi di notifica, comunicazione e registrazione, l'incidente deve costituire un'occasione di apprendimento organizzativo. In tal senso, le autodeterminazioni del titolare – che può coinvolgere direttamente tutti gli operatori sotto la sua autorità (incluso il responsabile, ma solo qualora tali compiti siano stati espressamente previsti nell'accordo stipulato con lo stesso) – possono essere finalizzate a documentare le cause e le misure adottate, ad aggiornare le procedure interne e le policy di sicurezza, nonché a rivedere periodicamente i sistemi di protezione, anche sulla base di eventuali suggerimenti del responsabile della protezione dei dati, il quale, come noto, esercita

³⁵ Vedi punto 6 delle Linee Guida 9/2022.

³⁶ Vedi punto 37 delle Linee Guida 9/2022.

³⁷ Vedi punto 38 delle Linee Guida 9/2022.

³⁸ *Recommendations for a methodology of the assessment of severity of personal data breaches*, https://www.enisa.europa.eu/sites/default/files/publications/Data%20breach%20severity%20methodology_1.0.pdf.

funzioni di informazione e sorveglianza in relazione ai trattamenti di dati personali (cfr. art. 39 RGPD).

Il ciclo di gestione degli incidenti, quindi, non si esaurisce nell'evento, né negli obblighi dallo stesso derivanti, ma, soprattutto, si traduce in un processo continuo di revisione, miglioramento e implementazione dell'organizzazione nel suo complesso.

Per il *data breach*, infatti, le Linee Guida 9/2022 raccomandano un'analisi sistematica delle cause tecniche e organizzative, volta a valutare l'adeguatezza delle misure di sicurezza preesistenti (art. 32, RGPD) e ad aggiornare la valutazione del rischio per i diritti e le libertà degli interessati.

Per l'incidente di sicurezza puro, il soggetto essenziale o importante deve condurre un'analisi approfondita dell'evento, evidenziando le vulnerabilità sfruttate e predisponendo una relazione finale che contenga cause, impatto e misure adottate.

In entrambi i casi, la fase successiva, che potrebbe essere svolta cumulativamente (ma, ciò, dipende anche dalla procedura che il titolare si è imposto) richiede interventi concreti per limitare danni attuali e futuri, dalla rimozione delle vulnerabilità al potenziamento delle misure di sicurezza (cifatura, segmentazione di rete, autenticazione forte), dall'aggiornamento delle procedure interne di gestione degli incidenti e di *business continuity* alla formazione mirata del personale sui punti di debolezza emersi, dalla sostituzione o sospensione di fornitori che non rispettino le clausole contrattuali di sicurezza alla modifica degli accordi contrattuali in essere con tali fornitori.

Le norme previste per la gestione degli incidenti (siano essi un *incidente di sicurezza* puro, così come una *violazione di dati personali*), introducono un approccio sistemico alla gestione della sicurezza, fondato sui pilastri della prevenzione, dell'*accountability* e della risposta agli incidenti, in quanto, come si è visto, l'approccio integrato, che unisca tecniche di prevenzione avanzata, *accountability* sostanziale e capacità di reazione, può garantire la resilienza delle organizzazioni.

La normativa eurounitaria in materia, come si è già avuto modo di accennare, non è quindi una normativa che mira unicamente a punire le violazioni, ma tende a favorire lo sviluppo di una cultura proattiva della sicurezza, finalizzata a trasformare la crisi in occasione di miglioramento e adeguamento.

PARTE VI – ETICA DEL DIGITALE

ETICA DELL'INTELLIGENZA ARTIFICIALE

Giorgio Bongiovanni, Claudio Novelli

SOMMARIO: 1. Dagli androidi alle chatbot: intelligenza e agency. 2. Questioni di etica dell'IA e diritti umani. 3. Etica del digitale e dell'IA. 4. Dall'Etica alla Regolamentazione dell'IA. 5. Visioni critiche

1. Dagli androidi alle chatbot: intelligenza e agency

La riflessione sulle questioni etiche poste dall'Intelligenza Artificiale (IA d'ora in avanti) è quasi contemporanea alla nascita di questo ambito di ricerca. Va segnalata, tuttavia, una differenza significativa tra le analisi del primo periodo e quelle più recenti. Nel primo caso, si tratta di riflessioni che fanno riferimento a quella che è stata chiamata la *Good Old-Fashioned AI* (GOFAI) o *Intelligenza simbolica*, mentre le seconde hanno quale oggetto i sistemi basati sul *Machine Learning* (ML) e l'utilizzo dei *Large Language Models* (LLMs). Il primo tipo di IA adotta «una visione top-down dell'intelligenza» basata sulla «capacità degli esseri umani di comprendere il mondo attraverso rappresentazioni simboliche[concettuali]», il secondo utilizza, invece, «un approccio statistico [...] per trovare modelli in un mondo disordinato»¹. L'etica legata al primo tipo di IA (old-fashioned, simbolica, cognitiva) è quella probabilmente più nota perché è stata al centro di romanzi di science fiction e di film famosi: basti pensare ai romanzi di Philip K. Dick e Isaac Asimov e ai film di Stanley Kubrick (*2001: Odissea nello spazio* del 1968, basato su un racconto di Arthur C. Clarke) e Ridley Scott (*Blade Runner* del 1982)². Tutte queste opere sono centrate su automi/androidi o macchine che, fornite di una intelligenza vicina a quella umana (cioè dotata di «comprensione,

¹ N. GOLTZ, T. DOWDESWELL (eds.), *Real World AI Ethics for Data Scientists. Practical Case Studies*, Boca Raton: CRC Press, 2023, pp. 2-3, che notano che l'approccio statistico è nato come «una risposta ai primi fallimenti dell'IA simbolica»; L. FLORIDI, *Etica dell'intelligenza artificiale*, Milano: R. Cortina, 2023, ha sintetizzato la distinzione tra i due approcci di IA come differenza tra IA *cognitiva* e IA *ingegneristica*. Per una chiara ricostruzione del passaggio dal primo al secondo approccio, N. CRISTOFOLINI, *La scorciatoia*, Bologna: Il Mulino, 2023.

² Si può ricordare di P.K. DICK, *Do Androids Dream of Electric Sheep?* (Il cacciatore di androidi) del 1968, da cui è tratto *Blade Runner*, e di I. ASIMOV, *I, Robot* (I Robot) del 1950, che è una raccolta di racconti nei quali vengono sviluppate le tre leggi della robotica.

consapevolezza, acume, sensibilità, preoccupazioni, sensazioni, intuizioni, semantica, esperienza [...] significato, [...] saggezza», si ribellano agli esseri umani o cercano di imporre, anche al costo di vite umane, un dato piano. Questo tipo di IA non ha, tuttavia, alcun riscontro nello stato dell'arte tecnologico attuale, né sembra prevedibile un tale sviluppo nelle tendenze di breve-medio periodo³.

L'attuale ricerca etica è invece centrata sul secondo tipo di IA (ingegneristica) che è un'intelligenza che cerca principalmente di replicare la capacità di «risoluzione efficace dei problemi» e dell'«esecuzione corretta dei compiti» e lo fa estraendo schemi «non ovvi e utili da grandi insiemi di dati» sulla base di una capacità di tipo statistico e sintattico che non necessita di una competenza semantica, cioè della comprensione del significato delle cose⁴.

Questo passaggio ha portato a chiedersi se per il secondo tipo di IA sia effettivamente possibile parlare di intelligenza: ci sono posizioni che lo negano e altre che, anche se in forma moderata e che la distingue da quella umana, lo affermano. Da un lato, si è sostenuto che l'IA sia solo «una nuova forma dell'agire, che può affrontare con successo compiti e problemi, in vista di un obiettivo, senza alcun bisogno di essere intelligente», mentre, dall'altro, che si tratta comunque di «una forma di intelligenza, anche se non ne ha tutte le qualità», e che se una macchina «risolve un problema per cui non abbiamo alcuna teoria [...] è appropriato parlare di comportamento autonomo e “diretto a uno scopo”, e anche di apprendimento e intelligenza»⁵.

In ogni caso, la ricerca etica cerca di individuare i problemi che potrebbero nascere dall'IA, e le possibili soluzioni, in considerazione sia della struttura sia delle possibilità che tale intelligenza offre («capacità di percepire e classificare, formulare previsioni e proporre soluzioni, prendere decisioni e funzionare di conseguenza, eventualmente godendo di una piena autonomia operativa per alcuni compiti»)⁶. L'etica dell'IA è infatti un'*etica applicata*, cioè quella parte dell'etica che affronta pratiche e comportamenti specifici nel mondo reale⁷.

³ Si possono consultare dati sullo stato dell'arte tecnologico e sugli investimenti in IA su: <https://ourworldindata.org/artificial-intelligence>.

⁴ N. GOLTZ, T. DOWDESWELL (eds.), *Real World AI Ethics for Data Scientists. Practical Case Studies*, cit., pp. 2-3; L. FLORIDI, *Etica dell'intelligenza artificiale*, cit., sottolinea il «successo sbalorditivo» della seconda e la «triste delusione» generata dalle ricerche della prima fase.

⁵ L. FLORIDI, *Etica dell'intelligenza artificiale*, cit., sostiene inoltre che le nuove macchine sono «stupide come un vecchio frigorifero»; D. ANDLER, *Il duplice enigma. Intelligenza artificiale e intelligenza umana*, Torino: Einaudi, 2024; D. CRISTOFOLINI, *La scorciatoia*, cit. Una discussione importante su questa questione è quella che, negli anni '80, si è originata a partire dall'esperimento mentale della stanza cinese di J. Searle.

⁶ F. FOSSA, V. SCHIAFFONATI, G. TAMBURRINI (a cura di), *Automi e persone. Introduzione all'etica dell'intelligenza artificiale e della robotica*, Roma: Carocci, 2021.

⁷ L'etica applicata più nota è la bioetica, ma vi sono molti altri ambiti quali, ad. es., le etiche delle professioni.

In questo contributo, analizzeremo nel secondo paragrafo le questioni etiche (o l'intensificazione di quelle già presenti) poste dall'IA, anche alla luce del rapporto con i diritti umani. Nel terzo paragrafo, vedremo in che modo la riflessione etica (quale, ad. es. l'approccio chiamato *principlism*) li può affrontare. Nel quarto paragrafo, mostreremo come la riflessione etica ha ispirato la regolamentazione sulla IA, con particolare attenzione al contesto Europeo. Il paragrafo 5 conclude l'articolo illustrando alcune posizioni critiche nei confronti dell'etica dell'IA.

2. Questioni di etica dell'IA e diritti umani

In una rassegna del 2020 del *The Berkman Klein Center for Internet & Society* di Harvard⁸ vengono esaminati 36 documenti (sia di organizzazioni private sia di enti pubblici o internazionali) e individuati i temi e gli ambiti in cui è necessario che l'IA trovi dei principi regolatori. Allo stesso modo, ma dalla prospettiva dei diritti umani riconosciuti a livello internazionale, si muove il documento dell'ONU sui rischi che l'IA potrebbe comportare⁹. Nel primo caso, gli aspetti messi in evidenza sono: privacy, responsabilità (*Accountability*), sicurezza (*Safety and Security*) trasparenza ed esplicabilità (*Explainability*), equità e non-discriminazione, controllo umano della tecnologia; nel secondo caso, il riferimento è a: libertà da danni fisici e psicologici, uguaglianza di fronte alla legge e protezione contro le discriminazioni, diritto alla privacy, garanzia della proprietà, libertà di pensiero, religione, coscienza e opinione, libertà di espressione e di accesso alle informazioni, diritto di partecipazione alla vita politica, diritto al lavoro e a una vita dignitosa, diritti del bambino, diritti alla cultura, all'arte e alla scienza.

Questi aspetti sono tra quelli più importanti, ma non si può dire che racchiudano tutte le criticità legate all'IA: ciò dipende, tra l'altro, dal fatto che è «la tecnologia [che] spinge (*drives*) l'etica e [che] molte questioni che ora fanno parte dell'«etica digitale» sono antecedenti alla tecnologia digitale»¹⁰. Una complessiva

⁸ J. FJELD ET AL., *Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-based Approaches to Principles for AI*, Berkman Klein Center for Internet & Society, 2020, <http://nrs.harvard.edu/urn3:HULInstRepos:42160420>

⁹ UNHUMANRIGHTS, 2023, *Taxonomy of Human Rights Risks Connected to Generative AI*, <https://www.ohchr.org/sites/default/files/documents/issues/business/btech/taxonomyGenAI-Human-Rights-Harms.pdf>

¹⁰ V.C. MÜLLER, *The History of Digital Ethics*, in C. VÉLIZ (ed.), *The Oxford Handbook of Digital Ethics*, Oxford: Oxford University Press, 2023. Ciò naturalmente non significa dire che «l'innovazione digitale è alla guida, e tutto il resto rimane indietro», ma semplicemente che lo sviluppo della tecnologia può porre nuovi problemi. Sui rischi di una visione acritica della tecnologia e del suo ruolo, L. FLORIDI, *Etica dell'intelligenza artificiale*, cit.

classificazione degli aspetti critici dell'AI è comunque molto difficile¹¹: è tuttavia possibile individuare, tenendo conto della distinzione tra i sistemi di IA come *oggetti*, cioè strumenti realizzati e utilizzati dall'uomo e sistemi di IA come *soggetti*, cioè gli stessi sistemi di IA, nove punti principali («main ethical issues») ¹². Si tratta di: a) Privacy e profilazione, b) Manipolazione del comportamento, c) Opacità e Spiegabilità, d) Pregiudizi nei sistemi decisionali, e) Interazione uomo-robot, f) Automazione e occupazione, g) Machine Ethics, h) Sistemi autonomi e Responsabilità, i) Singularità. A questi punti, va poi aggiunto quello che riguarda l'analisi del (l) Peso ambientale dell'IA. Li analizzeremo sinteticamente.

a) *Privacy e profilazione*. In questo ambito, l'IA aggiunge alcuni aspetti critici a un rischio già presente e regolato. Si tratta in particolare, in relazione alla dimensione negativa del diritto, della possibilità che l'IA offre di una più ampia raccolta e analisi dei nostri dati digitali (ottenuti via internet, social media, banche dati): ciò può avvenire, ad esempio, con l'opportunità, permessa dall'IA, di un migliore riconoscimento facciale (da telecamere di sorveglianza e fotografie) e dunque dell'acquisizione di dati non solo digitali, ma biometrici. Inoltre, l'abilità di analisi dei dati da parte dei sistemi di IA facilita e ottimizza la profilazione degli aspetti, interessi, preferenze di vita (politiche, culturali, alimentari, ecc.) dei diversi soggetti e, in questo modo, aumenta (o forse crea) la capacità di renderli un prodotto commerciale: ciò può rafforzare l'idea che quello che sembra essere «l'obiettivo principale dei social media, dei giochi e della maggior parte di Internet», sia «ottenere, mantenere e dirigere l'attenzione – e quindi la fornitura di dati». Questo, a sua volta, ha consentito di dire che «la sorveglianza è il modello di business di Internet»¹³.

b) *Manipolazione del comportamento*. Anche la possibile manipolazione non è un fenomeno nuovo, è anzi antica, ma può acquisire nuove modalità attraverso i sistemi di intelligenza artificiale¹⁴. La manipolazione minaccia l'autonomia dei soggetti attraverso il controllo del «contenuto e la fornitura di informazioni in

¹¹ Sulle diverse classificazioni proposte, si veda S. BUIJSMAN, M. KLENK, J. VAN DEN HOVEN, *Toward a "Design for Values" Approach*, in N.A. SMUHA (ed.), *The Cambridge Handbook of the Law, Ethics and Policy of Artificial Intelligence*, Cambridge: Cambridge University Press, 2025, p. 63.

¹² Questa proposta è formulata da V.C. MÜLLER, *Ethics of Artificial Intelligence and Robotics*, in E.N. ZALTA e U. NODELMAN (eds.), *The Stanford Encyclopedia of Philosophy*, 2023, <https://plato.stanford.edu/archives/fall2023/entries/ethics-ai/>, che sostiene che su questi aspetti «there seems to be reasonable agreement».

¹³ *Ibid.*, che cita B. SCHNEIER, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*, New York: W.W. Norton, 2015, e nota che «questa economia della sorveglianza e dell'attenzione viene talvolta definita "capitalismo della sorveglianza"». Il riferimento è S. ZUBOFF, *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*, Roma: LUISS, 2023, e alla tesi che questo tipo di capitalismo si basa sulla previsione dei comportamenti.

¹⁴ V.C. MÜLLER, *Ethics of Artificial Intelligence and Robotics*, cit.

modo tale che la persona non sia consapevole della manipolazione»¹⁵. In questo contesto, l'IA può potenziare la manipolazione, ad esempio, migliorando l'accuratezza delle tecniche di *nudge* o quelle di inganno. Il *nudge* (spinta gentile) interviene sull'«architettura della scelta» delle persone allo scopo di modificare il loro comportamento senza che vi siano proibizioni o incentivi¹⁶ (ad esempio, mettendo in primo piano, in un supermercato, i prodotti che si vuole favorire). Il *nudge* sfrutta i nostri *bias* cognitivi¹⁷ e può essere considerato una forma di paternalismo (leggero) volto a indurre scelte positive per la vita pubblica. Può tuttavia essere considerato manipolatorio in quanto «in conflitto con due componenti critiche dell'autonomia personale: il consenso informato e il libero arbitrio».

In ambito digitale, il *nudge*, grazie alla possibilità di creare spinte più precise e personalizzate, opera con strumenti volti a incentivare la presenza online quali il «caricamento automatico di nuovi contenuti», la «riproduzione automatica di contenuti musicali o video», i «premi collegati all'interazione con la piattaforma»¹⁸. Il secondo aspetto (inganno), connesso tra l'altro alla propaganda politica, è legato alle «faking technologies» dell'IA che possono creare, «con qualsiasi contenuto», falsi testi, foto, video e trasformare «ciò che una volta era una prova affidabile in una prova inaffidabile»¹⁹.

c) *Opacità e Spiegabilità*. L'IA basata sul machine learning è in grado di prendere decisioni (ad esempio, sull'assegnazione di un credito, sulla scelta di un candidato per una posizione lavorativa) e di fare analisi previsionali (ad esempio, sulla libertà vigilata o la probabilità di contrarre una determinata malattia). La precisione e la rapidità con cui alcune di queste funzioni vengono svolte rende necessario garantire un livello sufficiente di trasparenza per spiegarne le ragioni (e inferenze) retrostanti.

Tuttavia, come abbiamo accennato, decisioni e previsioni avvengono estraendo «schemi (*pattern*) da un determinato set di dati» e selezionando quelli che «vengono etichettati in un modo che appare utile per la decisione»: ciò non solo limita «le opportunità di partecipazione umana», ma spesso rende impossibile «sapere come il sistema è giunto a questo output» sia per «per la persona in-

¹⁵ J. WILLIAMS, *Ethical Dimensions of Persuasive Technology*, in C. VÉLIZ (ed.), *The Oxford Handbook of Digital Ethics*, cit.

¹⁶ Si veda R. THALER, C.R. SUNSTEIN, *Nudge. La spinta gentile*, Milano: Feltrinelli, 2009.

¹⁷ Su questi *bias* e la loro derivazione dai nostri meccanismi cognitivi (sistema 1 e sistema 2), si veda M. GALLETTI, *Quando l'Intelligenza Artificiale incontra le scienze comportamentali. Una riflessione sui valori morali*, in M. GALLETTI, S. ZIPOLI CAIANI (a cura di), *Filosofia dell'Intelligenza Artificiale. Sfide etiche e teoriche*, Bologna: Il Mulino, 2024.

¹⁸ M. IENCA, E. VAYENAIN, *Digital Nudging. Exploring the Ethical Boundaries*, in C. VÉLIZ (ed.), *The Oxford Handbook of Digital Ethics*, cit.

¹⁹ V.C. MÜLLER, *Ethics of Artificial Intelligence and Robotics*, cit.

teressata» sia «per l'esperto»²⁰. I sistemi che presentano bassi livelli di trasparenza, e quindi di possibilità di fornire spiegazioni, sono spesso «chiamati *black box* (scatole nere) perché operano in un modo così complesso da rendere impossibile la piena comprensione di come vengono elaborate le informazioni»²¹: sono perciò «opachi» in quanto non si è in grado di sapere «come è stato identificato un particolare schema o persino qual è lo schema». Modelli che apprendono attraverso tecniche di deep learning ricadono in questo gruppo. Ciò ha condotto a prospettare una «minaccia dell'algocrazia»²².

d) *Pregiudizi (bias) nei sistemi decisionali*. Questo fenomeno riguarda «i modi in cui gli algoritmi possono riprodurre o addirittura amplificare i pregiudizi del passato lavorando su dati storici che riflettono pregiudizi precedenti»²³. Ciò è avvenuto diverse volte al punto che «per alcuni anni, gli algoritmi “razzisti” e “sessisti” hanno fatto notizia». Il caso più noto è probabilmente quello dell'algoritmo COMPAS (*Correctional Offender Management Profiling for Alternative Sanctions*) del sistema giudiziario americano deputato a prevedere la recidiva di chi aveva commesso crimini: questo sistema «aveva tassi di errore differenziali per i neri e i bianchi»²⁴ che favorivano i secondi e discriminavano i primi. Si ha perciò un pregiudizio quando la decisione è «influenzata da una caratteristica che è in realtà irrilevante per la questione»²⁵. Anche se i casi più frequenti riguardano appartenenza e genere, ce ne sono molti altri, quali, ad esempio, «insegnanti licenziati a causa di oscuri sistemi di valutazione algoritmica, famiglie che non hanno ricevuto l'assistenza (insurance) perché vivevano nel quartiere sbagliato e bambini a rischio che non sono stati allontanati da ambienti sociali pericolosi a causa di problemi nei sistemi di previsione del rischio»²⁶. La distorsione di questi sistemi può essere determinata dalla qualità dei dati utilizzati per

²⁰ *Ibid.*

²¹ M. DI MICHELE, *Intelligenza Artificiale. Etica, rischi e opportunità di una tecnologia rivoluzionaria*, Santarcangelo di Romagna: Diarkos, 2023.

²² V.C. MÜLLER, *Ethics of Artificial Intelligence and Robotics*, cit., che fa riferimento a J. DANAHER, *The Threat of Algocracy: Reality, Resistance and Accommodation*, in *Philosophy & Technology*, 2016 (29/3).

²³ P. BODDINGTON, *AI Ethics. A Textbook*, Berlin, Singapore: Springer, 2023, p. 50.

²⁴ L. HERZOG, *Algorithmic Bias and Access to Opportunities*, in C. Véliz (ed.), *The Oxford Handbook of Digital Ethics*, cit., che indica anche casi di discriminazione verso le donne di algoritmi di Google, Amazon, Apple.

²⁵ V.C. MÜLLER, *Ethics of Artificial Intelligence and Robotics*, cit.

²⁶ L. HERZOG, *Algorithmic Bias and Access to Opportunities*, cit., che sottolinea che «l'uso di tali algoritmi sta diventando sempre più diffuso» e che essi «svolgono già un ruolo in molte decisioni potenzialmente in grado di cambiare la vita, come il credito, l'alloggio, l'ammissione al college o la libertà vigilata». Un caso emblematico è lo scandalo danese degli ingenti rimborsi chiesti dal Fisco ad alcuni beneficiari di assegni familiari perché fraudolenti: l'algoritmo che aveva individuati le presunte frodi era basato su pregiudizi (sociali e razziali). Si veda B. TEN SELDAM, A. BRENNINKMEIJER, *The Dutch benefits scandal: A cautionary tale for algorithmic Enforcement*, in *EU Law Enforcement*, 2021 (April 30).

il machine learning (che possono contenere indicatori sensibili o essere scarsamente rappresentativi) o dai *pattern* ritenuti rilevanti per la decisione²⁷. Ciò potrebbe anche derivare da uno «statistical bias» che si avrà, dato che un «set di dati [è] imparziale solo per un singolo tipo di problema», se tale set viene «utilizzato per un diverso tipo di problema [...] e quindi risultare distorto»²⁸.

e) *Interazione uomo-robot*. Il riferimento è alle «dinamiche di percezione di entrambe le parti»²⁹ che può essere inteso sia in senso psicologico (attaccamento, repulsione, ecc.)³⁰, sia in chiave etica. Da quest'ultimo punto di vista, un possibile approccio è quello basato sulla distinzione tra agenti morali e pazienti morali. La questione, in questo caso, è «come queste macchine dovrebbero comportarsi nei confronti degli esseri umani e, d'altro canto, come gli esseri umani dovrebbero comportarsi nei confronti di queste macchine». Di fronte alla questione se sia corretto dare calci a un cane robot, possiamo chiederci se quest'ultimo sia un paziente morale (cioè, schematicamente, che prova sensazioni) verso cui un agente morale umano compie atti crudeli o sia anche un agente morale (implicito o esplicito). Le possibili alternative sono quattro: i robot sono agenti e pazienti, solo agenti, solo pazienti, né agenti né pazienti³¹ (v. *infra* punto h per le diverse categorie di agenti).

f) *Automazione e occupazione*. IA e robotica potrebbero, a causa dell'aumento dell'automazione (e di quello correlativo della produttività), trasformare il mercato del lavoro, rendendo di minor valore alcune capacità e obsoleti alcuni mestieri. Sebbene questa dinamica ricorra con molte innovazioni tecnologiche, rispetto a quelle del passato vi è una significativa differenza: mentre «l'automazione classica ha sostituito la forza umana», quella «digitale sostituisce il pensiero umano o l'elaborazione delle informazioni e, a differenza delle macchine, è molto economica da duplicare». Ciò potrebbe condurre a una ««polarizzazione del lavoro»» nella quale i lavori richiesti sarebbero quelli «tecnici altamente qualificati e con alti stipendi» e quelli «di servizio poco qualificati e con bassi salari», mentre quelli in pericolo sarebbero «i lavori di media qualificazione nelle fabbriche e negli uffici, ovvero la maggior parte dei lavori [...] perché sono relativa-

²⁷ L. FLORIDI, *Etica dell'intelligenza artificiale*, cit., parla di limiti epistemici (connessioni basate su prove inconcludenti, imperscrutabili e fuorvianti) e di apofenia, cioè «vedere schemi ricorrenti (patterns) dove in realtà non ne esistono».

²⁸ V.C. MÜLLER, *Ethics of Artificial Intelligence and Robotics*, cit.

²⁹ *Ibid.*

³⁰ L. CRACCO, *Machine ethics: stato dell'arte e osservazioni critiche*, in *Filosofia*, 2020 (65), <https://doi.org/10.13135/2704-8195/5234>, mostra che «in uno studio del 2005, è stato utilizzato un robot per interagire con bambini con disturbi dello spettro autistico».

³¹ S. NYHOLM, *The Ethics of Human-Robot Interaction and Traditional Moral Theories*, in C. VÉLIZ (ed.), *The Oxford Handbook of Digital Ethics*, cit.

mente prevedibili e molto probabilmente destinati a essere automatizzati»³². Questa transizione e i costi sociali che ne deriveranno pongono un importante problema di giustizia distributiva.

A ciò va aggiunto che alcuni lavori sembrerebbero maggiormente tutelati rispetto al pericolo di automazione per il valore intrinseco che viene socialmente riconosciuto all'input umano. Questo riconoscimento li rende meno facilmente sostituibili dalle capacità statistico-generative dell'IA. Così, ad esempio, modelli linguistici come ChatGPT, Claude, o Deepseek, sembrano in grado di sostituire un certo tipo di funzioni lavorative (scrivere un programma informatico), ma non altre (fornire assistenza psico-terapeutica).

g) *Machine Ethics*. Questo tema fa riferimento all'«idea di programmare in qualche modo l'etica in una macchina»³³, cioè «dare alle macchine principi etici o una procedura volti al fine di individuare la soluzione dei dilemmi etici che potrebbero trovarsi di fronte, consentendo loro di funzionare e decidere in modo autonomo ed eticamente responsabile»³⁴. Ciò significa considerare le macchine, «sistemi dell'IA e della robotica», come soggetti dotati «di qualche competenza morale» a cui è possibile attribuire diritti e doveri³⁵: per fare ciò «potrebbe non bastare generare algoritmi nei limiti dei principi etici; sarà necessario infondere i principi morali negli algoritmi stessi»³⁶. La machine ethics e la possibilità «di fornire alle macchine la capacità di prendere decisioni etiche in maniera esplicita», è tuttora un programma di ricerca «e non ha ancora prodotto, a livello pratico, nulla che possa considerarsi minimamente all'altezza delle promesse fatte inizialmente».

La ricerca si è indirizzata sia su «cosa implichi un tale tentativo e se sia desiderabile intraprenderlo», sia sui modi nei quali è possibile dotare una macchina di principi etici. Le ragioni a favore sono, tra altre, legate al fatto che «i sistemi autonomi attualmente in via di sviluppo – come le auto a guida autonoma, i ro-

³² V.C. MÜLLER, *Ethics of Artificial Intelligence and Robotics*, cit.

³³ L. FLORIDI, *Etica dell'intelligenza artificiale*, cit., richiama la sperimentazione del MIT *Moral-Machine* (un sito nel quale venivano proposti dilemmi etici per le auto a guida autonoma e si chiedeva ai partecipanti di indicare quale fosse la scelta corretta) quale esempio di ricerca in questa direzione.

³⁴ M. ANDERSON, S.L. ANDERSON, *General Introduction*, in IDD. (eds.), *Machine Ethics*, Cambridge: Cambridge University Press 2011.

³⁵ F. FOSSA, V. SCHIAFFONATI, G. TAMBURRINI (a cura di), *Etica dei sistemi intelligenti e autonomi: una mappa per orientarsi*, cit.

³⁶ L. CRACCO, *Machine ethics: stato dell'arte e osservazioni critiche*, cit., nota che «la disciplina non si occupa di *software* o di sistemi di intelligenza artificiale che “agiscono” in maniera eticamente accettabile perché le loro funzioni interne implicano di *default* un comportamento che esternamente giudicheremmo morale, senza fare riferimento a valori o teorie etiche. L'obiettivo non è, in altri termini, quello di creare macchine eticamente allineate, ma quello di fornire alla macchina una capacità di formulare giudizi morali complessi in autonomia e in linea di principio “nuovi”».

bot per l'assistenza sanitaria o i droni da guerra – dovranno prendere decisioni morali», a quello per cui è meglio fare in modo che ciò avvenga sulla base di una «capacità di ragionamento etico» e, infine, al dato per cui «le macchine con una capacità di ragionamento etico potrebbero anche migliorare il comportamento etico degli umani»³⁷.

La possibilità di rendere le macchine moralmente autonome ha seguito tre strategie principali: «partendo dall'alto (*top-down*), dal basso (*bottom-up*) o adottando un ibrido tra le due strategie». Le prime due strategie non sono decisive e mostrano vari problemi: la prima, che prevede di creare regole di scelta morale a partire dalle principali teorie etiche – deontologismo, consequenzialismo, etica delle virtù, intuizionismo, non fornisce indicazioni univoche e ha difficoltà di implementazione; la seconda, basata sull'apprendimento a partire da casi concreti, potrebbe seguire esempi sbagliati o non distinguere tra azione e azione corretta. La terza strategia, che sembra quella «più promettente», è quella «dei modelli in cui si combina l'apprendimento dai casi con tecniche di correzione dall'alto»³⁸.

h) *Sistemi autonomi e responsabilità*. In generale, il problema è quello del rapporto tra autonomia, in particolare etica, dei sistemi intelligenti e dei robot e responsabilità, cioè a chi si deve attribuire la responsabilità di un evento negativo. Dato che «l'autonomia nella robotica è relativa e graduale, si dice che un sistema è autonomo rispetto al controllo umano fino a un certo punto»: è perciò necessario capire «chi ha il controllo e chi è responsabile». Tuttavia, non è semplice individuare quali possano essere effettivamente considerati agenti autonomi. Una classificazione è stata proposta da Moor³⁹ nel 2006 che ha identificato, considerando i computer ordinari, cinque categorie: *agenti normativi*, non etici (computer), che lo sono «nel senso limitato in cui possiamo valutare la loro prestazione in termini di quanto bene svolgono i compiti assegnati»; *agenti di impatto etico* che hanno un influsso (idealmente positivo) sul mondo⁴⁰; *agenti etici impliciti* che sono quelli che dispongono di un «software che supporta implicitamente un comportamento etico», che permette alla macchina di agire «eticamente perché le sue funzioni interne promuovono implicitamente un comportamento etico, o

³⁷ *Ibid.*, nota che anche se «l'impresa della *machine ethics* sembra avere dei motivi *prima facie* validi per essere perseguita», sono molti anche quelli negativi.

³⁸ *Ibid.*

³⁹ J.H. MOOR, *The Nature, Importance, and Difficulty of Machine Ethics*, in M. Anderson, S.L. Anderson (eds.), *Machine Ethics*, cit.

⁴⁰ *Ibid.*, indica quale esempio i «fantini robot» che hanno sostituito i ragazzi, liberandoli dalla schiavitù, per guidare i cammelli nelle corse in Qatar.

almeno evitano un comportamento non etico»;⁴¹ *agenti etici espliciti* quelli che sarebbero «in grado di formulare giudizi etici plausibili e giustificarli» ed essere autonomi «in quanto in grado di gestire situazioni di vita reale» imprevedibili e che implicano dilemmi etici⁴²; *agente etico completo* che è quello che «può formulare giudizi etici espliciti e può giustificarli in modo ragionevole» e può esserlo solo «un essere umano adulto».

Di fronte alla possibilità di avere macchine e robot (come le auto a guida autonoma e i robot militari) in grado di essere agenti etici espliciti e capaci di affrontare dilemmi morali come il *trolley problem* per le auto⁴³, il problema è «come dovrebbero essere distribuiti responsabilità e rischi nel complesso sistema in cui operano i veicoli». Si tratta di un problema che richiederà l'adattamento e la modifica dei nostri «attuali schemi concettuali» (etici, giuridici, tecnici) quale potrebbe essere l'attribuzione della personalità giuridica ai robot o l'individuazione di una responsabilità distribuita⁴⁴.

i) *Singularità*. Si tratta della possibilità, prefigurata da Irving John Good nel 1965⁴⁵, che «l'intelligenza artificiale raggiunga un livello di intelligenza umano (IA generale)», che, a questo punto, «i sistemi di IA sviluppino autonomamente sistemi che, superando il livello di intelligenza umano, diventino superintelligenti» (o ultraintelligenti) e che, a loro volta, diano vita a un ulteriore e rapido sviluppo di sistemi ancora più intelligenti. Questo percorso e la svolta che include (essere fuori dal controllo umano) è la singolarità tecnologica il cui sviluppo sarebbe difficile da prevedere⁴⁶. Questo «ciclo di auto-miglioramento ricorsivo, in cui ogni nuova iterazione crea una versione più intelligente di se stessa, culminando nella creazione di una superintelligenza», porta con sé, per alcuni studiosi, il timore che «i sistemi futuri, se non gestiti correttamente, [possano] rappre-

⁴¹ *Ibid.*, quale l'Autopilota di un aereo che contribuisce al fatto che l'aereo arrivi a destinazione in sicurezza e tempo.

⁴² *Ibid.*, p. 16, si chiede: queste macchine saranno in grado di «fare scelte etiche (do ethics) in un modo in cui, ad esempio, un computer può giocare a scacchi?».

⁴³ Questo dilemma etico, proposto da P. Foot, è nella versione originale (ve ne sono diverse) la scelta tra far morire 5 persone che saranno investite da un vagone fuori controllo o salvarle deviando il vagone su un altro binario uccidendone però una che si trova sulla deviazione.

⁴⁴ V.C. MÜLLER, *Ethics of Artificial Intelligence and Robotics*, cit., che rinvia M. TADDEO, L. FLORIDI, *How AI Can Be a Force for Good*, in *Science*, 2018 (361), sostiene questo tipo di responsabilità alla luce del fatto che «gli effetti delle decisioni o delle azioni basate sull'intelligenza artificiale sono spesso il risultato di innumerevoli interazioni tra molti attori, tra cui designer, sviluppatori, utenti, software e hardware».

⁴⁵ I.J. GOOD, *Speculations Concerning the First Ultraintelligent Machine*, in F.L. ALT, M. RUBINOFF (eds.), *Advances in Computers 6*, New York, London: Academic Press, 1965.

⁴⁶ V.C. MÜLLER, *Ethics of Artificial Intelligence and Robotics*, cit. K. VOLD, D.R. HARRIS, *How Does Artificial Intelligence Pose an Existential Risk?*, in C. VÉLIZ (ed.), *The Oxford Handbook of Digital Ethics*, cit., caratterizzano la superintelligenza come «qualsiasi intelletto che superi di gran lunga le prestazioni cognitive degli esseri umani in praticamente tutti i domini di interesse».

sentare una minaccia esistenziale» per il genere umano. Si tratterebbe di un percorso progressivo nel quale ci si troverebbe di fronte a diversi rischi. Il primo è quello della perdita di controllo: «l'opacità e l'imprevedibilità di questi sistemi» e il fatto di essere «strategicamente avvantaggiati (più intelligenti) li rendono potenzialmente pericolosi» in quanto, senza controllo, potrebbero «impazzire prima di quanto pensiamo e prima di avere la possibilità di intervenire». Il secondo è relativo ai possibili «danni per ragioni strumentali» nei quali la «considerazione per la vita umana» potrebbe essere superata dalla necessità di raggiungere un determinato obiettivo o da altre considerazioni⁴⁷. Il terzo è quello del *disallineamento* dei valori, cioè che, nonostante l'IA sia programmata a fini benevoli («o che i suoi valori siano allineati in modo affidabile con i nostri», è possibile che li interpretino in modo distorto o contrario. Questo sia perché è molto difficile definire in modo chiaro i valori, sia in quanto sono suscettibili di diverse interpretazioni⁴⁸.

l) *Ambiente*. Uno dei temi che non è sempre al centro dell'attenzione è «se lo sviluppo dell'IA sia sostenibile dal punto di vista ambientale: come tutti i sistemi informatici, i sistemi di IA producono rifiuti molto difficili da riciclare e consumano grandi quantità di energia, soprattutto per l'addestramento dei sistemi di apprendimento automatico»⁴⁹. ChatGP3, ad esempio, avrebbe prodotto 550 milioni di tonnellate di anidride carbonica in fase di addestramento e richiesto qualcosa come 3,5 milioni di litri d'acqua⁵⁰. In generale, «secondo l'Agenzia internazionale dell'energia, i centri dati, l'intelligenza artificiale e le criptomonete sono responsabili del 2 per cento del consumo mondiale di elettricità, un dato che potrebbe raddoppiare entro il 2026». Allo stesso modo, secondo una stima riportata dal Financial Times «entro il 2027 la crescita dell'IA [potrebbe] produrre un aumento del prelievo idrico compreso tra 4,2 e 6,6 mi-

⁴⁷ K. VOLD, D.R. HARRIS, *How Does Artificial Intelligence Pose an Existential Risk?*, cit., rinviano a S. HAWKING, *Brief Answers to the Big Questions*, London: Hodder & Stoughton, 2018: «[I]l vero rischio con l'IA non è la cattiveria, ma la competenza [...] Probabilmente non sei un malvagio odiatore di formiche che calpesta le formiche per cattiveria, ma se sei responsabile di un progetto di energia verde idroelettrica e c'è un formicaio nella regione da allagare, tanto peggio per le formiche. Non mettiamo l'umanità nella posizione di quelle formiche».

⁴⁸ K. VOLD, D.R. HARRIS, *How Does Artificial Intelligence Pose an Existential Risk?*, cit., mettono in luce ulteriori problemi, quali: la possibilità che si scateni, senza la necessaria prudenza, una corsa all'IA da parte dei diversi gruppi in vista dei vantaggi strategici che potrebbe avere l'IA avanzata; la militarizzazione dell'IA in riferimento al suo uso da parte di attori malintenzionati, il rischio di armi letali completamente autonome e quello della presenza di un'IA malintenzionata.

⁴⁹ V.C. MÜLLER, *Ethics of Artificial Intelligence and Robotics*, cit.

⁵⁰ L. TECEME, *Qual è l'impatto ambientale dell'intelligenza artificiale*, 2024, <https://valori.it/impatto-ambientale-intelligenza-artificiale/>

liardi di metri cubi all'anno, più o meno la metà di quanta ne consuma il Regno Unito»⁵¹.

3. Etica del digitale e dell'IA

L'etica dell'IA è una ramificazione dell'etica del digitale, ossia «quel settore dell'etica che studia e valuta i problemi morali relativi a dati e informazioni», e che comprende tre settori di ricerca (etica dei dati, degli algoritmi e delle pratiche) tra loro strettamente intrecciati. Si tratta di un'indagine intrapresa per «formulare e supportare soluzioni moralmente buone, per esempio buone condotte o buoni valori» con l'obiettivo di rendere «la regolazione digitale e la governance digitale» non solo «sostenibil[i] [o accettabili], ma anche socialmente preferibil[i] (equ[e])»⁵²

Come già indicato, l'etica dell'IA è un'etica *applicata* (applied ethics) che cerca di dare risposte alle questioni etiche o a specifici dilemmi morali che si presentano in determinati ambiti di attività o di ricerca. L'etica digitale, per lungo tempo, non si è trovata di fronte a veri e propri dilemmi morali come avviene, ad esempio, nella bioetica (eutanasia, gestazione per altri), ma piuttosto problemi generali (anche futuribili) e, di conseguenza, cerca di indicare linee di scelta volte a rendere l'IA, come visto, socialmente vantaggiosa. I compiti dell'etica dell'IA sono perciò quelli di individuare «quali sono i problemi etici rilevanti» e di formulare principi e metodi per giungere a soluzioni eticamente valide. In sostanza, l'etica digitale applicata ha cercato di individuare alcuni principi e un metodo per giungere alla soluzione (spesso da tradurre in termini giuridici) dei diversi problemi che l'IA pone (come abbiamo visto, violazioni della privacy, manipolazione del comportamento, opacità, discriminazioni, equità sociale, desiderabilità di macchine etiche, rischi esistenziali).

Per capire come l'etica dell'IA individua e tratta queste situazioni, è necessario partire dalle riflessioni che vengono sviluppate negli altri livelli della ricerca etica. L'etica applicata è infatti solo una parte dell'indagine etica che comprende anche l'etica *normativa* e la *metaetica*⁵³. Le prime due sono relative, in modi diversi, alle scelte dei soggetti (etica applicata e normativa), mentre la terza analizza le

⁵¹ G. CRESCENTE, *Il peso dell'intelligenza artificiale sull'ambiente*, 2024, <https://www.internazionale.it/notizie/gabriele-crescente/2024/03/22/intelligenzaartificialemambiente>, nota che questa «crescita sta già mettendo in crisi le reti elettriche di alcuni paesi, come l'Irlanda, che dopo aver cercato per anni di attirare i giganti del settore dell'informatica, ha recentemente deciso di limitare le autorizzazioni per nuovi centri dati».

⁵² L. FLORIDI, *Etica dell'intelligenza artificiale*, cit.

⁵³ V.C. MÜLLER, *The History of Digital Ethics*, cit., sottolinea che «i campi della filosofia pratica sono trattati in genere come il cugino povero e un po' imbarazzante che deve lavorare per vivere piuttosto che avere soldi in banca».

basi di queste scelte. La prima, come visto, riguarda scelte pratiche (ad es., «Il suicidio assistito è eticamente accettabile?», la machine ethics è auspicabile?), la seconda, le impostazioni generali di tali scelte (ad es., è necessario promuovere il miglior risultato, vanno seguiti i principi che sono universalizzabili, è necessario essere virtuosi per fare scelte corrette), la terza, i fondamenti di tali scelte (ad es., «quando pronunciamo giudizi etici come “uccidere innocenti è sbagliato”, stiamo esprimendo le nostre convinzioni o stiamo facendo qualcos'altro?» Vi sono fatti etici?)⁵⁴.

In generale, le teorie etiche normative sono quelle che cercano di stabilire valori di riferimento per guidare giudizi e azioni, con ciò stabilendo cosa è giusto e cosa è sbagliato. Vi sono tre correnti principali: il *conseguenzialismo*, che ha quale riferimento «i risultati delle azioni»; le *teorie deontologiche*, focalizzate «sulla natura delle azioni»; l'*etica delle virtù*, centrata sul «carattere morale dell'agente». Per il consequenzialismo, è moralmente giusto ciò che produce «i migliori risultati complessivi»⁵⁵, perciò «un atto o una regola vanno valutati in relazione agli effetti che producono, ovvero in base alla loro capacità di realizzare un qualche bene identificabile». La corrente più importante di questo approccio è l'*utilitarismo* che sostiene che «l'oggetto di valore da tenere in considerazione è l'utilità, che può essere intesa, a seconda delle diverse versioni utilitariste, come piacere, come felicità o come soddisfazione di preferenze» (welfarismo) e che «la valutazione delle conseguenze», cioè se una scelta conduce alla massimizzazione dell'utilità per il maggior numero di persone (benessere collettivo definito come somma delle utilità) deve essere «formulata da un osservatore imparziale in termini di utilità aggregata» (ordinamento somma)⁵⁶.

Le teorie deontologiche di derivazione kantiana cercano di determinare quali possono essere le «regole fisse e generali di azione morale» che, «formulate a un livello di elevata astrazione», hanno «un'applicabilità universale». Ciò può essere fatto, ad esempio, in base all'imperativo categorico kantiano espresso nei termini del principio di universalizzazione («agisci solo secondo quella massima che puoi allo stesso tempo volere che diventi una legge universale») o come rispetto universale per la dignità e l'autonomia morale delle persone («non trattare l'umanità mai semplicemente come un mezzo per raggiungere un fine, ma sempre allo stesso tempo come un fine»).

⁵⁴ Si veda, T. MCPHERSON, D. PLUNKETT, *Introduction. The Nature and Explanatory Ambitions of Metaethics*, in IDD. (eds.), *The Routledge Handbook of Metaethics*, Abington: Routledge, 2018, pp. 2 ss.

⁵⁵ P. BODDINGTON, *AI Ethics. A Textbook*, cit., pp. 231-232.

⁵⁶ B. CASALINI, L. CINI, *Giustizia, uguaglianza e differenza*, Firenze: Firenze University Press, 2012, p. 14.

L'etica della virtù ha le sue radici nella filosofia greca (in particolare Aristotele) e si basa su tre concetti ne derivano: *arête* (eccellenza o virtù), *phronesis* (saggezza pratica, prudenza) ed *eudaimonia* (fioritura umana o felicità). A differenza degli approcci consequenzialisti e deontologici, questo orientamento non valuta le azioni (in relazione alle conseguenze o ai doveri), ma si basa «sulle caratteristiche morali dei singoli agenti [...] (come l'onestà, l'umiltà, il coraggio, la compassione)» e l'utilizzo della saggezza pratica (esperienza di vita e capacità di capire i diversi aspetti di una situazione) nelle scelte etiche⁵⁷.

La *metaetica*, invece, studia la natura generale dell'etica ponendosi quattro domande basilari: a) cosa facciamo e a cosa ci riferiamo quando utilizziamo le espressioni etiche quali giusto o sbagliato (indagine semantica); b) qual è la natura, se esiste, dei fatti e proprietà morali a cui ci riferiamo, se sono cioè fatti o desideri (indagine metafisica); c) quali stati mentali abbiamo quando usiamo espressioni morali, se si tratta di credenze o attitudini conative (indagine psicologico-cognitiva); d) ammesso che esistano, come possiamo conoscere le entità morali a cui ci riferiamo (indagine epistemologica)⁵⁸.

Le etiche normative sembrano essere un punto di partenza importante per la soluzione delle questioni etiche legate all'IA. Un'etica consequenzialista, ad esempio, permette di valutare «l'introduzione di nuove tecnologie [...] in base ai benefici e ai danni complessivi» che può comportare. Questi approcci si prestano cioè all'utilizzo «di metodi computazionali di analisi quantitativa in cui [...] i potenziali danni e benefici di un particolare corso d'azione possono essere conteggiati [...], opportunamente adattati per scala e probabilità di impatto e ottimizzati per un risultato netto vantaggioso». Vi sono poi ampie applicazioni delle teorie deontologiche, ad esempio, nei diversi codici di etica dell'IA che prescrivono regole e doveri di applicazione generale, come rispettare la privacy degli individui, non generare danni, cercare di dar vita a sistemi equi, ecc. L'etica della virtù sembra poi fornire un utile strumento preparatorio, e di metodo, che indica di basarsi su «tratti specifici di eccellenza morale» nel proprio comporta-

⁵⁷ S. VALLOR, *Virtues in the Digital Age*, in C. VÉLIZ (ed.), *The Oxford Handbook of Digital Ethics*, cit.; R. HURSTHOUSE, G. PETTIGROVE, *Virtue Ethics*, in E.N. ZALTA e U. NODELMAN (eds.), *The Stanford Encyclopedia of Philosophy*, cit., 2023.

⁵⁸ L'analisi metaetica è fondamentale per questioni quali quelle dell'allineamento dei valori (supra punto 2i). Si possono distinguere due grandi gruppi di teorie metaetiche: il *cognitivismo* e il *non cognitivismo*. Per il primo, le cui due principali correnti sono il *naturalismo* e il *non naturalismo*, vi sono fatti etici e perciò valori che possiamo conoscere; per il secondo, la cui principale corrente è l'*espressivismo*, questi fatti non esistono, i giudizi etici esprimono desideri e i valori sono relativi.

mento digitale e di esercitare la prudenza pratica nelle «dinamiche morali degli ambienti digitali»⁵⁹.

Tuttavia, questi approcci di etica normativa hanno mostrato una serie di importanti problemi. Il consequenzialismo corre il «rischio di trascurare danni e benefici non quantificabili», di non tenere conto, in particolare nell'utilitarismo, delle «richieste di giustizia e dei diritti morali dell'individuo», di ignorare la difficoltà del calcolo delle conseguenze, specialmente nel campo digitale caratterizzato da «complessità, innovazione, e interdipendenza sistemica».

Le teorie deontologiche hanno il problema della difficoltà di applicazione dei principi generali individuati, quella di stabilire «un metodo rigoroso e affidabile per conciliare doveri contrastanti o per risolvere casi in cui esiste più di un modo per seguire tutte le regole o, molto più comunemente, nessun modo per seguirle tutte», quella della «relativa insensibilità al contesto morale e alla particolarità» dei diversi casi⁶⁰. L'etica della virtù non riesce a produrre in qualche modo principi codificabili, a fornire un resoconto adeguato di quale deve essere l'azione giusta (si può compiere un'azione giusta senza essere virtuosi e una persona virtuosa può compiere l'azione sbagliata), vi può essere un conflitto tra diverse virtù, le diverse culture possono sostenere virtù diverse⁶¹.

Una proposta ulteriore per sviluppare l'etica dell'IA è il *principialismo* (principlism). Si tratta di un approccio che è stato sviluppato nell'ambito della bioetica da Beauchamp e Childress⁶² e che una serie di autori ha proposto di utilizzare per l'IA⁶³. È una proposta che individua quattro principi etici (beneficenza, non maleficenza, autonomia, giustizia) che sono considerati la chiave per superare le difficoltà di applicazione delle etiche normative alle diverse questioni pratiche. I quattro principi vengono infatti visti come principi *intermedi* che «non sono concepiti come assiomi o principi supremi – come ad esempio l'imperativo kantiano, o la formula della massimizzazione della felicità nell'utilitarismo –, ma [...] come principi che intermediano tra quelli “supremi” e la pratica dei casi concre-

⁵⁹ P. BODDINGTON, *AI Ethics. A Textbook*, cit.; S. VALLOR, *Virtues in the Digital Age*, cit., che aggiunge che «nel contesto più ristretto dell'etica aziendale e organizzativa», vi sono «forme correlate di analisi costi-benefici (CBA) adattate alla “gestione del rischio” etica».

⁶⁰ S. VALLOR, *Virtues in the Digital Age*, cit., che sottolinea, per il deontologismo, il problema di «stabilire quali doveri sono più importanti da soddisfare», di cosa fare «quando il modo migliore per seguire una regola (ad esempio, rispettare la privacy degli utenti) sembra a tutti gli effetti incompatibile con un'altra (come garantire la trasparenza o promuovere l'equità)».

⁶¹ R. HURSTHOUSE, G. PETTIGROVE, *Virtue Ethics*, cit.

⁶² T.L. BEAUCHAMP, J.F. CHILDRESS, *Principles of Biomedical Ethics*, Oxford: Oxford University Press, 2019.

⁶³ L. FLORIDI ET AL., *AI4People-An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations*, in *Minds and Machines*, 2018 (28).

ti»⁶⁴. L'idea di fondo è «che gli aspetti moralmente rilevanti di molte situazioni del mondo reale non possono essere ridotti a un singolo, supremo principio morale, ma devono essere catturati da una pluralità di principi irriducibili». I quattro principi derivano (o fanno parte) dalla *common morality*, cioè sono «requisiti morali universali e fondamentali che tutte le persone imparziali e moralmente impegnate accettano». In questa impostazione, i principi, che per essere utilizzati devono essere specificati rispetto ai casi, sono *prima facie*, si applicano cioè a meno che non entrino in conflitto, in una determinata situazione, con qualcuno degli altri principi (ad esempio, in bioetica, autonomia vs. beneficenza). I principi sono «ragioni morali a favore o contro certi atti in ogni caso a cui si applicano»: la soluzione avviene attraverso un *bilanciamento* nel quale vengono valutati il peso e l'importanza dei diversi principi. La possibilità di soluzioni contrastanti e la necessità di giustificare il risultato richiede, per il principialismo, un metodo di valutazione specifico, l'equilibrio riflessivo che è un requisito di coerenza tra scelte, principi e intuizioni morali⁶⁵.

L'adozione del principialismo per l'etica dell'IA è motivata da tre aspetti preminenti: «l'enorme volume di principi proposti» nel campo dell'IA dai vari enti e strutture che «rischia di risultare soverchiante e fuorviante», «un elevato grado di sovrapposizione»⁶⁶ tra i principi proposti, il fatto che tra «le aree dell'etica applicata, la bioetica è quella che più assomiglia all'etica digitale nell'affrontare ecologicamente nuove forme di agenti, pazienti e ambienti»⁶⁷. I quattro principi bioetici sembrano per questo adattarsi «bene alle nuove sfide etiche poste dall'IA»: ad essi, va affiancato, per le peculiarità dell'IA, un «ulteriore nuovo principio: l'esplicabilità, intesa come incorporazione sia di intelligibilità che di responsabilità».

Da questa prospettiva, l'etica dell'IA si baserebbe dunque su cinque principi, beneficenza, non maleficenza, autonomia, giustizia, esplicabilità. Li vediamo brevemente:

– *beneficenza*: fare del bene può essere sintetizzato nel rispetto della dignità umana e della sostenibilità. Per quest'ultimo aspetto, «la tecnologia dell'IA deve essere in linea con [...] l'assicurare le precondizioni di base per la vita sul nostro

⁶⁴ G.N. PINTO, *I fondamenti epistemologici della bioetica*, in *L'Altro Diritto*, 2019 (3).

⁶⁵ T.L. BEAUCHAMP, O. RAUPRICH, *Principlism*, in H. TEN HAVE (ed.), *Encyclopedia of Global Bioethics*, Cham: Springer, 2016.

⁶⁶ L. FLORIDI, *Etica dell'intelligenza artificiale*, cit., che nota che «l'enorme volume di principi proposti [...] rischia di diventare soverchiante e fuorviante, sollevando due potenziali problemi. O i vari insiemi di principi etici per l'IA sono simili, portando a inutili ripetizioni e ridondanze, oppure, se differiscono in modo significativo, sono suscettibili di ingenerare confusione e ambiguità».

⁶⁷ L. FLORIDI ET AL., *AI4People-An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations*, cit.

pianeta, la continua prosperità per l'umanità e la conservazione di un buon ambiente per promuovere il benessere delle persone e del pianeta»;

– *non maleficenza*: si pone «contro le varie conseguenze negative derivanti dall'uso eccessivo o improprio delle tecnologie» che comprende: «la prevenzione delle violazioni della privacy», «le minacce di una corsa agli armamenti» basati sull'IA, «l'automiglioramento ricorsivo dell'IA» e richiede di operare «all'interno di limiti sicuri»;

– *autonomia*: nel contesto dell'IA, questo principio «significa trovare un equilibrio tra il potere decisionale che ci riserviamo e quello che deleghiamo agli agenti artificiali» e implica la possibilità che l'autonomia di questi ultimi sia «resa intrinsecamente reversibile, qualora l'autonomia umana debba essere protetta o ristabilita»;

– *giustizia*: significa «promuovere la prosperità, preservare la solidarietà, evitare l'iniquità», eliminare «tutti i tipi di discriminazione» e il «rischio di distorsioni (bias) negli insiemi di dati utilizzati per addestrare i sistemi di IA»;

– *esplicabilità*: è un principio che «completa gli altri quattro: affinché l'IA sia benefica e non malefica, dobbiamo essere in grado di comprendere il bene o il danno che sta effettivamente facendo alla società e in quali modi; affinché l'IA promuova e non limiti l'autonomia umana, la nostra “decisione su chi dovrebbe decidere” deve essere informata dalla conoscenza di come l'IA agirebbe al nostro posto [...] affinché l'IA sia giusta, dobbiamo sapere chi ritenere eticamente o legalmente responsabile in caso di un esito grave e negativo»⁶⁸. Persegue gli stessi obiettivi, quale corrente dell'etica applicata, l'approccio dell'etica umanistica (*humanistic ethics*). Questa impostazione ha quale punto di partenza, come il principlismo, le insufficienze e difficoltà dell'etica normativa e pone come obiettivo dell'innovazione tecnologica e dell'impatto dell'IA «lo sviluppo e la fioritura umana» (del singolo e di tutti) nella direzione di una «prosperità condivisa e del bene comune». Allo stesso modo, viene richiamata la bioetica come disciplina di riferimento e l'utilizzo di un metodo ex ante volto a prevedere i rischi dell'IA. I principi di base di questo approccio sono, in estrema sintesi, la pluralità dei valori da considerare, l'importanza delle procedure di scelta, la partecipazione alla definizione del «benessere umano e della moralità»⁶⁹.

⁶⁸ L. FLORIDI, *Etica dell'intelligenza artificiale*, cit.

⁶⁹ R. FIORAVANTE, A. VACCARO, *Introduction*; IDD., *Humanism, Dehumanization, Integral Human Development: An Overview of Boundaries and Capabilities of Human-Centered Artificial Intelligence in Business and Organizations*; J. TASIOLAS, *Artificial Intelligence, Humanistic Ethics*, tutti in R. FIORAVANTE, A. VACCARO (eds.) *Humanism and Artificial Intelligence*, Cham: Springer, 2025.

4. Dall'Etica alla regolamentazione dell'IA

I principi etici e gli approcci sopra descritti hanno spesso influenzato le regolamentazioni sull'IA discusse e adottate negli ultimi anni. L'Unione Europea (UE) ha svolto un ruolo pionieristico in questo ambito, producendo numerosi documenti, soprattutto negli ultimi cinque anni. Tuttavia, la debolezza del settore tecnologico europeo ha suscitato scetticismi riguardo alla necessità di introdurre nuovi principi, norme e standard giuridici. Nonostante ciò, considereremo l'UE come un osservatorio privilegiato, in quanto rappresenta un interessante laboratorio di regolamentazione dell'IA.

4.1. Le linee guida etiche sull'AI (AI HLEG): un approccio principialista

L'approccio europeo all'IA è incentrato sul rispetto della centralità dell'essere umano nello sviluppo e nell'impiego di questa tecnologia, un valore spesso definito come *human-centric A.I.*⁷⁰. Il primo documento giuridico della strategia europea in materia è stato l'*Ethics Guidelines for Trustworthy Artificial Intelligence*, pubblicato nel 2019 dal gruppo di esperti indipendenti di alto livello. Queste linee guida, di natura non vincolante, stabiliscono che un'IA può essere considerata affidabile solo se basata su quattro principi fondamentali: rispetto dell'autonomia umana, prevenzione dei danni, giustizia (intesa come fairness) e spiegabilità.

Per tradurre questi principi in pratica, le linee guida individuano sette requisiti specifici che i sistemi di IA devono dimostrare di avere: 1) Intervento e sorveglianza umani; 2) Robustezza tecnica e sicurezza; 3) Riservatezza e governance dei dati; 4) Trasparenza (intesa come tracciabilità e spiegabilità dei processi); 5) Diversità, non discriminazione ed equità; 6) Benessere sociale e ambientale; 7) Responsabilità (intesa come verificabilità, segnalazione degli effetti negativi potenziali e loro minimizzazione). A supporto dell'attuazione di questi requisiti, le linee guida includono una lista di valutazione sotto forma di questionario, destinata agli operatori del settore, con l'obiettivo di rendere i criteri più operativi e applicabili nella pratica.

L'approccio etico delineato in queste linee guida si ispira al principialismo, come evidenziato dall'assenza di una gerarchia tra i sette principi fondamentali. Questa scelta implica che, in situazioni di conflitto o interferenza tra i principi – ad esempio, tra robustezza e benessere ambientale – sarà necessario operare un bilanciamento, valutando attentamente le specificità del contesto di applicazione.

⁷⁰ A citare questo principio è lo stesso portale dell'UE: <https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence>.

Un ulteriore aspetto rilevante sottolineato nel documento è la reale portata di questi principi, che assumono piena pregnanza nei casi in cui siano direttamente o indirettamente coinvolti esseri umani. Al contrario, nelle applicazioni puramente industriali, la loro rilevanza potrebbe risultare attenuata. Tuttavia, benché questa sia una precisazione ragionevole, la distinzione tra ambiti di applicazione umani e industriali non è sempre netta e facilmente definibile.

4.2. L'AI Act: proporzionalismo ponderato

La strategia europea assume contorni decisamente più concreti con l'Artificial Intelligence Act (AIA), il regolamento più dibattuto degli ultimi anni in questo ambito. A differenza delle linee guida precedenti, l'AIA introduce un quadro normativo articolato e giuridicamente vincolante, caratterizzato però da un'elevata complessità nell'implementazione. Il regolamento disciplina in modo estensivo l'intero ciclo di vita dell'IA – dalla progettazione allo sviluppo fino all'utilizzo – superando un approccio frammentario legato a singoli aspetti, come la privacy o la responsabilità civile.

Nei prossimi anni, chiunque voglia produrre o commercializzare tecnologie basate sull'IA all'interno dell'Unione Europea dovrà conformarsi agli standard stabiliti dall'AIA e dai relativi atti implementativi. In questo senso, il regolamento può essere considerato una sorta di «Costituzione europea sull'IA», destinata ad avere un impatto cruciale sulla strategia europea. La sua efficacia sarà determinante per rendere l'UE un mercato attrattivo per l'IA e per esercitare un'influenza normativa a livello globale, secondo il cosiddetto Brussels effect, ovvero la capacità dell'UE di imporre i propri standard su scala internazionale.

Alcuni segnali preliminari di questo effetto sono riscontrabili in alcune proposte legislative avanzate negli Stati Uniti a livello dei singoli stati, sebbene l'approccio federale americano, come vedremo, si differenzi sensibilmente da quello europeo. È sicuramente possibile che l'impatto dell'AIA sulla legislazione globale sia molto più ridimensionato di quello che ci si aspetta, ma per il momento sembra aver orientato il dibattito su alcune questioni nodali (e.g., la valutazione del rischio).

L'AIA introduce un quadro normativo che classifica i sistemi di IA in quattro categorie di rischio: inaccettabile, alto, limitato e minimo. In base a questa classificazione, il legislatore adotta un approccio proporzionato, distribuendo gli oneri normativi in modo da prevenire o mitigare i potenziali impatti negativi dell'IA. I sistemi ritenuti a rischio inaccettabile, ovvero quelli che minacciano i valori fondamentali europei e i diritti fondamentali – come nel caso dei sistemi di social scoring – sono vietati del tutto. Per le categorie di rischio inferiore, invece, vengono introdotti obblighi di conformità progressivi, che impongono

oneri crescenti agli sviluppatori e, in misura ancora maggiore, agli utilizzatori dei sistemi di IA, con l'obiettivo di ridurre i rischi e prevenire eventuali danni.

I sistemi ad alto rischio sono soggetti agli obblighi più stringenti, che includono: a) il rispetto di rigorosi requisiti sulla qualità dei dati di addestramento, b) la rendicontazione trasparente delle informazioni rilevanti, c) l'obbligo per i *deployers* (chi utilizza il sistema) di effettuare una valutazione d'impatto sui diritti fondamentali.

Tuttavia, questa ultima disposizione ha sollevato diverse perplessità. Da un lato, emergono dubbi metodologici riguardanti l'effettiva coerenza e armonizzazione delle valutazioni tra i diversi attori coinvolti⁷¹. Dall'altro, si rileva una questione più profonda di natura istituzionale: affidare il bilanciamento tra diritti fondamentali, una funzione tradizionalmente riservata agli organi giurisdizionali, a soggetti privati potrebbe compromettere la coerenza e l'imparzialità del processo.

Queste criticità sollevano interrogativi sull'efficacia e sull'equità del quadro normativo proposto, rendendo necessario un attento monitoraggio della sua implementazione pratica.

La classificazione dei sistemi di IA in categorie di rischio è basata su criteri computazionali e, soprattutto, sugli ambiti di utilizzo che vengono delineati in termini piuttosto generici, includendo settori come l'educazione, la giustizia, i processi democratici e i servizi essenziali. Se un sistema di IA viene sviluppato o utilizzato in questi ambiti, viene automaticamente classificato come ad alto rischio, indipendentemente dalle specificità del caso d'uso.

Tuttavia, per affrontare contesti più complessi e variegati, come quelli legati all'IA ad uso generale, inclusa l'IA generativa, l'AIA introduce la nozione di «significatività del rischio», un criterio che impone di valutare in modo più dettagliato l'impatto potenziale della tecnologia. In questo contesto, si considerano fattori come i soggetti esposti e la magnitudine del rischio, permettendo un'analisi più contestualizzata e adattabile.

L'approccio basato sul rischio dell'AIA è uno dei principali punti di forza della strategia regolatoria dell'UE. Questo approccio consente, infatti, di stabilire un ordine di priorità valoriale e di obiettivi, definendo chiaramente quali ambiti richiedano maggiore attenzione e intervento; responsabilizzare i policy-maker, fornendo un quadro strutturato per bilanciare innovazione e protezione dei diritti fondamentali; valutare i costi sociali associati all'impiego dell'IA, assicurando un bilanciamento tra benefici e potenziali impatti negativi. Le normati-

⁷¹ C. NOVELLI, G. GOVERNATORI, A. ROTOLO, *Automating Business Process Compliance for the EU AI Act*, in G. SILENO ET AL. (eds.), *Legal Knowledge and Information Systems*, Amsterdam: IOS Press, 2023.

ve basate sul rischio offrono, inoltre, strumenti utili per affrontare l'incertezza tecnologica, fornendo risposte sia qualitative che quantitative attraverso metodologie consolidate, come l'analisi costi-benefici. Questo approccio fornisce una base razionale per la gestione delle complessità legate all'adozione dell'IA, garantendo flessibilità e adattabilità alle diverse evoluzioni tecnologiche e sociali.

Per tutte queste caratteristiche, l'AIA sembra ispirarsi a un approccio etico di matrice consequenzialista, in quanto pone al centro dell'attenzione le conseguenze – positive o negative – derivanti dall'uso dell'IA, con particolare riguardo alla possibilità di ledere diritti fondamentali. Tuttavia, l'AIA non può essere considerato interamente consequenzialista o utilitaristico, poiché riconosce un valore intrinseco a determinati principi morali, introducendo così un elemento deontologico e, nel bilanciamento, principialista. Questo equilibrio tra conseguenze e principi diversi richiama una prospettiva proporzionalista, in cui la deviazione da determinati principi è giustificabile solo in presenza di circostanze che lo rendano strettamente necessario⁷².

Secondo questa impostazione, per giustificare moralmente un'azione che comporta potenziali danni, è indispensabile dimostrare – ed è qui che emerge l'aspetto più consequenzialista dell'approccio – che i benefici risultanti siano quantitativamente e qualitativamente superiori o almeno proporzionati ai danni. L'AIA, in questo senso, cerca di bilanciare il principio di precauzione, volto a proteggere individui e gruppi vulnerabili, con interessi individuali (ad esempio, la tutela dei diritti dei consumatori) e collettivi (come la promozione dell'innovazione tecnologica). Un esempio tipico di questo bilanciamento è rappresentato dal trade-off tra sicurezza e privacy: se un sistema di IA migliora la sicurezza pubblica, è accettabile una riduzione della privacy solo se il beneficio ottenuto è proporzionato e giustificato rispetto al sacrificio imposto.

Uno dei limiti principali del proporzionalismo, e quindi dell'impianto etico dell'AIA, risiede nelle difficoltà legate alla quantificazione e commensurabilità dei diversi fattori coinvolti. Bilanciare elementi di natura etica, economica e sociale richiede criteri abbastanza chiari che spesso sono difficili da definire e applicare in modo uniforme, rendendo il processo vulnerabile a interpretazioni soggettive. Inoltre, l'assenza di parametri univoci rischia di generare discrepanze nelle valutazioni di conformità.

Nonostante queste criticità, il bilanciamento tra diritti e interessi è una pratica consolidata nel diritto, che legislatori e giudici esercitano abitualmente per ri-

⁷² B. HOOSE, *Proportionism: The American Debate and its European Roots*, Washington, DC: Georgetown University Press, 1987. L'utilizzo dei principi intermedi (beneficenza, non maleficenza ecc.) consente, nei bilanciamenti, di arrivare a compromessi nei casi in cui non vi sia accordo sui valori fondamentali in conflitto.

solvere conflitti tra principi di pari rango, come quelli di natura costituzionale⁷³. Analogamente, un'applicazione e un'interpretazione dell'AIA ispirata a questa logica potrebbero favorire decisioni coerenti e trasparenti, contribuendo a una regolamentazione dell'IA che sia al tempo stesso efficace e rispettosa dei valori fondamentali dell'Unione Europea.

4.3. Il resto del mondo

Come anticipato, la strategia di regolamentazione adottata dall'Unione Europea è attualmente la più articolata e complessa. Tuttavia, diversi paesi stanno progressivamente cercando di introdurre proprie normative e standard per disciplinare la commercializzazione dell'IA. Alcuni di essi, come il Regno Unito e il Canada, sembrano allinearsi all'approccio europeo basato sui principi, enfatizzando aspetti etici e valoriali nella gestione dell'IA. Altri, invece, adottano strategie differenti, come nel caso degli Stati Uniti, il principale attore globale nello sviluppo di questa tecnologia⁷⁴, la cui impostazione normativa merita un approfondimento specifico.

Negli Stati Uniti, a livello federale, l'intervento più significativo finora è stato l'Executive Order (EO) emanato dall'amministrazione Biden, che delineava un primo quadro di principi guida per la regolamentazione dell'IA. Tuttavia, il provvedimento, privo di carattere vincolante per gli Stati federati, è stato revocato poche ore dopo l'insediamento dell'amministrazione Trump, evidenziando la fragilità di un approccio privo di una solida base legislativa⁷⁵.

A livello statale, invece, si osservano sviluppi più concreti, con la California che emerge come il principale laboratorio normativo per l'IA negli Stati Uniti. Lo Stato ha introdotto diverse iniziative legislative, focalizzandosi su temi come la trasparenza degli algoritmi, la protezione dei dati e la responsabilità d'uso, cercando di bilanciare lo sviluppo tecnologico con la tutela dei diritti dei cittadini.

In sintesi, mentre l'UE punta a una regolamentazione dettagliata e preventiva, volta a garantire un elevato livello di protezione dei diritti fondamentali, gli

⁷³ Alcune metodologie di bilanciamento sono presenti in R. ALEX, *On Balancing and Subsumption. A Structural Comparison*, in *Ratio Juris*, 2003 (16), <https://doi.org/10.1046/j.0952-1917.2003.00244.x>, e in A. BARAK, *Proportionality: Constitutional Rights and Their Limitations*, Cambridge: Cambridge University Press, 2012. Viene esplorata l'applicazione di uno di questi due metodi in C. NOVELLI, F. CASOLARI, A. ROTOLO ET AL., *AI Risk Assessment: A Scenario-Based, Proportional Methodology for the AI Act*, in *Digital Society*, 2024 (3), <https://doi.org/10.1007/s44206-024-00095-1>.

⁷⁴ L'Artificial Intelligence Index Report della Stanford University segnala che negli USA sono stati sviluppati 51 dei modelli di IA più rilevanti contro i 21 dell'UE e i 15 della Cina. Fonte: <https://aiindex.stanford.edu/wp-content/uploads/2024/05/HAI-AI-Index-Report-2024.pdf>.

⁷⁵ C. NOVELLI, A. GUR, L. FLORIDI, *Two Futures of AI Regulation under the Trump Administration*, 2025, <http://dx.doi.org/10.2139/ssrn.5198926>

Stati Uniti, pur con approcci differenti a livello federale e statale, privilegiano un modello più flessibile e adattivo, volto a favorire l'innovazione e la competitività nel mercato globale dell'IA. Talvolta, come con l'amministrazione Trump, questa flessibilità è esasperata e diventa una vera e propria svolta verso la deregolamentazione.

Più nel dettaglio, l'EO americano rappresenta l'emblema opposto dell'approccio europeo. È, infatti, un esempio di *soft law* che promuove l'auto-regolamentazione da parte dell'industria dell'IA senza imporre limiti stringenti o standard vincolanti. A differenza dell'AIA europeo, che è esplicitamente basato su principi etici e diritti fondamentali, l'EO adotta un approccio *market-driven*, orientato principalmente alla concorrenza e all'innovazione⁷⁶. Questa impostazione è evidente anche nella totale assenza di sanzioni per il mancato rispetto delle linee guida, lasciando così ampio margine di discrezione agli operatori del settore.

Di conseguenza, l'approccio regolatorio delineato dall'EO non può essere ricondotto a quello dell'"AI Ethics", ossia, come visto, un quadro normativo che promuove valori etici fondamentali. Al contrario, si inserisce nella prospettiva della "AI Safety", che si concentra esclusivamente sulla prevenzione di malfunzionamenti tecnici e danni non intenzionali, senza definire principi etici specifici da proteggere o promuovere. In questo senso, l'EO non si preoccupa delle potenziali discriminazioni o degli impatti sociali più ampi dell'IA, ma piuttosto della sua affidabilità tecnica e della sicurezza operativa.

Un'unica eccezione a questa impostazione emerge nel settore dell'occupazione, in cui l'EO riconosce la necessità di proteggere i lavoratori dai rischi connessi alla sorveglianza tramite IA e dalla possibile disoccupazione derivante dall'automazione. Tuttavia, anche in questo ambito, il documento si limita a formulare raccomandazioni generali senza introdurre misure concrete di tutela.

Sebbene l'EO sembri adottare un approccio privo di un'esplicita presa di posizione etica, si potrebbe obiettare che, implicitamente, sottoscrive una visione morale specifica. Questa visione risulta essere un'ibridazione tra consequenzialismo e deontologia. Dal consequenzialismo, eredita l'attenzione alla minimizzazione delle conseguenze negative e l'applicazione del principio di precauzione, mirato a evitare danni futuri. Tuttavia, il fatto che la sicurezza e la libertà di innovare e auto-regolamentarsi siano considerate valori imprescindibili, non

⁷⁶ Per una sintesi dei più rilevanti elementi di differenza tra la regolamentazione europea basata sui principi e quella americana orientata al mercato, si veda M. WÖRSDÖRFER, *Biden's Executive Order on AI and the E.U.'s AI Act: A Comparative Computer-Ethical Analysis*, in *Philosophy & Technology*, 2024 (37).

negoziabili, rivela la presenza di una componente deontologica, che conferisce a questi principi uno status quasi assoluto.

In definitiva, l'EO riflette un approccio apparentemente pragmatico e privo di riferimenti etici espliciti, ma che, in realtà, incorpora una visione morale sottostante, fondata sull'equilibrio tra precauzione e libertà di mercato.

Su questa scia, nel luglio 2025, l'amministrazione Trump ha anche inaugurato un Action Plan⁷⁷ con l'intento di promuovere le infrastrutture collegate all'IA (ad esempio, i data centers), incoraggiare la competitività dell'industria americana, anche sulla base processi di certificazione velocizzata e finanziamenti federali. Tuttavia, il supporto federale verrà garantito soltanto a quelle aziende che non mostrano pregiudizi ideologici. Il riferimento negativo (ufficioso) è a quelle aziende che hanno aderito a policy che la società americana conservatrice etichetta come «woke» e che spesso si traducono in un approccio etico alla regolamentazione dell'IA (AI Ethics), opposto ad un approccio incentrato sulla mera sicurezza da malfunzionamento (AI Safety).

Un atteggiamento regolatorio che similmente privilegia l'innovazione è emerso anche in Giappone con l' "Act on Promotion of Research and Development and Utilization of Artificial Intelligence-Related Technologies" (2025). Il regolamento ricorre a norme di soft law, stabilendo obiettivi e linee guida strategiche generali e insistendo sull'esigenza che le aziende cooperino tra di loro e con il governo centrale, ma senza prescrivere sanzioni o requisiti obbligatori per la progettazione dei sistemi di IA.

L'approccio della Cina alla regolamentazione dell'IA, sebbene meno articolato rispetto ad altri modelli, presenta alcune somiglianze con la strategia dell'Unione Europea, piuttosto che con quella adottata finora dagli Stati Uniti. Sebbene sia la Cina che gli Stati Uniti abbiano dimostrato una certa flessibilità e apertura verso il business⁷⁸, anche in Cina come in UE la regolamentazione è in gran parte esplicitamente valoriale, sebbene i principi di riferimento siano radicalmente diversi. Mentre l'UE fonda il proprio impianto normativo sui valori liberali e sullo stato di diritto, la strategia cinese intende tutelare anzitutto i valori centrali del Partito Comunista Cinese, ai quali le tecnologie di IA devono rigorosamente conformarsi.

Un aspetto distintivo della regolamentazione cinese è l'obbligo per i modelli di IA generativa di rispettare precise direttive ideologiche, evitando la genera-

⁷⁷ Trump White House, *White House Unveils America's AI Action Plan*, 2025, <https://www.whitehouse.gov/articles/2025/07/white-house-unveils-americas-ai-action-plan/>.

⁷⁸ A. HUYUE ZHANG, *The Promise and Perils of China's Regulation of Artificial Intelligence*, in *Columbia Law School*, April 2024, <https://www.law.columbia.edu/sites/default/files/202404/The%20Promise%20and%20Perils%20of%20Chinese%20AI%20Regulationpdf>

zione di contenuti considerati politicamente sensibili o in contrasto con la narrazione ufficiale. Questo vincolo evidenzia un controllo centralizzato sull'IA, volto a preservare la stabilità politica e sociale secondo le priorità governative.

Un'altra differenza significativa rispetto all'approccio europeo riguarda il processo di autorizzazione. In Cina, qualsiasi modello di IA destinato alla commercializzazione o all'uso pubblico deve ottenere una approvazione preventiva da parte delle autorità governative, in particolare dalla Cyberspace Administration of China (CAC), secondo quanto stabilito dalle "Misure ad Interim per la gestione dei servizi di IA generativa". Questo sistema si discosta dal modello europeo, che prevede valutazioni e certificazioni da parte di agenzie indipendenti, garantendo così una maggiore separazione tra regolatore e soggetti regolati.

5. Visioni critiche

La discussione critica sull'etica dell'IA può essere ricondotta a due visioni principali: una di tipo costruttivo e una di tipo distruttivo.

Nel primo gruppo, rientrano quelle critiche che denunciano l'apparato concettuale e l'imprecisione terminologica dell'etica dell'IA, senza per questo rigettare in maniera globale l'area di ricerca, ma anzi cercando di suggerire dei miglioramenti. La terminologia finora utilizzata sarebbe in grado di evocare intuizioni ingannevoli, capaci di spostare la sensibilità etica e l'attenzione politica verso false credenze o di sopravvalutare profili di secondaria importanza. Questo tipicamente accadrebbe quando si ricorre a metafore o altre forme di linguaggio non letterale. Ad esempio, espressioni come «intelligenza (dell'IA)» o «“allucinazioni” (dei modelli linguistici)» cercherebbero di antropomorfizzare il fenomeno⁷⁹. Bisognerebbe evitare, secondo i critici, di accostare i due campi semantici, come appunto l'intelligenza degli esseri umani a quella forma di ragionamento espressa dai sistemi di IA, che svolgono operazioni di mera associazione statistica.

Talvolta, le critiche costruttive suggeriscono di ridimensionare le aspettative (e le paure) che alimentano i dibattiti etici sull'IA, invitando a trattare questa tecnologia in maniera più neutrale, antropomorfizzandola meno e guardandola più come una infrastruttura (alla pari dell'elettricità). In questo modo, la parte costruttiva di queste critiche suggerisce di spostare l'attenzione della riflessione etico-giuridica verso le risorse materiali e umane che permettono alla tecnologia

⁷⁹ L. FLORIDI, A.C. NOBRE, *Anthropomorphising Machines and Computerising Minds: The Crosswiring of Languages between Artificial Intelligence and Brain & Cognitive Sciences*, in *Minds & Machines*, 2024 (34), <https://doi.org/10.1007/s11023-024-09670-4>.

di esistere e funzionare. Infatti, sarebbero sistematicamente sottovalutate una serie di questioni – e relazioni di potere – relative a come vengono raccolti i dati su cui l'IA viene addestrata, all'impatto ambientale della produzione e conservazione dei dati e allo sfruttamento di lavoratori coinvolti nel processo di produzione (e anche successivamente). Ciò sarebbe dovuto, in parte, all'erroneo apparato concettuale che supporta l'analisi etica in questo ambito.

Un'interessante critica costruttiva è anche quella che stigmatizza l'eccessivo ricorso all'IA per la risoluzione di problemi, siano essi di carattere tecnico o sociale. Il bersaglio polemico di questa critica può essere definito come “tecnottimismo” o “tecnosoluzionismo”⁸⁰. In particolare, ciò che viene avvertito come dannoso per la riflessione etica è lo scarso spirito critico che dovrebbe guidare la scelta strategica di ricorrere all'IA. L'assenza di tale spirito critico porterebbe, in ultima istanza, a sottovalutare la componente ideologico-politica della tecnologia. L'IA diventerebbe una sorta di panacea anche per situazioni che potrebbero essere affrontate senza di essa, e con meno complicazioni. Pertanto, chi sviluppa questa critica sostiene che l'etica dell'IA debba interessarsi in primo luogo (e maggiormente) dell'effettiva necessità di utilizzare questa tecnologia, valutandone il vantaggio in comparazione con soluzioni alternative (che possono contemplare altre tecnologie digitali). In alcuni casi, l'utilizzo dell'IA potrebbe risultare inutile – o addirittura dannoso – perché i problemi che si intendono risolvere fanno parte di una dimensione che precede causalmente quella su cui interviene l'IA. Il problema della discriminazione nelle predizioni dell'IA è in questo senso emblematico. Esso rivela spesso che la discriminazione riguarda i dati di addestramento oppure il modo in cui i dati sono stati raccolti e processati. Magari sono dati inaffidabili o parziali. In situazioni come questa, impiegare acriticamente l'IA non solo risolve il problema, ma rischia di amplificarne la pericolosità.

Nel secondo gruppo rientrano invece le critiche che, contestando l'etica dell'IA su diversi fronti (soprattutto metodologici), ne mettono in dubbio l'intero impianto e lo statuto di riflessione morale indipendente. Spesso, queste critiche la bollano come semplice «ethics washing», un esercizio retorico asservito agli interessi di potenti attori privati, in primis le Big Tech. In realtà, l'ethics washing non è prerogativa esclusiva delle compagnie private, ma emergerebbe anche dai documenti legislativi o di indirizzo di attori pubblici, come stati nazionali e sovranazionali (democratici e non). Secondo alcuni, come James Steinhoff, la subordinazione a interessi privati è frutto di un monopolio intellettuale – sia culturale sia economico – che le grandi aziende esercitano per centralizza-

⁸⁰ J.C. HEILINGER, *The Ethics of AI Ethics. A Constructive Critique*, in *Philosophy & Technology*, 2022 (35), <https://doi.org/10.1007/s13347-022-00557-9>.

re l'innovazione⁸¹. Da tale prospettiva, l'etica dell'IA sarebbe parte integrante di un'agenda capitalistica, con la ricerca affidata in subappalto a organizzazioni e ricercatori (universitari o indipendenti) finanziati in modo diretto o indiretto dalle Big Tech. Ciò influenzerebbe non solo l'elaborazione di principi e linee guida – considerate semplici operazioni di marketing e pubbliche relazioni – ma anche i tentativi di tradurre questi stessi principi in standard pratici, i quali finirebbero sempre subordinati alla necessità di sviluppare rapidamente nuovi modelli e trarne profitto.

Di conseguenza, secondo questa critica «distruttiva», non ci sarebbe una via d'uscita per salvare l'etica dell'IA come vera disciplina e realizzare gli obiettivi che dichiara di perseguire. Finché rimane nei confini della logica capitalistica, non potrà mai costituirsi come riflessione etica indipendente. L'unica strada sarebbe una critica organica ai vincoli strutturali del capitalismo, che richiederebbe però un radicale cambio di passo: lasciare il classico linguaggio etico per una prospettiva più ampia di critica socio-economica.

⁸¹ J. STEINHOFF, *AI Ethics as Subordinated Innovation Network*, in *AI & Society*, 2024 (39), <https://doi.org/10.1007/s00146-023-01658-5>

GLI AUTORI

Aurucci Paola – Titolare di Borsa di Ricerca, Dipartimento di Management “Valter Cantino”, Università di Torino

Billi Marco – Assegnista di ricerca, Dipartimento di Scienze Giuridiche – Centro Alma Human AI, Alma Mater Studiorum Università di Bologna

Bompreschi Chantal – Assegnista di ricerca e Professoressa a contratto, Dipartimento di Scienze Giuridiche – Centro Alma Human AI, Alma Mater Studiorum Università di Bologna

Bongiovanni Giorgio – Professore ordinario, Dipartimento di Scienze Giuridiche – Centro Alma Human AI, Alma Mater Studiorum Università di Bologna

Brighi Raffaella – Professoressa associata, Dipartimento di Scienze Giuridiche – Centro Alma Human AI, Alma Mater Studiorum Università di Bologna

Chiara Pier Giorgio – Ricercatore di tipo a), Dipartimento di Scienze Giuridiche – Centro Alma Human AI, Alma Mater Studiorum Università di Bologna

Contissa Giuseppe – Professore associato, Dipartimento di Scienze Giuridiche – Centro Alma Human AI, Alma Mater Studiorum Università di Bologna

Di Cocco Claudio – Avvocato, Foro di Bologna; Coordinatore e Docente del Master universitario in “Diritto digitale. Dati, algoritmi e intelligenza artificiale”; Docente del Master universitario in “Trattamento dei dati personali e Data Protection Officer”

Di Tano Francesco – Ricercatore di tipo a), Dipartimento di Scienze Giuridiche – Centro Alma Human AI, Alma Mater Studiorum Università di Bologna

Ferrazzano Michele, Professore a contratto, Università di Modena e Reggio Emilia e Università di Milano; Consulente, Dipartimento di Scienze Giuridiche – Centro Alma Human AI, Alma Mater Studiorum Università di Bologna

Galli Federico – Ricercatore di tipo a), Dipartimento di Scienze Giuridiche – Centro Alma Human AI, Alma Mater Studiorum Università di Bologna

Lagioia Francesca – Professoressa associata, Dipartimento di Scienze Giuridiche – Centro Alma Human AI, Alma Mater Studiorum Università di Bologna

Monducci Juri – Avvocato cassazionista, Foro di Bologna; Professore a Contratto, Dipartimento di Scienze Giuridiche – Centro Alma Human AI, Alma Mater Studiorum Università di Bologna

Novelli Claudio – Associate Research Scientist and Research Fellow Lead, Yale Digital Ethics Center, Yale University

Palmirani Monica – Professoressa ordinaria, Dipartimento di Scienze Giuridiche – Centro Alma Human AI, Alma Mater Studiorum Università di Bologna

Sapienza Salvatore – Ricercatore TT, Dipartimento di Scienze Giuridiche – Centro Alma Human AI, Alma Mater Studiorum Università di Bologna

Sartor Giovanni – Professore ordinario, Dipartimento di Scienze Giuridiche – Centro Alma Human AI, Alma Mater Studiorum Università di Bologna e European University Institute, Fiesole

Finito di stampare nel mese di marzo 2026
per i tipi di Bologna University Press