



Università degli Studi di Urbino Carlo Bo
Dipartimento di Giurisprudenza (DiGiur)

Licia Califano, Valentina Fiorillo, Federico Galli

La protezione dei dati personali: natura, garanzie e bilanciamento di un diritto fondamentale

Prefazione di Antonello Soro



Giappichelli

Parte I

LA NATURA DEL DIRITTO

Capitolo I

L'EVOLUZIONE NORMATIVA E GIURISPRUDENZIALE DEL DIRITTO ALLA PRIVACY

Sommario: 1. Il cittadino nell'era dei *big data*. – 2. L'attuazione e l'evoluzione della tutela della privacy quale diritto fondamentale di matrice europea: la dimensione della riservatezza; l'ampliamento alla protezione dei dati; la privacy nell'era del digitale. – 3. *Segue:* l'elaborazione giurisprudenziale del diritto alla privacy in Europa.

1. Il cittadino nell'era dei *big data*

Lo sviluppo tecnologico prosegue inarrestabile e, con esso, la progressiva affermazione della realtà digitale nella vita dell'uomo. Al fondo vi è la condivisibile convinzione di migliorare la vita di ciascuno di noi, aumentando la qualità e la quantità dei beni e dei servizi che ci vengono offerti quali utenti/consumatori.

Ma, se i vantaggi non possono certo essere negati, occorre al contempo capire e spiegare che il mondo, così profondamente mutato, non è esente da rischi che hanno inevitabilmente una ricaduta sulla vita delle persone, sui diritti e sulle libertà: rischi e pericoli di cui dobbiamo essere consapevoli.

Altrimenti detto, non sono in discussione i nuovi orizzonti di sviluppo che sistemi tecnologici capaci di interagire con l'uomo aprono al genere umano; sono piuttosto da considerare attentamente i profili di regolazione delle tecnologie digitali e del loro uso, affinché esso non diventi abuso, con inevitabili riflessi sull'idea stessa di democrazia.

Oggi la produzione, la memorizzazione e l'utilizzo delle dati, che noi stessi generiamo nel vissuto di una tecnologia digitale che sempre più ci accompagna nelle azioni quotidiane, avviene attraverso sistemi automatici a (apparente) costo zero che rendono disponibili le informazioni personali di una moltitudine di individui; informazioni che si prestano ad una infinità di utilizzi – aziendale, economico, sociale e, come vedremo, anche politico – e in molti settori che dal commercio via via si estendono al turismo, ai trasporti e che sempre più trovano spazi nel mondo della sicurezza e della sanità.

Più viviamo nella rete – sempre connessi – tanto più mostriamo la nostra vita quotidiana, le nostre abitudini e preferenze, rendendo così irrealizzabile e contraddittoria la pretesa di vedere rispettata e tutelata la nostra privacy come accadeva in passato.

La diffusione di *IoT*, delle tecnologie di *machine learning* e di intelligenza artificiale (IA) sta producendo una quantità di dati, personali e no, mai visti prima nella storia dell'uomo.

Questa quantità di dati e informazioni è ciò che oggi chiamiamo *big data*: banche dati di grandi dimensioni in cui le informazioni contenute vengono continuamente interconnesse e automaticamente rielaborate sulla base di complessi algoritmi, per dare vita a informazioni di secondo grado (*data mining*), riutilizzabili per altri fini.

Se anche volessimo ipotizzare che tali informazioni non consentono la re-identificazione degli interessati che avevano inizialmente ed inconsapevolmente fornito i dati grezzi¹, non-

¹ Questa ipotesi è stata peraltro sconfessata da numerosi studi che hanno dimostrato come le attuali tecniche di analisi dei dati aumentano le possibilità di re-identificazione di persone fisiche partendo da dati apparentemente anonimi, in quanto consentono di ricollegare i dati non identificati (compresi quelli anonimizzati o pseudonimizzati) ai soggetti interessati a cui tali dati fanno riferimento. Ad esempio, quando nel 2006 la piattaforma di contenuti *on-demand* Netflix ha reso pubblici una serie di dati anonimizzati contenenti le valutazioni di film rese da 500.000 utenti abbonati, uno studio ha dimostrato che un utente del servizio poteva essere facilmente identificato.

dimeno questo perfetto automatismo, basandosi su leggi probabilistiche, potrebbe condurre a categorizzazioni e classificazioni della società che, oltre ad essere discutibili sul piano dell'esattezza e della correttezza, portano con sé il rischio di generare pregiudizi e discriminazioni.

Non a caso si è sottolineato come non sia eccessivo affermare che le informazioni, oltre ad accompagnare e migliorare gli scambi economici e le transazioni tradizionali, diventano un fattore di produzione al pari della terra, del capitale e del lavoro².

L'applicazione di nuove modalità di calcolo e di analisi, le sempre maggiori capacità sia di raccolta che di conservazione e analisi di dati personali hanno completamente modificato il

Per ottenere questo risultato, lo studio aveva confrontato e collegato le valutazioni dei film degli utenti di Netflix anonimizzati con le recensioni disponibili pubblicamente sul sito di informazioni cinematografiche *Internet Movie Database* (IMDb), dove gli utenti spesso usano i loro veri nomi. Lo studio ha dimostrato che in media sono necessarie da due a otto recensioni su IMDb per identificare gli utenti nel dataset anonimizzato di Netflix. Uno studio più risalente condotto negli Stati Uniti aveva altresì dimostrato come la combinazione di codice postale, genere e data di nascita rappresentasse una combinazione unica per 216 su 248 milioni di cittadini statunitensi (87%) e quindi rendeva l'identificazione dell'oggetto persona fisica altamente probabile.

² Sul punto ampiamente F. BERNABÈ, *Libertà vigilata*, Editori Laterza, Roma-Bari, 2012. Più recentemente, S. ZUBOFF, *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*, Luiss University Press, Roma, 2020, che, rifacendosi alle teorie economiche di Karl Polanyi, individua nell'attuale conformazione dell'economia digitale un ulteriore stadio di penetrazione del mercato nello spazio sociale. In particolare, Polanyi aveva osservato che il capitalismo trasforma in merci (prodotti da vendere sul mercato) anche entità che non sono state prodotte per il mercato: la terra (l'ambiente), il lavoro, e il denaro. Ne risultano tensioni potenzialmente distruttive per l'intera società, se le dinamiche del mercato non sono soggette a limiti e controlli, da parte del diritto, dalla politica e dei movimenti sociali (come quelli di lavoratori e consumatori). Nel capitalismo della sorveglianza – afferma Zuboff – il dominio del mercato si estende all'esperienza umana: il comportamento degli individui viene registrato ed analizzato e i dati, le previsioni e le conseguenti capacità di influenza, diventano una nuova merce.

concetto stesso di tutela della privacy, rendendo di fatto obsolete, o comunque non più efficienti, le norme che fino a qualche anno fa tutelavano la riservatezza degli individui intesa semplicemente come diritto ad essere lasciati soli³.

Nel mondo digitale “essere lasciati soli” non basta, dal momento che è l’individuo stesso che, più o meno consapevolmente, produce contenuti e con essi genera dati personali che viaggiano liberamente in rete. Il paradigma è cambiato completamente perché appare mutato il concetto stesso di “solitudine” e, dunque, di riservatezza nell’epoca digitale. Prima l’individuo voleva e poteva “semplicemente” evitare che ingerenze esterne entrassero nella sfera della propria riservatezza ed intimità (una logica, dunque, *protettiva*). Oggi, invece, l’individuo deve prima di tutto poter decidere di sottrarre i propri dati personali a quei processi di raccolta, aggregazione e riutilizzo che caratterizzano i *big data* e che sono alla base anche dei sistemi di IA. La logica, dunque, è prima di tutto *ablativa* nel senso che non è tanto il mondo ad essere tenuto fuori (privacy *protettiva*) quanto piuttosto l’individuo a sottrarsi al mondo (privacy *ablativa*).

In questo panorama la normativa in materia di protezione dati rappresenta un fondamentale presidio di garanzia, tanto in termini di diritti esercitabili dall’utente, quanto nella direzione di stimolo verso una logica di responsabilizzazione dei titolari coinvolti a vario titolo nella sempre più articolata filiera in cui si svolgono i trattamenti.

Una direzione, questa, che deve considerare prioritaria la necessità di escludere, o quantomeno minimizzare, il rischio di intendere la cessione dei propri dati quale tributo necessario alla fruizione dei vantaggi offerti dalla rete: una prospettiva pre-

³ Sull’uso delle nuove tecnologie in relazione ai rischi per le libertà e i diritti degli individui cfr.: A. SORO, *Persone in Rete. I dati tra poteri e diritti*, Fazi Editore, Roma, 2018; T.E. FROSINI-O. POLLICINO-E. APA-M. BASSINI (a cura di), *Diritti e libertà in Internet*, Le Monnier, Firenze, 2017. Ma vedi anche G. DE MINICO, *Antiche libertà e nuove frontiera digitale*, Giapichelli, Torino, 2016.

occupante e inaccettabile sul piano culturale, prima ancora che giuridico.

Ma la riflessione ci porta più lontano: così, se pensiamo a Facebook dobbiamo chiederci se siamo in presenza di una piazza virtuale, un luogo neutro dove si formano e agiscono liberamente quelle formazioni sociali dove si svolge la personalità individuale, in conformità ai principi costituzionali, o abbiamo di fronte un orizzonte più complesso e, certamente, a tratti più oscuro.

Dalla osservazione che siamo di fronte ad una grande agenzia pubblicitaria, che vende spazi pubblicitari e li mostra costantemente ai propri iscritti, possiamo giungere a chiederci quanto l'uso della rete per le interazioni sia funzionale a creare dialogo, tolleranza e attenzione per le ragioni degli altri o invece, all'opposto, quanto sia reale il rischio di irrigidire contrapposizioni e ostilità.

A ben guardare buona parte dell'attuale ecosistema informativo digitale tende a sottrarre il cittadino alla regola base degli ordinamenti democratici, costruita sul confronto e la scelta fra opinioni diverse. Un mondo che, al contrario, tende alla creazione di enclave che si chiudono, ciascuna in sé stessa, in una dinamica mirata a far arrivare a ciascuno opinioni confermate di ciò che si presume rappresenti già una posizione, comunque un orientamento già assunto da ciascuno sulla base di un giudizio o di un pregiudizio poco importa.

Se davvero quelle che tendono a crearsi oggi in rete sono le formazioni sociali dei tempi nuovi, allora, si è osservato, la funzione cui assolvono è esattamente opposta a quella educazione agli affari collettivi per cui le aveva valorizzate il costituente⁴.

Ma il discorso si allarga se pensiamo ai rischi che corriamo se guardiamo al trasferimento in atto, del fenomeno ora descritto, all'ambito dell'esercizio dei diritti politici e al modo in cui

⁴ Così G. AMATO, *Prefazione*, in A. SORO, *Democrazia e potere dei dati: libertà, algoritmi, umanesimo digitale*, Baldini-Castoldi, Milano, 2019.

si stanno affinando le tecniche di profilazione dell'elettore: campagne elettorali con monitoraggio di gusti e bisogni, da Obama a Trudeau, ne sono state fatte oramai diverse. Il caso "Cambridge Analytica" ha certamente rappresentato lo spartiacque in tal senso, dal momento che ha rivelato un sistema molto complesso e strutturato finalizzato alla profilazione elettorale e all'orientamento dei comportamenti degli elettori, evidenziando così anche una "ricchezza" e un valore "misurabile" del dato idoneo a rivelare opinioni politiche⁵.

Una gravità del fenomeno che ha spinto anche le istituzioni politiche europee a prendere posizione su tali temi; in occasione delle elezioni per il Parlamento europeo della primavera 2019, la Commissione ha varato un pacchetto di misure legislative al fine di "garantire elezioni europee libere e regolari"⁶, volte ad assicurare il rispetto della privacy, il contrasto alle *fake news* e alla disinformazione, la trasparenza della propaganda politica online, per finire con norme più rigide per i finanziamenti dei partiti politici europei.

Un fenomeno, legato all'uso dei *big data* che, non vi è dubbio, rischia di cambiare il rapporto fra democrazia, rappresentanza politica e società.

L'utilità della profilazione elettorale consiste principalmente nella ottimizzazione dell'invio di messaggi elettorali, basati sulla previsione di comportamento ed opinione degli individui, di cui si sono studiate le abitudini attraverso operazioni di raccolta, analisi e rielaborazione delle informazioni presenti sul web, poi incrociate con ulteriori informazioni quali i dati relativi all'età, al reddito, allo stato civile etc., insomma, le "impronte digitali" lasciate sul web.

Trattandosi a tutti gli effetti di una profilazione (viene anche usato il termine tecnico di *micro-targeting*), questo tipo di trat-

⁵ Cfr.: L. CALIFANO, *Comunicazione politica e social network*, in *Cultura giuridica e diritto vivente*, 2022, n. 20.

⁶ M. RUBECHI, *Le modalità di elezione dei membri del Parlamento europeo, tra normative nazionali e profili eurolunionali*, in *federalismi.it*, 2019, n. 11.

tamento genera molti problemi non solo dal punto di vista della privacy, a maggior ragione perché parliamo di dati idonei a rivelare potenzialmente opinioni e orientamenti politici e, dunque, dati che necessitano di una particolare tutela.

Le principali problematicità, analogamente a quanto avviene per la profilazione commerciale, sono connesse all'opacità o assenza totale delle informazioni sul trattamento, al mancato rispetto del principio di legalità, all'assenza di una base legale, dal momento che nella maggior parte dei casi tali informazioni sono raccolte in origine per finalità del tutto diverse da quelle di marketing elettorale⁷.

Per altro verso, se operazioni di questo genere servono a comprendere cosa i cittadini desiderano che i loro rappresentanti facciano e, dunque, cosa è bene che i candidati propongano per essere eletti, è evidente che le criticità non si fermano alla protezione dei dati.

Bisogna anzitutto chiedersi quale sia l'idea di democrazia che l'impiego di siffatti strumenti presuppone e, dunque, quali siano le nuove forme che la sovranità popolare e la rappresentanza politica assumono all'interno della società contemporanea al tempo dei *big data*.

In altre parole, la domanda di fondo è in che modo evitare che il cittadino venga sempre più concepito (e si concepisca a sua volta) come utente o consumatore politico, piuttosto che come soggetto di partecipazione politica.

Perché, se per un verso i cittadini chiedono e pretendono più informazioni e dati per conoscere e controllare il potere politi-

⁷ Come ben evidenziano alcuni recenti provvedimenti del Garante per la protezione dei dati personali, relativamente alla funzionalità "Election Day Information (EDI)", applicata da Meta in occasione delle elezioni per il rinnovo del Parlamento italiano nel settembre 2022. Si vedano le argomentazioni del Garante in: Provvedimento n. 448 del 21 dicembre 2022, [doc. web n. 9853406] e Provvedimento n. 77 del 22 marzo 2023 [doc. web n. 9879700]. Per un commento sia consentito il rinvio a L. CALIFANO, *Chat GPT e Meta EDI: spunti problematici su profili regolatori e ruolo delle autorità di controllo di protezione dati*, in *federalismi.it*, 2023, n. 10.

co – ma anche per partecipare, organizzarsi e mobilitarsi utilizzando la rete – dall’altro il rischio, già da tempo paventato⁸, è che per questa strada si giunga ad un modello di “iperdemocrazia” basato sui limiti e sui controlli che i cittadini tramite la rete pretendono di esercitare sugli eletti.

Ora la Costituzione nella sua essenza stessa è limite al potere e ognuno vede bene che con l’uso della rete e l’idea di una consultazione perenne dell’elettorato si registra tanto il prevalere del concetto di limite su quello di decisione e autorità, quanto l’effetto indotto di una crescente sfiducia del cittadino nei confronti degli eletti e delle istituzioni in generale.

Una dinamica che trasforma geneticamente il potere di controllo dei cittadini in automatico meccanismo di delegittimazione delle istituzioni, delineando così un esito paradossale proprio rispetto al concetto originario di sovranità popolare e rappresentanza.

Ma, è al contempo vero che, se l’elettore è sempre più assimilato a un consumatore, il primo effetto sarà, anche qui, quello della massificazione delle opinioni, della libera determinazione individuale, a tutto detrimento del pluralismo informativo e politico.

Non ultimo è il rischio che possa concretamente innestarsi un silenzioso meccanismo di svuotamento e, dunque, delegittimazione degli eletti e con essi dei partiti politici.

Una premessa che non comporta, sia chiaro, l’idea che l’utilizzo dei mezzi di comunicazione nell’era digitale sia un male in sé. Al contrario, essi possono rappresentare una risorsa per la democrazia rappresentativa, purché ci si limiti a concepire la rete e i social network in maniera strumentale e non finalistica, preservando il ruolo fondamentale di intermediazione democratica offerta dai partiti e dagli altri soggetti intermedi quali sindacati e associazioni.

In altri termini si può osservare che il tema della democrazia digitale ha posto all’attenzione di tutti noi costi e benefici

⁸ S. RODOTÀ, *Iperdemocrazia*, cit.

che le nuove tecnologie pongono ai sistemi democratici contemporanei.

Come conciliare i due aspetti è domanda che deve condurci, forse, non tanto al problema astratto di quanto, in che misura l'innovazione tecnologica metta in crisi i sistemi democratici, ma forse, piuttosto, ribaltando la prospettiva, a chiederci quali siano le sfide che l'avanzamento tecnologico pone alla democrazia e, lungo questa strada, come individuare e scegliere l'ordine delle priorità delle sfide cui far fronte. Un percorso di cauta ponderazione e analisi delle incognite poste dal processo tecnologico, che coinvolge anzitutto la comprensione dell'impatto prodotto dal cambiamento e, di conseguenza, la priorità delle scelte in grado di facilitare, ad esempio, la trasformazione dei modelli partecipativi. Perché, se guardiamo meglio i tratti di questa nuova sovranità tecnologica, scavando oltre l'immagine dell'innovazione come fattore di crescita, di sviluppo e di liberazione della persona, ne scopriamo una dinamica interna di crescita esponenziale ed una sua diffusione che si mostra insofferente tanto all'idea di limitazioni, quanto alle forme conosciute di regolazione giuridica.

Superata in radice l'idea di una crescita lineare della tecnologia, di pari passo è la consapevolezza dell'enorme concentrazione economica che la potenza di automazione e di rielaborazione ha prodotto nelle mani dei privati.

Un nuovo potere⁹ che, esattamente come in passato si trasferisce da una sede ad un'altra: un potere che non ha più caratteri necessariamente pubblici o privati, personali o collettivi, ma ha essenzialmente caratteri tecnici. Un potere che fonda la sua legittimazione su competenze di carattere tecnico-scientifico e sulla capacità di implementazione tecnologica e di controllo delle informazioni che da tali sistemi derivano.

Il tema, peraltro, non è tanto il cambiamento di sede del potere, e con esso dei tratti della sovranità, e nemmeno che si trat-

⁹ Ampiamente in tal senso A. SORO, *Democrazia e potere dei dati: libertà, algoritmi, umanesimo digitale*, Baldini-Castoldi, Milano, 2019.

ti di mani ignote¹⁰, il tema vero è la necessità di ripensare regole capaci di fissare la misura del potere e proteggere i diritti fondamentali.

Nel paradigma digitale fatto di *big data*, di Internet delle cose, di IA, di automazione di tutti i processi produttivi e comunicativi, l'incidenza sulla sfera individuale, sulla dignità e libertà dell'uomo da parte di chi detiene le conoscenze tecnologiche può manifestarsi in molti modi: dai sistemi che generano un controllo a distanza dell'individuo lavoratore all'informazione connessa al corredo genetico di ciascuno di noi, dalla profilazione piegata alle finalità elettorali e politiche alla massiva raccolta dei dati sanitari connessi a dispositivi medici che diventano un patrimonio economico inestimabile per le aziende farmaceutiche e le compagnie assicurative. E che dire, lungo questa strada, dell'uso dell'intelligenza artificiale nel settore militare e della sicurezza che può giungere a sostituire l'essere umano con un robot con risultati la cui imprevedibilità spaventa o, ancora, l'uso di algoritmi e robot che già ora cominciano a sostituire il giudice, ad esempio nella scelta di una famiglia cui affidare un bambino o, ancora nel valutare gli estremi e le ragioni che giustificano la carcerazione preventiva in relazione al rischio di fuga o reiterazione del reato¹¹.

Certamente non basta più la disciplina nazionale; è in regolazioni sovranazionali efficaci, che ci garantiscano una piattaforma comune, la miglior difesa della stessa sovranità naziona-

¹⁰ Sul punto R. BIN, *La sovranità nazionale e la sua erosione*, in A. PUGIOTTO (a cura di), *Per una consapevole cultura costituzionale. Lezioni magistrali*, Jovene Editore, Napoli, 2013, pp. 369-381, ma vedi anche A. SIMONCINI, *Sovranità e potere nell'era digitale*, in T.E. FROSINI-O. POLLICINO-E. APA-M. BASSINI (a cura di), *op. cit.*, p. 19 ss.

¹¹ Cfr.: Sul tema in vario modo: A. BONFANTI, *Big data e polizia predittiva: riflessioni in tema di protezione del diritto alla privacy e dei dati personali*, in *Medialaws*, 2018, n. 3. Ma si vedano anche gli esiti dei lavori della Commissione europea per l'efficienza della giustizia (Cepej) del Consiglio d'Europa, *European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their environment*, Strasburgo, 3-4 dicembre 2018.

le. In questo senso il nuovo Regolamento Generale sulla Protezione dei Dati¹² (da qui in avanti “GDPR” o “Regolamento”) può rappresentare uno strumento idoneo a fornire almeno qualche soluzione ai tanti interrogativi che ci stiamo ponendo¹³ e che nelle pagine di questo studio troveranno ampio spazio e possibili soluzioni.

In primo luogo, l’impiego anzidetto di una fonte normativa sovranazionale, capace tanto di uniformare, quanto di lasciare margini all’implementazione in ambito statale.

In secondo luogo, la positivizzazione e la conseguente giustiziabilità del principio di responsabilizzazione e della valutazione di impatto preliminare (nel senso della loro invocabilità come parametri normativi nelle controversie e come parametri di accertamento da parte delle Autorità di controllo); regole, queste, già testate in altri settori e che, chiamando in causa i soggetti privati, tenuti a definire e giustificare i limiti della propria azione, hanno dato buona prova di sé.

Vi è poi da considerare l’importanza di avere affermato la natura di diritto fondamentale della protezione dei dati personali.

Ma, per far fronte alle sfide che l’era digitale comporta, le autorità pubbliche necessitano di nuovi strumenti normativi, in grado di superare i confini territoriali dei singoli Paesi e persi-

¹² Regolamento (Ue) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la Direttiva 1995/46/CE (Regolamento generale sulla protezione dei dati personali).

¹³ Sul GDPR sia consentito il rinvio a L. CALIFANO-C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona: il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Editoriale Scientifica, Napoli, 2017; G. FINOCCHIARO (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, il Mulino, Bologna, 2017; F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla direttiva 95/46 al nuovo Regolamento europeo*, Giappichelli, Torino, 2016.

no dei continenti (si pensi al principio del c.d. *targeting*¹⁴); in questa prospettiva il GDPR si configura quale strumento in grado di essere applicato in maniera omogenea in tutta Europa, conciliando la massima circolazione delle informazioni con la massima tutela per gli individui.

Resta al fondo, in ogni caso, e prima di entrare nello specifico di singole questioni problematiche, una domanda che va oltre il diritto e che, al contempo, non possiamo esimerci dal porci preliminarmente. Se l'essenza dell'uomo risiede nella sua libertà, ovviamente intesa in senso alto, filosofico, quale espressione di consapevolezza, creatività e responsabilità, ne consegue che l'intelligenza artificiale di cui dotiamo le macchine che costruiamo potrà essere un fattore di crescita, una preziosa alleata, se sarà capace di conservare e magari stimolare la pienezza della condizione umana come vita libera. Ma, al contrario, di fronte alla trasformazione dell'uomo e del mondo e alla obbedienza della logica dei numeri e della tecnologia in una condizione di riduzione o affievolimento del godimento di alcune libertà individuali, bisognerà avere il coraggio di fermarsi e di stabilire la regola per cui un numero rilevante di Paesi dovrà porre un limite all'uso dell'IA applicata a determinati ambiti.

¹⁴ Con questa espressione ci si riferisce al criterio del c.d. indirizzamento (*targeting*) del trattamento (art. 3, par. 2 GDPR), uno dei due criteri relativi all'ambito di applicazione del GDPR (il primo è il c.d. stabilimento, art. 3, par. 1). Cfr.: *Linee-guida 3 del 2018 sull'ambito di applicazione territoriale del GDPR (articolo 3)*, Versione 2.1, adottate dall'EDPB il 12 novembre 2019, dove si chiarisce che «l'applicazione del “criterio dell'indirizzamento (*targeting*) del trattamento” nei confronti di interessati che si trovano nell'Unione, come disposto nell'art. 3, par. 2, può configurarsi in rapporto ad attività di trattamento svolte da un titolare o da un responsabile del trattamento non stabiliti nell'Unione con riguardo a due diverse e alternative tipologie di attività, a condizione che tali attività di trattamento si riferiscano a interessati che si trovano nell'Unione. Oltre a essere applicabile solo al trattamento effettuato da un titolare o da un responsabile del trattamento non stabilito nell'Unione, il criterio dell'indirizzamento fa perno sostanzialmente su ciò che le “attività di trattamento” “riguardano”, da valutare caso per caso» (p. 15).

2. L'attuazione e l'evoluzione della tutela della privacy quale diritto fondamentale di matrice europea: la dimensione della riservatezza; l'ampliamento alla protezione dei dati; la privacy nell'era del digitale

Se superiamo la prospettiva strettamente economicistica, connessa alle quattro libertà fondamentali su cui si è costruito il processo di integrazione europea (libertà di circolazione di merci, persone, servizi e capitali), pochi altri diritti appartenenti alla cosiddetta “nuova generazione” possono vantare l'autentica e solida matrice europea che è propria del diritto alla privacy.

La protezione giuridica di questo diritto, infatti, ha seguito una strada di progressiva positivizzazione caratterizzata non solo, come normalmente avviene nel percorso di emersione dei diritti, da un proficuo dialogo fra interpretazione giurisprudenziale e scelte del legislatore nazionale, quanto ed in particolare dall'intreccio costante fra il livello nazionale e la dimensione europea: il circuito sovranazionale che si affianca, fino a compenetrarsi e integrarsi, al circuito costituzionale interno e che, come vedremo, vive nella centralità del ruolo assunto delle Corti.

Possiamo ormai considerare patrimonio comune, nazionale ed europeo, la costruzione del diritto alla privacy quale diritto fondamentale dell'uomo in ragione della sua intima connessione con la difesa della dignità della persona; dalle Carte dei diritti alle scelte normative, dalle sentenze di ogni grado alle prassi amministrative nessun dubbio si può oggi sollevare su una tale sua natura e configurazione; esempio concreto ed emblematico della tutela multilivello dei diritti fondamentali e della tutela giurisdizionale assicurata dalle tre Corti che animano, almeno in tema di diritti individuali, l'ordinamento costituzionale italiano e l'ordinamento sovranazionale europeo (Corte costituzionale, Corte europea dei diritti dell'Uomo, Corte di giustizia dell'Unione europea). Abbandonata ben presto la più ristretta nozione di riservatezza di matrice anglosassone (*right to be let alone*), la privacy nasce, si sviluppa ed evolve come

diritto fondamentale europeo. Sia che si voglia guardare alle sue prime codificazioni in testi scritti e in dichiarazioni dei diritti, sia che la si voglia leggere esclusivamente come portato dell'elaborazione giurisprudenziale delle Corti, il diritto fondamentale alla privacy nasce all'interno dello spazio giuridico europeo latamente inteso (Consiglio d'Europa e Unione europea), per poi transitare negli ordinamenti nazionali e nuovamente – come dimostrato sia dalla Carta di Nizza che dal Regolamento generale – ritornare in Europa sotto forma di diritto fondamentale di tutti i cittadini europei, con una disciplina immediatamente applicabile in tutti gli Stati membri.

Distingueremo nell'evoluzione del diritto tre passaggi fondamentali che, come vedremo, coincidono tanto con interventi normativi, quanto con pronunce giurisprudenziali. Utile usare una metafora che, forse, potrà sembrare a tratti un po' forzata, ma che aiuterà a comprendere un percorso formativo così peculiare, così come l'intrinseca pluralità contenutistica di un diritto che l'interprete deve studiare nella sua complessa struttura e definizione.

La dimensione della riservatezza. Come nella storia della televisione, possiamo iniziare l'analisi dall'epoca della privacy in “bianco e nero” e del tubo catodico. Una prima fase costruita sul modello americano, in cui il concetto di privacy coincideva (e si esauriva) con quello di riservatezza, di protezione della vita familiare e intima, intesa anche come tutela della sfera in cui l'individuo matura le proprie convinzioni di carattere esclusivamente personale. Questa è l'impostazione che, in ambito europeo, si ritrova, già nel 1950, con la formulazione letterale dell'art. 8 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (da qui in avanti “CEDU”). La tutela offerta dalla CEDU alla vita privata e familiare dei cittadini viene formulata come una classica libertà negativa, specificando che gli interventi delle autorità pubbliche devono essere limitati allo stretto necessario e a pochi casi di indispensabile tutela di interessi pubblici prevalenti (sicurezza nazionale, repressione dei reati, pubblica sicurezza etc.).

Una configurazione del diritto, dunque, quale libertà di tipo negativo costruita a difesa della propria sfera personale e familiare da ingerenze altrui; un'esigenza che, come noto, si è primariamente e significativamente affermata in contrapposizione alla libertà di espressione e di stampa come testimonia la vicenda che interessò in prima persona Samuel Warren e Louis Brandeis, fornendo il *casus belli* che consentì la prima elaborazione giuridica del diritto alla privacy.

In questo primo significato la tutela della riservatezza assume una dimensione socio-relazionale e presuppone forme e modalità di protezione giuridica di quella particolare sfera delle vicende umane che, come già osservato, si qualifica normalmente come vita privata o intima e, proprio in quanto tale, meritevole di tutela giuridica nei confronti di ingiustificate interferenze o altre indebite forme di indiscrezione provenienti dall'esterno. Gli ordinamenti giuridici sentono l'esigenza, cioè, di garantire ai cittadini la tutela della loro intimità nei confronti tanto di soggetti privati quanto pubblici, escludendo il trattamento (raccolta, comunicazione e diffusione) di dati, fatti e informazioni che possano violare, appunto, lo spazio strettamente riservato e personale di ciascuno¹⁵.

¹⁵ Difficile suggerire esaustivamente la bibliografia sul tema della riservatezza e l'evoluzione di tale diritto ma per tutti si vedano: A.M. SANDULLI-A. BALDASSARRE, *Profili costituzionali della statistica in Italia*, in *Diritto e società*, 1973; S. RODOTÀ, *La "privacy" tra individuo e collettività*, in *Politica del diritto*, 1974; S. RODOTÀ, *Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali*, in *Rivista critica del diritto privato*, 1997; A. CERRI, *Riservatezza (diritto alla), diritto costituzionale*, in *Enciclopedia giuridica*, vol. XXVIII, Roma, 1995; F. MODUGNO, *I "nuovi diritti" nella giurisprudenza costituzionale*, Giappichelli, Torino, 1995; G. BUSIA, *Riservatezza (diritto alla)*, in *Digesto delle discipline pubblicistiche*, agg., Torino, 2000, p. 481. U. DE SIERVO, *Tutela dei dati personali e riservatezza*, in AA.VV., *Diritti, nuove tecnologie, trasformazioni sociali: scritti in memoria di Paolo Barile*, CEDAM, Padova, 2003; G.M. SALLERNO, *La protezione della riservatezza e l'inviolabilità della corrispondenza*, in P. RIDOLA-R. NANIA (a cura di), *I diritti costituzionali*, Giappichelli, Torino, 2006, vol. II, p. 617 ss.; L. CALIFANO, *Privacy: affermazione e*

Per altro verso, se la dimensione internazionale della CEDU, che si nutrive delle tradizioni costituzionali comuni anche di Paesi con sistemi di *common law*, segue una impostazione finalizzata a riconoscere alla riservatezza la natura di autonomo diritto rispetto alle altre libertà civili classiche, il Costituente italiano, immerso nella tradizione civilistica, non aveva esplicitato in una specifica disposizione costituzionale il diritto alla riservatezza.

In assenza di una sua formulazione espressa nella Costituzione italiana, la giurisprudenza¹⁶ e la dottrina hanno fatto ricorso a quei principi di rilievo costituzionale che, collocando il pieno sviluppo della persona umana al centro delle finalità che devono essere perseguite dai poteri pubblici e riconoscendo, nonché garantendo, i diritti inviolabili dell'uomo, consentono una lettura sistematica delle disposizioni costituzionali collegate alla tutela della sfera della riservatezza ed alla sua sicura classificazione fra i diritti fondamentali.

Si tratta, in primo luogo, delle disposizioni costituzionali che garantiscono in modo inequivocabile specifiche sfere di libertà individuale dall'altrui ingerenza: dalla libertà personale (art. 13) all'inviolabilità del domicilio (art. 14); dalla libertà e segretezza della comunicazione (art. 15) alla libertà di manifestazione del pensiero (art. 21).

Possono altresì essere utilmente ricordati i casi in cui la nostra Costituzione fa espresso riferimento a situazioni, rapporti e comunque ambiti di attività umane giuridicamente protetti da interferenze esterne. Così per il diritto all'esercizio privato del culto religioso (art. 19), il diritto al nome (art. 22), l'inviolabilità del diritto di difesa (art. 24), i diritti della famiglia come so-

pratica di un diritto fondamentale, Editoriale Scientifica, Napoli, 2016. Come noto, la primissima concettualizzazione si deve a S.D. WARREN-L. BRANDEIS, *The right to privacy*, in *Harvard Law Review*, 1890, n. 4.

¹⁶ Cfr. fra le sentenze più rilevanti della Corte costituzionale: sentenze n. 38 del 1973; n. 139 del 1990; n. 366 del 1991; n. 81 del 1993; n. 135 del 2002; n. 271 del 2005. Fondamentale l'intervento della Corte di cassazione nel noto "caso Soraya", Cass., sez. I, 27 maggio 1975, n. 2129.

cietà naturale (art. 29), il rispetto della persona umana nell'assoggettamento ai trattamenti sanitari obbligatori (art. 32).

Peraltro, è specificamente l'art. 2 della Costituzione, nella sua accezione di clausola a "fattispecie aperta"¹⁷, a consentire al diritto alla riservatezza di trovare posto tra i diritti fondamentali della persona, in particolare nella sua costruzione quale vero e proprio diritto della personalità.

Importante sottolineare, inoltre, che la corretta interpretazione del diritto alla privacy, inteso nella sua accezione di tutela della riservatezza, ha prodotto un ampliamento del contenuto dei diritti fondamentali classici: così, ad esempio, la libertà personale si espande progressivamente anche nella dimensione della tutela della libertà morale del singolo e, analogamente, nel significato di domicilio alla realtà materiale si accompagna il riconoscimento, e conseguente protezione, della sfera intima, anche in termini di domicilio ideale.

Ad ogni modo, tanto in ambito europeo che in ambito italiano, la parola chiave per comprendere questa prima fase è senza dubbio riservatezza.

Una costruzione del diritto che nel nostro Paese la giurisprudenza della Corte costituzionale e, ancor più significativamente, della Corte di cassazione, riconducono alla natura di un diritto della personalità, imperniato sull'art. 2 della Costituzione, nella sua accezione di clausola generale di riconoscimento e tutela dei diritti inviolabili dell'uomo in relazione allo svolgimento della personalità, nonché del "pieno sviluppo della personalità umana" (art. 3, comma 3, della Costituzione).

Una volta di più, è la "matrice aperta" della Costituzione italiana a consentire alla protezione della riservatezza di essere qualificata come diritto fondamentale della persona.

La garanzia del godimento di spazi di libertà del tutto protetti dall'ingerenza altrui: questa sembra essere la definizione minima di diritto alla riservatezza che, in questa prima accezione,

¹⁷ A. BARBERA, *Art. 2*, in G. BRANCA (a cura di), *Commentario della Costituzione. Principii fondamentali, art. 1-12*, Bologna, 1975.