NAD
Nuovi Autoritarismi e Democrazie:
Diritto, Istituzioni, Società

Il trattamento dei dati biometrici nel quadro della strategia europea dei dati, fra rischi di *mass surveillance* e tutela dei diritti fondamentali

*Francesca Mollo**

Abstract

The contribution reconstructs the theme of mass surveillance, intertwined with the protection of personal data. It starts to investigate the criticality profiles connected to the treatment of some specific categories of data, in particular biometric data, the treatment of which –systematically and on a large scale – is likely to define new surveillance models.
Under these profiles, the article analyzes the jurisprudence of the European Court of Human Rights and Court of Justice.

Keywords: surveillance, biometric data, data protection.

SOMMARIO: 1. Introduzione. 2. I dati biometrici quali oggetto di trattamenti suscettibili di definire nuovi modelli di sorveglianza. 3. *Segue.* La tutela dei dati biometrici nella prospettiva nazionale ed europea. 4. Il tema della sorveglianza connessa al controllo dei dati nella giurisprudenza della Corte europea dei diritti dell'uomo. 5. La questione della sorveglianza negli orientamenti della Corte di giustizia dell'Unione europea. 6. Conclusioni.

* Ricercatrice di Diritto privato presso il Dipartimento di Sociologia e Diritto dell'Economia, Alma mater Studiorum Università di Bologna. Il saggio è stato sottoposto a doppio referaggio cieco. Responsabile del controllo editoriale: Christian Mosquera Arias.

1. *Introduzione*

Come è stato efficacemente sottolineato[1], la società odierna è caratterizzata da «poteri nuovi, privati, penetranti, opachi», per cui

> il potere è un gioco complesso, a più voci, sempre meno decifrabile, stabile e riconoscibile [...] Grandi imprese, associazioni professionali, burocrazie, gruppi finanziari occupano posizioni strategicamente importanti dove si decidono le nuove regole per il mondo globalizzato. Abbandonate le severe vesti del government, più verticale e decifrabile, a favore di quelle della governance, più orizzontale e diffusa, il potere ha assunto nuove facce, diventando di volta in volta nazionale, internazionale, pubblico, privato, hard, soft, smart, poco visibile, indiretto. Numerosi nuovi attori, non solo poteri finanziari ed economici, ma anche tecnologici e padroni dell'intelligenza artificiale, muovendosi disinvoltamente tra politica ed economia, forgiano le nuove fondamenta del nostro mondo.

L'odierna società dell'informazione si atteggia così sempre più spesso a società della sorveglianza[2] e del controllo, da un lato, e società del rischio[3], dall'altro.

Così il regime di sorveglianza globale vaticinato da Orwell[4] nell'immagine del Grande Fratello – spesso rievocata dalla dottrina[5] – e che tutto conosce del cittadino, anch'esso globale, immerso nella sua solitudine[6] si realizza nella conoscenza e nel trattamento massivo dei dati che caratterizza il nostro tempo. «Ormai la sicurezza è al di sopra delle leggi», si è affermato[7]. Il trattamento massivo di tali dati, incardinato su una struttura circolare del trasferimento di informazioni e sul principio «*make data by data*», infatti, pone le basi per una vera e propria «sorveglianza liquida»[8], orientata sempre più in senso predittivo[9].

Nella «società dell'accesso»[10] la persona è sempre più digitalizzata, profilata e trasparente; si viene delineando una società dell'integrale trasparenza che rievoca la metafora dell'«uomo di vetro»[11], che legittima la pretesa di altri di richiedere e ottenere ogni informazione e che implica la classificazione (*id est*, la divisione in classi) come

---

[1] M.R. Ferrarese, *Poteri nuovi. Privati, penetranti, opachi.*, il Mulino, 2022.
[2] Cfr. S. Rodotà, *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Laterza, 2004, 174.
[3] U. Beck, *La società del rischio. Verso una seconda modernità*, Carocci, 2004, 63.
[4] G. Orwell, *1984*, trad. it., Mondadori, 2002.
[5] Cfr. R. Pardolesi, *Diritto alla riservatezza e circolazione dei dati personali*, Giuffrè, 2003, 13. Cfr. M. Foucault, *Sécurité, territoire, population*, Paris, 2004; Id., *Sorvegliare e punire. Nascita della prigione*, Einaudi, 1976. Cfr., altresì, S. Rodotà, *Libertà personale. Vecchi e nuovi nemici*, in M. Bovero (a cura di), *Quale libertà. Dizionario minimo contro i falsi liberali*, Laterza, 2004, 54.
[6] Z. Bauman, *La solitudine del cittadino globale*, Feltrinelli, 2003, 24.
[7] M. Foucault, *Ormai la sicurezza è al di sopra delle leggi*, in Id., *La strategia dell'accerchiamento. Conversazioni e interventi 1975-1984*, a cura di S. Vaccaro,ed. duepunti, 2009, 63. Cfr. anche D. Lyon, *La cultura della sorveglianza*, trad. it. di C. Veltri, Luiss University Press, 2020.
[8] Z. Bauman, D. Lyon, *La sorveglianza nella modernità liquida*, Laterza, 2015.
[9] Cfr. Garante per la protezione dei dati personali, provvedimento del 24 novembre 2016 n. 488, doc. *web* n. 5796783 (consultabile al sito istituzionale *www.garanteprivacy.it*), che ha bloccato un progetto di banca dati privata per la misura del «*rating* reputazionale».
[10] J. Rifkin, *L'era dell'accesso*, Mondadori, 2001, 17.
[11] Per un'analisi della figura dell'«uomo di vetro» in relazione ai totalitarismi e al rispetto della vita privata, S. Niger, *Le nuove dimensioni della privacy*, Cedam, 2006, 33.

ISSN 2612-6672 | DOI 10.54103/2612-6672/22173

«sospetto, cattivo cittadino, nemico dello Stato» di chiunque rivendichi di mantenere spazi di intimità[12].

In effetti, il binomio accesso-segretezza è strettamente correlato con il potere[13] ed il suo esercizio, laddove «i nuovi poteri sono quelli che riducono la persona a oggetto, dal quale vengono costantemente estratte, con le tecniche più diverse, tutte le possibili informazioni, non solo per le tradizionali, anche se continuamente dilatate, forme di controllo, ma sempre più intensamente per costruire profili e identità, per stabilire nessi e relazioni, di cui ci si serve soprattutto per finalità economiche, per ritagliare dalla persona quel che interessa al mercato»[14]. Ciò segna il passaggio da una sorveglianza mirata ad una generalizzata, che non è più – quantomeno non solo – prerogativa degli Stati per perseguire interessi di portata generale, ma si configura sempre di più quale sorveglianza privata, svolta nel mondo dei consumi e della logica di mercato, «la cui fluidità è posta direttamente in relazione con la possibilità di disporre liberamente di una massa crescente di informazioni»[15], in una sempre più stretta alleanza tra logica di mercato e logica della sicurezza.

Ecco che il valore attribuito delle informazioni cresce esponenzialmente per i grandi attori economici e politici a livello globale[16], mentre pare pericolosamente decrescere in misura pressoché proporzionale per i titolari di dette informazioni[17], che sembrano non avvedersi adeguatamente del fatto che «nella società digitale noi siamo i nostri dati»[18]. I dati, nel contesto della c.d. «dittatura dell'algoritmo»[19], costituiscono una traccia della persona, frammenti della stessa che ne rivelano caratteristiche e peculiarità, anche attinenti alla vita privata, e che nella loro complessità e combinazione/ricombinazione consentono di ricostruire il sistema di relazioni, di vita, di abitudini e di interessi che la caratterizzano.

In questo contesto, in cui la sorveglianza non conosce più spazio, tempo né confini, è evidente come alcune tipologie di dati, come i dati biometrici, svolgano un ruolo chiave.

2. *I dati biometrici quali oggetto di trattamenti suscettibili di definire nuovi modelli di sorveglianza*

In questo contesto, in cui la sorveglianza non conosce più spazio, tempo né confini, è evidente come alcune tipologie di dati, come i dati biometrici, svolgano un ruolo chiave.

Il Regolamento UE 679/2016 in tema di protezione dei dati personali (GDPR) all'articolo 4 par. 1 n. 4, definisce i dati biometrici come i «dati personali ottenuti da un

[12] S. Rodotà, *Tecnopolitica*, cit., 175. Nello stesso senso, Id., *La vita e le regole. Tra diritto e non diritto*, Feltrinelli, 2006, 104.
[13] Cfr. N. Bobbio, *Il futuro della democrazia*, Einaudi, 1995, 215.
[14] S. Rodotà, *Il mondo nella rete, Quali i diritti, quali i vincoli*, Laterza, 2014, 27.
[15] S. Rodotà, *Tecnopolitica*, cit., 136.
[16] A. Joinson, K. Mckenna, T. Postmes, Ulf-Dietrich Reips (eds), *Oxford Handbook of Internet Psychology*, Oxford University Press, 2009.
[17] Cfr. R. D'Orazio, *Protezione dei dati by default e by design*, in S. Sica, V. D'Antonio e G.M. Riccio (a cura di), *La nuova disciplina europea della privacy*, Cedam-WKI, 2016, 88.
[18] Si vedano, in questo senso, le parole del Presidente dell'Autorità Garante per la Protezione dei Dati Personali, Antonello Soro, in occasione della Giornata europea della protezione dei dati del 28 gennaio 2015.
[19] S. Rodotà, *Il mondo della rete*, cit., 37.

 ISSN 2612-6672 | DOI 10.54103/2612-6672/22173

trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici».

Essi rientrano in quella categoria particolare di dati cui il Regolamento pone una specifica attenzione, vietando o limitandone il trattamento, tranne che in alcune particolari situazioni, indicate dall'art. 9 par. 2, solo se tramite il loro trattamento si può giungere all'identificazione univoca o all'autenticazione di una persona fisica[20]. Il GDPR per tali dati, che consentono o confermano l'identificazione univoca dell'individuo, crea cioè una sotto-categoria all'interno della più ampia categoria dei dati particolari disciplinati dall'art. 9, per i quali la liceità del trattamento è ancorata al requisito alternativo del consenso esplicito oppure della necessità, consentendo agli Stati membri di introdurre garanzie supplementari (art. 9, par. 4). Il consenso è quindi alternativo ad altre condizioni indicate dallo stesso art. 9, tra cui l'ipotesi in cui il trattamento sia necessario per motivi di interesse pubblico o per ragioni correlate alla sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi; ovvero il trattamento sia necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici; o ancora sia necessario in relazione all'esercizio del diritto di difesa o per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro, della sicurezza sociale e protezione sociale[21].

In ambito nazionale, l'art. 2 *septies* del D.lgs. 101/2018 attua l'art. 9, par. 4 del Regolamento, prevedendo che il trattamento dei dati biometrici, genetici e relativi alla salute sia subordinato all'osservanza di misure di garanzia, stabilite dal Garante con provvedimento adottato con cadenza almeno biennale, a seguito di consultazione pubblica, tenendo in particolare considerazione, oltre alle linee guida, raccomandazioni e migliori prassi pubblicate dal Comitato europeo per la protezione dei dati, anche l'evoluzione tecnologica e scientifica del settore a cui tali misure sono rivolte, nonché l'interesse alla libera circolazione dei dati nel territorio europeo.

Nel quadro degli obblighi generali incombenti sul titolare del trattamento *ex* art. 24, e delle misure di sicurezza adottabili *ex* art. 32 del Regolamento – letti in un'ottica di responsabilizzazione (o *accountability*) dello stesso, oltre che in funzione di protezione dei dati personali[22] – il livello di misure dovrà essere in questi casi molto elevato, trattandosi di trattamento che riguarda dati personali «particolarmente sensibili sotto il profilo dei diritti e delle libertà fondamentali, dal momento che il contesto del loro trattamento potrebbe creare rischi significativi per i diritti e le libertà fondamentali» (Cfr. considerando 51).

Posto che nell'odierna società dell'informazione basata sui *Big Data* emerge una sostanziale difficoltà nell'individuare l'*an*, il *quando* e il *quomodo* (inteso in termini di

[20] In tema di riconoscimento facciale, cfr. Considerando 51 GDPR.

[21] Sebbene non si riscontrino indicazioni in tal senso all'interno del Regolamento l'Autorità garante ha escluso esplicitamente che i dati biometrici possano essere trattati sulla base del legittimo interesse del titolare**.** Cfr. Garante, provvedimento del 22 febbraio 2018, recante «Indicazioni preliminari di cui in motivazione volte a favorire la corretta applicazione delle disposizioni del Regolamento (UE) 2016/679)».

[22] F. Mollo, *Gli obblighi previsti in funzione di protezione dei dati personali*, in Zorzi Galgano (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Wolters Kluwer Italia, 2019, 255.

 ISSN 2612-6672 | DOI 10.54103/2612-6672/22173

finalità) dei singoli concreti trattamenti cui i dati vengono sottoposti, il legislatore europeo della *privacy* mostra ampia consapevolezza delle proporzioni massive assunte negli ultimi decenni dal fenomeno circolatorio dei dati, avendo ben presente che «la portata della condivisione e della raccolta di dati personali è aumentata in modo significativo», e ha reso «disponibili al pubblico su scala mondiale informazioni personali» (considerando 6), che consentono di effettuare «trattamenti su larga scala, che mirano al trattamento di una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che potrebbero incidere su un vasto numero di interessati e che potenzialmente presentano un rischio elevato […] per i diritti e le libertà degli interessati, specialmente qualora tali trattamenti rendano più difficoltoso, per gli interessati, l'esercizio dei propri diritti». (considerando 91), con particolare riferimento al monitoraggio del comportamento dell'interessato attraverso tecniche di trattamento che ne consentano l'analisi, anche in termini predittivi, sotto il profilo delle preferenze, usi comportamentali o posizioni personali (considerando 24 e 71).

In tale contesto, assumono centrale rilevanza e maggiore complessità, in particolare, i profili di tutela dei diritti e delle libertà degli interessati sotto il profilo del trattamento di dati su larga scala di categorie di dati personali, tra cui i dati qui in commento. Ad essi si riferisce la previsione che rende obbligatoria la valutazione d'impatto[23] sulla protezione dei dati contenuta nella lett. *b)* dell'art. 35 del Regolamento, con formulazione peraltro speculare rispetto a quella adottata dalla dir. UE 2016/680, e ulteriormente specificata dal provvedimento adottato dal Garante per la protezione dei dati nell'ottobre 2018[24].

Con specifico riferimento ai dati biometrici, già oggetto di particolare attenzione del Garante per la protezione dei dati personali vigente la normativa precedente[25], occorre qui sottolineare come siano necessarie misure di garanzia specifiche. *Medio tempore*, l'art. 22 co. 11 del D.lgs. 101/2018 sembra suggerire la possibilità di continuare ad utilizzare i dati biometrici in conformità alle linee guida sulla biometria adottate nel 2014, adattando la base giuridica a quella indicata dal Regolamento[26].

3. *Segue. La tutela dei dati biometrici nella prospettiva nazionale ed europea*

Va qui detto come l'atteggiamento del Garante per la protezione dei dati personali sia particolarmente restrittivo nel ritenere necessaria una valutazione di insieme per evitare

---

[23] Sulla valutazione di impatto si veda R. Torino, *La valutazione d'impatto*, in V. Cuffaro, R. D'Orazio e V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, Giappichelli, 2019, 855.

[24] Cfr. Garante, doc. web n. 9058979 dell'11 ottobre 2018, contenente l'elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, par. 4 GDPR. Cfr. anche *European Data Protection Board, Opinion 12/2018 on the draft list of the competent supervisory authority of Italy regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR)*, adottata il 25 settembre 2018.

[25] Garante, provvedimento generale prescrittivo in tema di biometria del 12 novembre 2014 e relativo allegato A recante linee guida in materia di riconoscimento biometrico e firma grafometrica.

[26] L'articolo sopra richiamato, infatti, prevede espressamente che per il trattamento dei dati biometrici e genetici, le norme esistenti continuano a trovare applicazione in quanto compatibili, sino all'adozione delle misure di garanzia da parte del Garante. Si tenga altresì presente che, più in generale sul punto, sebbene non si riscontrino indicazioni in tal senso all'interno del Regolamento, l'Autorità italiana ha escluso esplicitamente che i dati biometrici possano essere trattati sulla base del legittimo interesse del titolare. Cfr. Provvedimento 22 febbraio 2018, recante indicazioni preliminari di cui in motivazione volte a favorire la corretta applicazione delle disposizioni del Regolamento (UE) 2016/679.

 ISSN 2612-6672 | DOI 10.54103/2612-6672/22173

che «singole iniziative aventi ad oggetto il trattamento di dati particolari come quelli biometrici, sommate fra loro, definendo un nuovo modello di sorveglianza, introducano di fatto un cambiamento non reversibile nel rapporto tra individuo ed autorità»[27].

L'attività provvedimentale dell'Autorità garante sul punto tiene conto proprio di queste premesse e considerazioni.

Già nel febbraio del 2020 l'Autorità aveva avuto modo di pronunciarsi[28] sull'utilizzo di dispositivi di video sorveglianza tramite riconoscimento biometrico in tempo reale adottati dagli enti locali, vietando, nello specifico, con parere adottato nei confronti del Comune di Como, prima amministrazione che intendeva fare ricorso a questa tipologia di sistema di IA. Secondo l'Autorità, la raccolta di dati biometrici – funzionale in particolare all'identificazione dei soggetti interessati nei soli casi nei quali emergano specifiche esigenze investigative, segnatamente ai sensi dell'art. 349 c.p.p. – può effettuarsi solo in presenza di un'idonea previsione normativa ai sensi dell'art. 7 d.lgs. n. 51/2018, che non pareva rinvenibile nel caso concreto.

Orientamento in linea con le posizioni coeve assunte delle Autorità nazionali di altri paesi, ad esempio in Spagna l'*Agencia Española de Protección de Datos* (AEPD) ha tratteggiato nel parere N/REF 010308/2019 i limiti dei trattamenti legati all'utilizzo di tecniche di riconoscimento facciale, atteso che «l'esistenza di un interesse pubblico non legittima alcun tipo di trattamento dati personali, ma devono essere, prima di tutto, presidiati da una norma di legge in combinato con i principi di limitazione delle finalità e minimizzazione dei dati». In Francia, la normativa di riferimento in materia di utilizzo di dispositivi per il riconoscimento facciale è contenuta, oltre che nel GDPR, nella Legge di Informatica e Libertà, che esordisce all'art. 1 con una dichiarazione di principio che ricorda la formulazione del considerando 4 del GDPR: «La tecnologia dell'informazione deve essere al servizio di ogni cittadino. […] Non deve attentare né all'identità umana, ai diritti umani, alla privacy o alle libertà individuali o pubbliche». In questo contesto, la *Commission Nationale de l'Informatique et des Libertés* (CNIL) ha dato atto in via formale con un paper[29] del 15 novembre 2019 che il riconoscimento facciale è sempre più presente nel dibattito pubblico a livello nazionale, europea e globale e solleva anzi nuove questioni relative a scelta della società, pronunciandosi in più occasioni in senso restrittivo su trattamenti di dati biometrici (nella fattispecie, riconoscimento facciale in due scuole superiori[30] e sistemi di videosorveglianza intelligente utilizzati da gestori di mezzi pubblici di linea a fini di prevenzione sanitaria nella gestione della pandemia da Sars-Cov-2)[31].

---

[27] Parere Garante per la protezione dei dati personali sul sistema Sari Real Time, n. 127 del 25 marzo 2021.
[28] Garante per la protezione dei dati personali, provvedimento del 26 febbraio 2020, doc. web n. 9309458.
[29] CNIL, *Reconnaissance faciale pour un debat à la hauteur des enjeux.*
[30] CNIL, *réunis en séance plénière le 17 octobre* 2019, provvedimento consultabile nel sito istituzionale dell'Autorità (www.cnil.fr).
[31] *Décret n° 2021-269 du 10 mars 2021 relatif au recours à la vidéo intelligente pour mesurer le taux de port de masque dans les transports.*

 ISSN 2612-6672 | DOI 10.54103/2612-6672/22173

Provvedimenti non dissimili emanati dalle rispettive Autorità garanti, sono rinvenibili anche in Olanda[32], Svezia e Danimarca[33].

Tornando, per quanto qui di interesse, all'attività provvedimentale del Garante italiano, è poi opportuno qui richiamare la posizione assunta con riferimento al sistema *Sari real time*[34], basato su una tecnologia di riconoscimento facciale in grado di coadiuvare le forze di polizia nella gestione dell'ordine e della sicurezza pubblica, oppure in relazione a specifiche esigenze di polizia giudiziaria, il Garante, con provvedimento del 25 marzo 2021, ha reso un parere negativo, dimostrando anzi una spiccata preoccupazione in ordine all'«evoluzione della natura stessa dell'attività di sorveglianza, passando dalla sorveglianza mirata di alcuni individui alla possibilità di sorveglianza universale allo scopo di identificare alcuni individui».

In particolare, richiamando gli articoli 8 CEDU, nonché 7, 8 e 52 CDFUE, l'Autorità ha ritenuto allo stato non sussistente una base giuridica idonea a consentire il trattamento dei dati biometrici nel caso concreto, fondato su un algoritmo di riconoscimento facciale che consente di analizzare in tempo reale i volti dei soggetti ripresi confrontandole con una banca dati predefinita per lo specifico servizio denominata "*watch-list*"[35].

Ancora più di recente, l'Autorità garante ha adottato un interessante provvedimento in tema di trattamento dati biometrici[36], con cui ha comminato una sanzione particolarmente elevata a *Clearview AI Inc*., in ragione dell'assenza di una base giuridica del trattamento di immagini, avvenuto senza il consenso e il mancato riscontro alle richieste degli interessati, specificatamente sull'accesso ai dati. Alla prima richiesta di informazioni dell'Autorità la società rispondeva di non effettuare il monitoraggio degli interessati all'interno dell'Unione secondo quanto stabilito dall'articolo 3, par. 2, lett. b) GDPR, in

---

[32] L'Autorità garante olandese (AP) è intervenuta, ad esempio, il 29 ottobre 2019, con una nota formale (reperibile nel sito istituzionale https://autoriteitpersoonsgegevens.nl/) di fronte dell'uso indiscriminato da parte di aziende di vendita al dettaglio, sicurezza, sport e intrattenimento, trasporti dei dispositivi di riconoscimento facciale.

[33] La DPA svedese ha esaminato il caso di una scuola comunale che ha condotto un progetto pilota di riconoscimento facciale per tenere traccia della frequenza scolastica degli studenti irrogando una sanzione di 200.000 SEK per la violazione le norme del GDPR, avendo la scuola ha elaborato dati biometrici sensibili illegittimamente e non essendo riuscita a eseguire un'adeguata valutazione dell'impatto, compresa la consultazione preventiva con il DPA svedese. La scuola ha basato il trattamento sul consenso, ma il DPA svedese ritiene che il consenso non fosse una base giuridica valida dato il chiaro squilibrio tra l'interessato e il responsabile del trattamento.
Un altro paese scandinavo ha però valutato l'impatto dell'IA in maniera diversa riguardo l'utilizzo dei dispositivi di riconoscimento facciale, dando un vero e proprio via libera all'installazione di telecamere intelligenti all'interno dello stadio di cui è proprietaria la squadra di calcio professionista di serie A del Broendby. Si tratta di un provvedimento che ha autorizzato un privato a dotarsi di un sistema di IA per finalità di interesse pubblico finalizzate ad impedire l'accesso allo stadio a una lista di tifosi che avevano ricevuto in passato un provvedimento amministrativo o giudiziale di ammonizione per fatti violenti. Il parere reso dall'Autorità garante ha però delimitato un perimetro preciso entro cui effettuare tale trattamento, quali l'obbligo di non conservare i dati biometrici di chi accede allo stadio, obbligo di cancellazione post-partita di tutti i dati residuali, obbligo di segnaletica *ad hoc*, conservazione dei dati temporanei in un server protetto da algoritmi crittografati, autenticazione a due fattori e divieto di accesso ai server da remoto.

[34] Provvedimento del Garante n. 127 del 25 marzo 2021, doc. web numero 9575877.

[35] Cfr. anche provvedimento n. 54 del 26 febbraio 2020, reperibile sul sito istituzionale dell'autorità, doc. web numero 9309458.

[36] Garante per la protezione dei dati personali, *Ordinanza ingiunzione nei confronti di Clearview AI - 10 febbraio 2022*, doc. web 9751362.

 ISSN 2612-6672 | DOI 10.54103/2612-6672/22173

quanto lo stesso presuppone un'osservazione che sia continua e perdurante nel tempo, mentre il servizio in questione non offre la possibilità di monitorare e tracciare le persone nel tempo, ma offre esclusivamente la funzionalità di ricerca delle immagini, come un semplice motore di ricerca, offrendo un'istantanea dei risultati.

Ponendosi l'attività predetta quale «mera raccolta di dati», le conclusioni che vengono tratte dalla ricerca sarebbero quindi, nell'ottica della convenuta, il risultato dell'operato delle forze dell'ordine che, grazie ai risultati forniti dal servizio, conducono ulteriori indagini investigative, condotte dagli organi inquirenti (e non dal software; quindi, non si potrebbe ritenere che si tratti di un monitoraggio attraverso mezzi automatizzati)[37].

Il Garante, con riferimento all'attività di monitoraggio, ritiene che il servizio offerto da *Clearview* non sia sovrapponibile a quello di un motore di ricerca, in quanto consistente in un'operazione di rielaborazione delle immagini per ricavarne dati biometrici al fine di effettuare la comparazione tra immagini; le informazioni relative alle immagini vengono altresì arricchite nel tempo grazie alle ulteriori immagini che vengono aggiunte, così da evidenziare altresì i cambiamenti degli individui nel corso del tempo. L'attività svolta da *Clearview* consiste, quindi, nella classificazione degli individui, ma anche nell'estrazione dei dati biometrici e nell'acquisizione di informazioni ulteriori riguardanti gli interessati.

E proprio con riferimento all'utilizzo di database privati di riconoscimento facciale da parte delle autorità di contrasto e dei servizi di *intelligence*, come *Clearview* (ivi esplicitamente richiamato), il Parlamento europeo ha espresso «profonda preoccupazione» nella risoluzione del 6 ottobre 2021[38].

In effetti, e in estrema sintesi, tre sono i punti che vengono in rilievo nella stessa: in primo luogo, l'invito alla Commissione ad «interrompere il finanziamento della ricerca o diffusione della biometrica o di programmi che potrebbero portare alla sorveglianza di massa indiscriminata nei luoghi pubblici» (punto 31); in secondo luogo il rilievo dei profili di criticità del trattamento di dati genetici e DNA (punto 29); nonché una presa di posizione netta a favore del divieto di qualsiasi sistema di *scoring* su larga scala di cittadini, sulla considerazione che «qualsiasi forma di "*citizen scoring*" normativo sul larga scala da parte delle autorità pubbliche […] conduce alla perdita di autonomia, indebolisce il principio di non discriminazione e non può essere considerato conforme ai diritti fondamentali, in particolare la dignità umana» (punto 32).

Facendo leva sul principio di finalità, il Parlamento raccomanda un controllo democratico rigoroso e una supervisione indipendente per qualunque tecnologia basata su intelligenza artificiale che venga utilizzata da parte delle autorità di contrasto e giudiziaria, in particolare se destinata alla sorveglianza e alla profilazione di massa; prende atto con grande preoccupazione del potenziale di determinate tecnologie

[37] In riferimento alla profilazione richiama le linee guida del Gruppo di lavoro Articolo 29, Linee guida sul Processo decisionale individuale automatizzato e Profilazione ai fini del Regolamento 2016/679 (wp251rev.01), in cui vengono elencate le fasi attraverso le quali si esplica l'attività di profilazione: raccolta dei dati; analisi automatizzata per ricercare le correlazioni; applicazione delle correlazioni emerse per predire i comportamenti futuri. La società ritiene che, anche se le prime due fasi sono presenti nell'attività svolta da Clearview, l'ultima non sarebbe presente, in quanto se anche fossero individuate delle caratteristiche future, sarebbe ascrivibile ad un comportamento del cliente del servizio, da qualificarsi quale titolare del trattamento.

[38] Risoluzione del Parlamento europeo del 6 ottobre 2021 sull'intelligenza artificiale nel diritto penale e il suo utilizzo da parte delle autorità di polizia giudiziaria in ambito penale 2020/2016 (INI).

 ISSN 2612-6672 | DOI 10.54103/2612-6672/22173

impiegate in tali settori per la sorveglianza di massa e sottolinea altresì «l'esigenza giuridica di prevenire la sorveglianza di massa tramite le tecnologie di IA, che per definizione non corrisponde ai principi di necessità e proporzionalità, e di vietare l'uso delle applicazioni che potrebbero risultare in tale sorveglianza»[39].

Sulla base di queste premesse e preso atto dei diversi tipi di utilizzo di riconoscimento facciale a fini di sorveglianza, il Parlamento chiede il «divieto permanente dell'utilizzo dei sistemi di analisi o riconoscimento automatico degli spazi pubblici di altre caratteristiche umane quali l'andatura, le impronte digitali, il DNA, la voce e altri segnali biometrici e comportamentali»; nonché una moratoria sulla diffusione di sistemi di riconoscimento facciale per le attività di contrasto con funzioni di identificazione, a meno che queste non siano usate strettamente a fini di identificazione delle vittime dei reati, almeno finché le norme tecniche non si potranno considerare «pienamente conformi con i diritti fondamentali» (punti 25, 26 e 27).

Una lettura, quindi, che esprime forte preoccupazione per la deriva che alcuni meccanismi, più o meno velatamente, di sorveglianza di massa, rischiano di prendere nell'odierna società informazionale e digitale.

4. *Il tema della sorveglianza connessa al controllo dei dati nella giurisprudenza della Corte europea dei diritti dell'uomo*

Il tema della sorveglianza ricollegata al controllo dei dati si rivela una preoccupazione da sempre ricorrente della giurisprudenza, anticipando una preoccupazione che rimarrà ricorrente nella giurisprudenza della Corte europea dei diritti dell'uomo.

Già nel 1983, infatti, la Corte costituzionale tedesca, in una storica pronuncia in materia di autodeterminazione informativa, aveva fondato il proprio sindacato di costituzionalità, incentrato sul valore della dignità dell'uomo, proprio sulla necessità di «impedire un passo importante, forse decisivo, per la trasformazione della Germania federale in uno stato di sorveglianza». Chiamata a pronunciarsi sulla costituzionalità di una legge sul censimento approvata dal Parlamento federale nel 1982, con una nota e importante decisione del 1983[40], aveva segnato un'evoluzione nella nozione di *privacy* e protezione dei dati personali, giungendo al riconoscimento un diritto all'autodeterminazione informativa (*informationelle Selbstbestimmungsrecht*) radicato nell'art. 2 comma 1, che sancisce il principio della libertà individuale, letto in combinato disposto con l'art. 1, comma 1 della *Grundgesetz* sulla dignità dell'uomo. Il ricorso al sindacato di costituzionalità veniva inteso come l'ultima possibilità per «porre un limite alla "fame di dati" dello Stato e impedire un passo importante, forse decisivo, per la trasformazione della Germania federale in uno "Stato di sorveglianza", trasformazione che avrebbe comportato la vanificazione di quelle garanzie che si riassumono nella formula "Stato di diritto"»[41]. Richiamando sul punto alcune proprie precedenti

[39] Sottolineando peraltro come l'approccio adottato da alcuni paesi terzi sotto il profilo delle tecnologie di sorveglianza di massa, interferendo in modo sproporzionato con i diritti fondamentali, non possa essere seguito dall'Unione europea (punto7).

[40] *Bundesverfassungsgericht*, sentenza del 15 dicembre 1983, in *Entscheidungen des Bundesverfassungsgerichts*, 1984, 65.

[41] G. Sartor, *Tutela della personalità e normativa per la «protezione dei dati». La sentenza della Corte costituzionale tedesca sul censimento del 1983 nel dibattito dottrinale sui profili costituzionalistici del «Datenschultz»*, in *Inf. e dir.*, 1986, 98.

 ISSN 2612-6672 | DOI 10.54103/2612-6672/22173

significative sentenze[42], la Corte riconosceva allora il diritto all'autodeterminazione sulle informazioni, inteso come la «facoltà del singolo di decidere essenzialmente da sé circa la cessione e l'uso dei propri dati personali», segnando con ciò un'importante evoluzione giurisprudenziale rispetto alla precedente cosiddetta «teoria delle sfere (*Sphärentheorie*)», fondata sull'assunto che l'intensità della tutela della persona dovesse essere inversamente proporzionale alla «socialità» del comportamento. La Corte afferma altresì che «non c'è nelle condizioni della moderna elaborazione dei dati alcun dato senza importanza, ha rilievo al fine di determinare il significato di un dato per il diritto della personalità, la conoscenza del suo contesto di utilizzo […] solo quando vi sia chiarezza sugli scopi per i quali dati sono stati richiesti, e sulle possibilità di connessione e di utilizzo che sussistano, è possibile rispondere alla domanda circa l'ammissibilità di una limitazione del diritto all' autodeterminazione informativa»[43].

Anche nella giurisprudenza della Corte di Strasburgo, il tema della sorveglianza ricorre con frequenza, riconnesso al rispetto della vita privata di cui all'art. 8 CEDU, messo in pericolo a più riprese da illegittime interferenze, su cui l'attenzione della Corte si rivela da sempre alta.

Fin dalla storica sentenza *Leander c. Finlandia* del 1987, in un caso di raccolta e memorizzazione di dati in un registro segreto di polizia, in cui però ancora non si fa alcun riferimento alla protezione dei dati personali, limitandosi la Corte a vagliare se tale memorizzazione costituisca un'ingerenza giustificabile alla luce del comma 2 dell'art. 8, e concludendo per un'assenza di violazione in tal senso. A poco più di un decennio di distanza, invece, nella sentenza *Rotaru c. Romania*, la Corte in un caso analogo di memorizzazione di dati relativi alla affiliazione politica e risalenti alla gioventù del soggetto interessato, con conseguente creazione di un dossier che lo riguardava, muta orientamento, assumendo a referente esterno di valutazione inerente la protezione dati personali (come accadrà poi in altre pronunce successive) la Convenzione del Consiglio d'Europa n. 108 del 1981, sottolineando «la rispondenza di un'interpretazione estensiva della nozione di vita privata e quella elaborata dalla Convenzione del 1981, il cui scopo è garantire il rispetto della vita privata con riferimento ai trattamenti automatizzati»[44].

Proprio valorizzando tale riferimento e il suo collegamento con l'art. 8 CEDU, la Corte afferma che anche dati pubblici possono rientrare nella sfera privata del soggetto se sistematicamente acquisiti, memorizzati e utilizzati dalle pubbliche autorità, per cui è ravvisabile un'ingerenza laddove vi siano tre condizioni, consistenti nella memorizzazione dei dati, nel loro utilizzo da parte dell'autorità, nonché nella

[42] Per una disamina di tali precedenti, si veda V. Roppo, *I diritti della personalità*, in G. Alpa e M. Bessone (a cura di), *Banche dati, telematica e diritti della persona*, Cedam, 1984, 73.

[43] *Bundesverfassungsgericht*, sentenza del 15 dicembre 1983, in *Entscheidungen des Bundesverfassungsgerichts*, 1984, 65, 45. A p. 43 si legge anche che «un ordinamento sociale ed un ordinamento giuridico […], nel quale i cittadini non potessero sapere da chi, come, quando, in quale occasione sono conosciute informazioni che ti riguardano, sarebbero incompatibili con il diritto all'autodeterminazione informativa. Chi è incerto se comportamenti devianti siano registrati, memorizzati durevolmente, utilizzati e trasmessi come informazione, sarà portato ad evitare quei comportamenti. Chi ritiene che la sua partecipazione ad una riunione o ad una iniziativa civica possa essere registrata dalle autorità e che da ciò possano derivare per lui dei rischi, rinuncerà forse ad esercitare i corrispondenti diritti fondamentali […]. Ciò pregiudicherebbe non solo le possibilità di realizzazione dell'individuo, ma anche l'interesse generale, in quanto l'autodeterminazione è una condizione elementare di una società libera e democratica [...]».

[44] Cfr. anche la sentenza della Corte EDU del 16 febbraio 2000, n. 27798/95, *Amann c. Svizzera*.

 ISSN 2612-6672 | DOI 10.54103/2612-6672/22173

impossibilità di confutare tali informazioni da parte dell'interessato. Tale ingerenza viene ritenuta non giustificabile dalla Corte alla luce del carattere generalizzato, indistinto e sistematico con cui le autorità trattano i dati *de quibus*, nell'assoluta assenza di criteri oggettivi di selezione e individuazione delle informazioni e dei soggetti, nonché di procedure e di meccanismi di controllo di tali operazioni, tali da implicare concretamente «il rischio di minare, persino distruggere, la democrazia per difenderla», creando di fatto un sistema di sorveglianza su base indiscriminata e generalizzata.

In tema, va registrata, peraltro, una vera e propria inversione di tendenza nell'atteggiamento della stessa Corte EDU. Nel 2010, infatti, nel caso *Kennedy c. Regno Unito*, la Corte, pronunciandosi sulla compatibilità con l'art. 8 CEDU di alcuni sistemi di captazione delle informazioni su base generalizzata e sistemica implementati dal Regno Unito, aveva rigettato la questione in assenza di allegazione da parte del ricorrente di una violazione specifica, assumendo e mantenendo quella prospettiva di *individual justice* che da sempre l'aveva contraddistinta.

Ma nel 2015, nel caso *Zakharov c. Russia*[45], tale interpretazione subisce una vera e propria battuta d'arresto, nella misura in cui viene riconosciuto, in accordo con le precedenti statuizioni in tema dei giudici di Lussemburgo, che la mancata allegazione di un pregiudizio o una conseguenza ricollegata al sistema di sorveglianza non costituisce un ostacolo per concludere sulla incompatibilità con l'art. 8 CEDU del sistema russo di captazione delle comunicazioni su base generalizzata e non ancorato a criteri oggettivi né a procedure di controllo specifiche.

Impostazione poi mantenuta nelle più recenti sentenze della Corte di Strasburgo in tema di sorveglianza di massa.

Ci si riferisce qui, anzitutto, alla sentenza del 5 marzo 2020, resa nel caso *ARM/Hambardzumyan* (ric. 43478/11), nonché, più di recente, con sentenza 8 marzo 2021, nel caso *MDA/Bostan (ric. 52507/09*), in relazione ad una perquisizione condotta dalla polizia presso l'abitazione del ricorrente nell'ambito di un procedimento per contravvenzione nei confronti di una terza persona, senza mandato o permesso giudiziario, contrariamente al diritto interno. E ancora, può farsi richiamo alla celebre sentenza del 25 maggio 2021 resa nel caso *UK./Big Brother Watch and Others* (ric. 58170/13). La questione riguardava alcune carenze nel regime di sorveglianza segreta, tra cui l'intercettazione di massa e l'ottenimento di dati sulle comunicazioni da fornitori di servizi di comunicazione nel Regno Unito prima del 2018, sotto il profilo della violazione degli articoli 8 e 10 CEDU.

Pur ritenendo che la Convenzione non proibisca l'uso dell'intercettazione in massa di per sé per proteggere gli interessi di sicurezza nazionale e altri interessi nazionali essenziali contro gravi minacce esterne, la Corte ha sottolineato la necessità di "salvaguardie *end-to-end*" e ha definito l'approccio da seguire in tali casi.

Ancora, la Corte EDU nel caso *SWE/Centrum for Rättvisa* (ric. 35252/08), con sentenza del 25 maggio 2021, in relazione al presunto rischio che le comunicazioni della fondazione ricorrente venissero intercettate ed esaminate tramite segnali di intelligence, in quanto comunicava quotidianamente con individui, organizzazioni e società in Svezia e all'estero via e-mail, telefono e fax, spesso su questioni delicate, ha rilevato, in particolare, che il regime delle intercettazioni in blocco presentava tre carenze.

[45] Corte EDU, sentenza del 4 dicembre 2015, *Roman Zakharov c. Russia*, n. 47143/06.

 ISSN 2612-6672 | DOI 10.54103/2612-6672/22173

In primo luogo, l'assenza di una norma chiara sulla distruzione del materiale intercettato che non conteneva dati personali; l'assenza di un requisito nel *Signals Intelligence Act* o in altra legislazione pertinente che, quando si decide di trasmettere materiale di intelligence a partner stranieri, si tenga conto degli interessi privati delle persone; e l'assenza di un effettivo riesame *ex post*. Di conseguenza, il sistema non soddisfaceva il requisito delle tutele "*end-to-end*", oltrepassava il margine di discrezionalità lasciato allo Stato convenuto al riguardo e, nel complesso, non metteva in guardia dal rischio di arbitrarietà e abusi[46].

5. *La questione della sorveglianza negli orientamenti della Corte di giustizia dell'Unione europea*

Nel contesto del circuito di dialogo tra le Corti europee in tema di diritti[47], la questione della sorveglianza[48] legata al controllo dei dati è affrontata anche dalla Corte di giustizia, in particolare, nella prima di quel trittico di sentenze[49] in materia di *privacy* e protezione dei dati personali, assunte tra il 2014 e il 2015, che hanno contribuito all'«emersione, sempre più prepotente, […], di un vero e proprio *digital right to privacy*»[50], poi confluito nel GDPR.

La Corte si è infatti occupata della circolazione dei dati personali nella «dimensione interna» nel noto caso *Digital Rights Ireland*, con sentenza, resa l'8 aprile 2014[51] , con

[46] Cfr. Report settembre 2022, *Personal data protection, Thematic factsheet, Department for the Execution of Judgments of the European Court*, consultabile al link https://www.coe.int/en/web/execution.

[47] Il tema è ampiamente studiato in dottrina. Nell'impossibilità di richiamare in maniera esaustiva la bibliografia inerente, ci si limita qui a rinviare a: P. Gianniti, *La CEDU e il ruolo delle Corti*, in *Commentario del Codice civile e codici collegati Scialoja- Branca- Galgano*, Zanichelli, 2015; R. Cosio e R. Foglia (a cura di), *Il diritto europeo nel dialogo delle Corti*, Giuffrè, 2013; A. Barbera, *Le tre Corti e la tutela multilivello dei diritti*, in P. Bilancia, E. De Marco (a cura di), *La tutela multilivello dei diritti*, Giuffrè, 2005; M. Cartabia, B. De Witte, P. Pérez Tremps (dirs.), I. Gómez Fernández (coord.), *Constitución europea y Constituciones nacionales*, Tirant lo Blanch, 2005; P. Grossi, *L'Europa del diritto*, Laterza, 2007; O. Pollicino e V. Sciarabba, *La Corte di Giustizia dell'Unione europea e la Corte europea dei diritti dell'uomo quali Corti costituzionali*, in L. Mezzetti (a cura di), *Sistemi e modelli di giustizia costituzionale*, Cedam, 2011, II; D. Tega, *I diritti in crisi. Tra Corti nazionali e Corte europea di Strasburgo*, Giuffrè, 2012. Più in generale, sul tema della equivalenza/comparabilità tra le tutele approntate in difesa dei diritti fondamentali a livello comunitario e della CEDU si vedano G. Zagrebelsky, *L'UE e il controllo esterno della protezione dei diritti e delle libertà fondamentali in Europa. La barriera elevata dalla Corte di Giustizia*, in *DUDI*, 2015, 1.

[48] Sul tema della sicurezza e della sorveglianza cfr G. Resta, *La sorveglianza elettronica di massa il conflitto regolatorio USA/UE*, in *Dir. inform.*, 4-5, 2015, 697; G. Buttarelli, *Privacy, sicurezza e nuove tecnologie al bivio di nuove scelte strategiche*, in *Federalismi.it*, 2015. Si vedano anche G. De Vergottini, *Guerra e Costituzione*, il Mulino, 2004; Id., *Il bilanciamento tra sicurezza e libertà civili nella stagione del terrorismo*, in Aa.Vv. (a cura di), *Sicurezza: le nuove frontiere*, 2005, 110; T. Giupponi, *Contro il "diritto alla sicurezza". Immigrazione, sicurezza e autonomie territoriali nella più recente giurisprudenza della Corte costituzionale*, in Aa.Vv. (a cura di), *Studi in onore di Giuseppe de Vergottini*, Cedam - Wolters Kluwer Italia, 2015, I, 719.

[49] Cfr. O. Pollicino e M. Bassini, *La Carta dei diritti fondamentali dell'Unione europea nel reasoning dei giudici di Lussemburgo*, in *Dir. inform.*, 2015.

[50] O. Pollicino, *Un digital right to privacy preso (troppo) sul serio dai giudici di Lussemburgo? Il ruolo degli artt. 7 e 8 della Carta di Nizza nel reasoning di Google Spain*, in *Dir. inform.*, 2014, 7.

[51] Per alcuni commenti, L. Trucco, *Data retention*: *la Corte di giustizia si appella alla Carta UE dei diritti fondamentali*, in *Giur. it.*, 8-9, 2014, 1850; F. Fabbrini, *The European Court of justice Ruling in the Data*

 ISSN 2612-6672 | DOI 10.54103/2612-6672/22173

riferimento al regime di conservazione dei dati previsto dalla dir. 2006/24/CE, riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione.

In particolare la Corte esordisce con la constatazione che l'obbligo di conservazione dei dati contenuto nella disciplina solleva questioni relative alla protezione della vita privata, in considerazione del fatto che i dati conservati, considerati nel loro complesso, sono suscettibili di consentire di «trarre conclusioni molto precise riguardo la vita privata delle persone», permettendo, in ultima analisi di tracciare un quadro completo e fedele dell'identità individuale e relazionale della persona, quale essa si esplica nell'ambito della propria vita privata[52].

La Corte, pertanto, ravvisa nel sistema approntato dalla direttiva un'ingerenza «di vasta portata e [...] e particolarmente grave»[53] nei diritti fondamentali sanciti dagli artt. 7 e 8 della Carta, sottolineando come l'obbligo di conservazione dei dati costituisca di per sé un'interferenza nel diritto al rispetto della vita privata, mentre l'accesso costituisca «un'ingerenza supplementare in tale diritto fondamentale», richiamando significativamente sul punto la giurisprudenza della Corte EDU sull' art. 8 CEDU[54] in tema di memorizzazione di dati a fini di creazione di dossier. E ciò indipendentemente dal carattere sensibile dell'informazione o degli eventuali inconvenienti o pregiudizi subiti dagli interessati a seguito di tale ingerenza, finendo per ingenerare nelle persone interessate «la sensazione che la loro vita privata sia oggetto di costante sorveglianza», amplificata peraltro dal fatto che tale conservazione e utilizzo ulteriore possono essere effettuati senza che l'utente ne sia neppure informato[55].

Sottolinea in primo luogo come la conservazione, pur costituendo un'ingerenza particolarmente grave in tali diritti, non permettendo di venire a conoscenza del contenuto delle comunicazioni elettroniche in quanto tale, «non è tale da pregiudicare il [...] contenuto» essenziale del diritto al rispetto della vita privata, così come non è idonea di per sé a pregiudicare neppure il contenuto dell'art. 8. D'altra parte, le limitazioni contenute nella direttiva rispondono indubbiamente, nel ragionamento della Corte, all'obiettivo di interesse generale della lotta contro la criminalità atteso che «l'art. 6 della Carta enuncia il diritto di ogni persona non solo alla libertà, ma altresì alla sicurezza».

Giungendo poi al vaglio di proporzionalità dell'ingerenza constatata, la Corte si sofferma su tre profili: la mancanza generale di limiti alla conservazione dei dati nella

---

Retention Case and its Lessons for Privacy and Surveillance in the U.S., in *Harvard Human Rights J.*, 28, 2015, 65.

[52] Analoghe considerazioni si ritrovano anche nella giurisprudenza costituzionale tedesca. Cfr. *BverfG*, 2 marzo 2010, I, Bvr 256/08, 1 BvR 263/08, 1 BvR 586/08., in cui la Corte costituzionale tedesca, nel dichiarare l'incostituzionalità della normativa tedesca di recepimento della Direttiva del 2006 per contrasto con l'art. 10.1 del *Grundgesetz*, ha considerato particolarmente grave l'ingerenza prodotta dalla sorveglianza delle comunicazioni nella vita privata degli utenti intercettate, perché le relazioni sociali di ciascuno sarebbero potute essere agevolmente ricostruite, proprio muovendo dai dati personali sul traffico telematico o telefonico.

[53] Cfr. par. 37 della sentenza.

[54] Corte EDU, sentenze *Leander c. Svezia* 26 marzo 1987, nonché *Rotaru c. Romania* n. 28341/1995, e *Weber e Saravia c. Germania*, n. 54934/00, richiamate al punto 35 della sentenza.

[55] Sullo sfondo di questa vicenda, e più in generale degli sforzi recente della Corte di giustizia, si colloca proprio la problematica della sorveglianza globale. Cfr. anche Rossi Dal Pozzo, *Protezione dei dati personali e diritti fondamentali della persona: le nuove norme sui "codici di prenotazione" (PNR)*, in *Riv. dir. int. priv. proc.*, 4, 2016, 1020.

 ISSN 2612-6672 | DOI 10.54103/2612-6672/22173

dir. 2006/24/CE, l'assenza di alcun criterio oggettivo che permetta di delimitare l'accesso a tali dati da parte delle autorità nazionali, nonché la durata stessa della conservazione.

Sulla base della valutazione di questi tre profili, la Corte conclude che «adottando la dir. 2006/24/CE, il legislatore dell'Unione ha ecceduto i limiti imposti dal principio di proporzionalità alla luce degli artt. 7, 8, 52 par. 1 della Carta», dal momento che la stessa da un lato non prevede norme chiare e precise che regolino la portata dell'ingerenza nei diritti fondamentali in questione, tali da garantire che essa sia effettivamente limitata a quanto strettamente necessario; né prevede garanzie sufficienti che consentano una protezione efficace dei dati contro i rischi di abusi, accessi ovvero utilizzi illeciti degli stessi.

Sulla scorta delle stesse premesse, poi, la Corte di giustizia è intervenuta pure successivamente, ancora una volta, nella propria affermazione quale «giudice dei diritti» che contribuisce a fondare l'Unione europea come «ordinamento a protezione avanzata»[56], nel dicembre 2016[57], a istituire un solido collegamento tra riservatezza e comunicazioni elettroniche, affermando che «la Direttiva 2002/58/CE , relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche, interpretata alla luce degli artt. 7, 8 e 11 nonché dell'art. 52, par. 1, CDFUE osta a una normativa nazionale che: *a*) preveda una conservazione generalizzata e indifferenziata dell'insieme dei dati relativi al traffico e all'ubicazione di tutti gli utenti; *b*) non limiti l'accesso delle autorità nazionali competenti alla sola lotta contro la criminalità grave e non ne sottoponga l'esercizio al controllo preventivo di un giudice o di un'autorità amministrativa indipendente; *c*) non richieda che i suddetti dati siano conservati nel territorio dell'Unione».

Sul punto, la segnalata inversione di tendenza in tema di intercettazioni nella giurisprudenza della Corte europea dei diritti dell'uomo[58] appare successiva e correlata proprio alla giurisprudenza della Corte di giustizia, segnatamente al caso *Digital Right Ireland*, ma ancor di più al successivo caso *Schrems*[59], in cui la Corte ripropone le medesime argomentazioni fornite nel primo caso nel bilanciamento tra esigenze di sicurezza e protezione dei dati personali nella dimensione esterna della loro circolazione (flusso transfrontaliero con gli USA).

Proprio la sentenza *Schrems* – e la successiva *Schrems II*[60] – si iscrivono in un filone di giurisprudenza che, assieme ai crescenti interventi per la regolazione delle reti e alle operazioni di sorveglianza così condotte, rivela il collegamento con la contesa fra «due super-potenze internazionali [...] per il controllo di una risorsa essenziale quale le reti globali di telecomunicazioni». In tale contesto, lo strumento impiegato dall'Unione europea è stato proprio una regolazione fortemente territoriale con effetti indirettamente (ma programmaticamente) ultraterritoriali. In linea con tale impostazione, la Corte UE si

[56] Cfr. B. Carotti, *La Corte di Giustizia costruisce un ponte tra riservatezza e comunicazioni elettroniche*, in *Giorn. dir. amm.*, 4, 2017, 479, che valorizza l'immagine di un «ponte» tra le due, nell'ambito dell'Unione quale ordinamento dotato di strumenti di protezione rafforzata.
[57] Corte UE, 21 dicembre 2016, C-03/15 e C-698/15, *Tele2SverigeAB c. Post-och Telestyrelsen, e Secretary of State for the Home Department c. Tom Watson et al.*
[58] V. *supra*, par. 4.
[59] Tanto da essere definita il c.d. «*follow up*» di Schrems. Cfr. O. Pollicino e M. Bassini, *La Carta dei diritti fondamentali dell'Unione europea nel reasoning dei giudici di Lussemburgo*, cit., 101.
[60] Corte di giustizia dell'Unione europea, 16 luglio 2020, causa C-311/18.

 ISSN 2612-6672 | DOI 10.54103/2612-6672/22173

erge nei casi sopracitati a strenua difesa dei diritti fondamentali per proclamare la c.d. «sovranità digitale» dell'Unione[61].

Anche più di recente, la Corte ha assunto la stessa posizione nel caso *Ligue des droits humains*[62], in cui è stata chiamata a pronunciarsi, tra l'altro, circa la validità della direttiva PNR alla luce dei diritti fondamentali sanciti dagli artt. 7 e 8 della Carta, nonché dell'art. 52, par. 1, della stessa. In tale occasione, si è soffermata in particolare sul rispetto del principio di proporzionalità e sul carattere necessario delle ingerenze risultati dalla direttiva 2016/681 sull'uso dei dati del codice di prenotazione (PNR), in relazione ai diritti fondamentali citati, giungendo alla conclusione che il trasferimento, il trattamento e la conservazione dei dati PNR previsti da tale direttiva possono essere considerati come limitati allo stretto necessario ai fini della lotta contro i reati di terrorismo e i reati gravi, a condizione che i poteri previsti da detta direttiva siano interpretati secondo quanto statuito dalla Corte di giustizia stessa.

6. *Conclusioni*

Si è dunque visto come l'utilizzo di tecniche di riconoscimento biometrico sia suscettibile di configurare una delle tappe verso la società della sorveglianza, proprio quella degenerazione della società dell'eguaglianza e della partecipazione guardata con sospetto dalla Corte europea dei diritti dell'uomo, dalla Corte di giustizia dell'Unione europea, così come dai Garanti (a livello nazionale ed europeo).

Come efficacemente sottolineato[63], «il capitalismo della sorveglianza si appropria dell'esperienza umana usandola come materia prima da trasformare in dati sui comportamenti», utilizzando alcuni dati quale «surplus comportamentale privato», sottoposto a processi governati dall'intelligenza artificiale per essere trasformato in

---

[61] V. Zeno-Zencovich, *Intorno alla decisione nel caso Schrems: la sovranità digitale e il governo internazionale delle reti di telecomunicazione*, in G. Resta e V. Zeno-Zencovich (a cura di), *La protezione transnazionale dei dati personali. Dai "Safe Harbour Principles" al "Privacy Shield"*, 7-9. Cfr. Anche G. Resta, F. Simonetti, *La c.d. sovranità digitale e il progetto Gaia-X*, in *Contr. e impr./Europa*, 3, 2022, 479.

[62] Corte di giustizia (Grande Sezione), sent. 21 giugno 2022, *Ligue des droits humains*, causa C-817/19, ECLI:EU:C:2022:491, in cui la Corte è stata chiamata a pronunciarsi in via pregiudiziale rispetto a molteplici questioni sollevate dalla Corte costituzionale belga, giudice del rinvio, adita a livello nazionale, a seguito di ricorso presentato dall'associazione Ligue des droits humains contro il Consiglio dei Ministri del Belgio, avente ad oggetto l'annullamento totale o parziale della legge belga del 25 dicembre 2016, che disciplina il trattamento dei dati dei passeggeri. In particolare, tale normativa dava attuazione, nel diritto interno, alla direttiva 2016/681 sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi e alla direttiva 2004/82 concernente l'obbligo dei vettori di comunicare i dati relativi alle persone trasportate (direttiva API), nonché in parte alla direttiva 2010/65 relativa alle formalità di dichiarazione delle navi in arrivo o in partenza da porti degli Stati membri. La disciplina contenuta in tale normativa prevedeva, tra l'altro, un obbligo, in diversi settori del trasporto internazionale di persone e in capo agli operatori di viaggio, di trasmettere i dati dei rispettivi passeggeri a una banca dati gestita dal Servizio federale pubblico dell'interno del Belgio. Secondo il legislatore nazionale, la finalità di tale legge rientrava quindi in tre categorie: in primo luogo, la prevenzione, l'indagine, l'accertamento o il perseguimento di reati o l'esecuzione di sanzioni penali, in secondo luogo, i compiti dei servizi segreti e di sicurezza e, in terzo luogo, il miglioramento dei controlli alle frontiere esterne e il contrasto all'immigrazione irregolare.

[63] S. Zuboff, *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*, II ed., Luiss University Press, 2023.

 ISSN 2612-6672 | DOI 10.54103/2612-6672/22173

prodotti predittivi, destinati poi ad essere scambiati su un nuovo tipo di mercato per le previsioni comportamentali, definito quale «mercato dei comportamenti futuri».

Una visione della protezione dei dati personali, quale «precondizione per il pieno godimento di altri diritti fondamentali»[64], nonché «espressione particolarmente forte – quasi metonimica – della dignità personale, meta-valore riassuntivo dell'impianto assiologico sui cui si innestano le situazioni giuridiche costituzionalmente protette»[65] impone, dunque, un approccio *data driven*, non solo in funzione del miglioramento di diagnosi e cura nel quadro dell'impiego dei dati biometrici, ma proprio come approccio di processo che restituisca centralità alla persona, la cui identità viene in gioco sotto vari profili[66].

Proprio in un'ottica di tutela della persona, la prospettiva da adottare fa leva sul bilanciamento[67] tra i principi che di volta in volta vengano in conflitto, da sempre criterio che preserva da precipitosa realizzazione di un valore a scapito di altri e dall'estensione dei cosiddetti «diritti desiderio»[68]; bilanciamento[69] da condursi secondo ragione[70], avendo sempre come punto di riferimento la dignità della persona[71]. Del resto, fin dalla Direttiva 95/46/CE[72] l'impianto normativo si basava su un'esigenza di bilanciamento tra diritto alla protezione dei dati personali – nella visione dinamica di controllo sugli stessi – e libera circolazione dei dati, che costituiscono anime bilanciate anche nel Regolamento del 2016[73].

Ma vi è di più. Come recentemente sottolineato[74], «non può bastare limitarsi a dire che occorre un sistema regolatorio che metta l'uomo al centro, ma bisogna invece mettere lucidamente al centro la necessità di adottare regole che rendano comprensibili i programmi usati dalla (o dalle) IA, verificabili e sindacabili i dati usati per

---

[64] Cfr. G. Alpa, *Diritto privato europeo*, Giuffrè, 2016, 182; G. Buttarelli, *Banche dati e tutela della riservatezza*, Giuffrè, 1997.

[65] N. Lipari, *Diritto civile e ragione*, Giuffrè, 2019, 183.

[66] Sull'approccio del legislatore europeo nella regolazione dell'intelligenza artificiale, si veda G. Finocchiaro, *La regolazione dell'intelligenza artificiale*, in *Riv. trim. dir. pubbl.*, 4, 2022, 1085. Per una riflessione di più ampio respiro sulle principali direttrici giuridiche del mercato digitale, cfr. G. Finocchiaro, L. Balestra e M. Timoteo (a cura di), *Major Legal Trends in the Digital Economy*, il Mulino, 2022.

[67] Si vedano le sempre attuali riflessioni sulla prudenza nel bilanciamento di G. Zagrebelsky, *Il diritto mite*, Einaudi, 1992, 200.

[68] P. Gianniti, *Problematiche connesse alla tendenza espansiva dei diritti fondamentali*, in P. Gianniti (a cura di), *I diritti fondamentali nell'unione europea. La carta di Nizza dopo il trattato di Lisbona*, Zanichelli, 2013, 218.

[69] A. Morrone, voce *Bilanciamento (giustizia costituzionale)*, in *Enc. dir., Annali*, Giuffrè. 2008, vol. II, tomo II, 185-204.

[70] Cfr. P. Gianniti, *I diritti fondamentali nell'unione europea. La carta di Nizza dopo il trattato di Lisbona*, cit., 223, in cui cita in proposito F. Galgano, *Democrazia politica e legge della ragione*, in *Contr. e impr.*, 2007, 393, nonché Id., *Globalizzazione dell'economia e universalità del diritto*, in *Pol. dir.*, 2009, 177.

[71] Cfr. anche Trib. Milano, 28 settembre 2016, in *Foro it.*, 2016, I, 3594, con nota di R. Pardolesi che sottolinea come tale impostazione sia l'unica compatibile con il principio personalistico e con la visione della persona umana quale valore etico in sé.

[72] M. Bin, *Privacy e trattamento di dati personali: entriamo in Europa*, in *Contratto e impresa Europa*, 1997, 2, 459; più di recente V. Cuffaro, *Il diritto europeo sul trattamento dei dati*, in *Contratto e impresa*, 2018, 3, 1098.

[73] N. Zorzi Galgano, *Le due anime del GDPR e la tutela del diritto alla* privacy, in N. Zorzi Galgano (a cura di) *Persona e mercato dei dati. Riflessioni sul GDPR* , Wolters Kluwer Italia, 2019, 255.

[74] F. Pizzetti, *Con AI Verso la Società digitale*, in *Federalismi.it*, 23, 2023.

 ISSN 2612-6672 | DOI 10.54103/2612-6672/22173

l'addestramento di queste tecnologie», proprio in bilanciamento con la necessità di salvaguardare e rafforzare il mercato unico digitale europeo e la competizione globale.

In quest'ottica, sotto il profilo dell'impatto delle nuove tecnologie, rimane centrale il nodo dei sistemi costituzionali e della tutela diritti fondamentali che li caratterizzano, destinati anch'essi a dover fare i conti con una trasformazione di vastissima portata e oramai inarrestabile.

ISSN 2612-6672 | DOI 10.54103/2612-6672/22173