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.

Fondazione Bologna University Press
Via Saragozza 10, 40123 Bologna
tel. (+39) 051 232 882

www.buponline.com
e-mail: info@buponline.com

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/Shutterstook.com

Prima edizione: marzo 2026

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 costitutore 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