Le fonti

Elia Cremona

Abstract: This chapter examines data protection sources, focusing on both European and national ones. It also deals with private sources such as codes of conduct.

Keywords: Legal sources, fundamental rights, codes of conduct

1. Introduzione

Sin dalle origini, a fine Ottocento, la disciplina giuridica dei dati personali si è caratterizzata per un elevato grado di dinamicità: nel corso del tempo, infatti, sono cambiate le esigenze di protezione, i centri del potere legislativo e di quello economico, sono cambiati i costumi ed è cambiata la società, oggi sempre più immersa nella dimensione digitale.

Il risultato di questa evoluzione è un paesaggio normativo complesso, fatto di princìpi e regole che promanano da soggetti diversi, che rispondono a logiche diverse, anche se tra loro complementari. Prima, dunque, di passare in rassegna le *fonti* di questa disciplina, ripercorriamo brevemente questa linea evolutiva.

Quando, come è stato ricordato in precedenza, Samuel D. Warren e Louis Brandeis si inventarono il diritto alla privacy, inteso nel senso di *right to be let alone* (Warren, Brandeis 1890), avevano in mente le intrusioni nella vita privata da parte della neonata stampa scandalistica, accusata da parte loro di aver varcato i limiti della decenza e del rispetto del diritto di proprietà. Il diritto alla privacy veniva cioè coniato come 'espansione' del più sacro dei diritti dello stato liberale: la proprietà, appunto, non più considerata come dominio sulle cose connotate da materialità, ma estesa al diritto di impedire la divulgazione di informazioni, pensieri e sentimenti riferibili al soggetto interessato.

Oggi, se pure l'etichetta privacy sia sopravvissuta e ancora largamente impiegata anche nel comune dibattito pubblico, è rimasto ben poco del «diritto

Elia Cremona, University of Siena, Italy, elia.cremona@unisi.it, 0000-0001-9336-218X

Referee List (DOI 10.36253/fup_referee_list)
FUP Best Practice in Scholarly Publishing (DOI 10.36253/fup_best_practice)

ad essere lasciati soli». Anzi, il principale campo di applicazione della normativa privacy è quello delle relazioni sociali e dei rapporti economici nello spazio digitale, nel quale l'*animus* dell'utente medio è non già quello di escludere qualcuno dal proprio dominio (*excludendi*) bensì di condividere (*communicandi*) informazioni, pensieri e sentimenti che lo riguardano con una platea più ampia possibile di soggetti.

Ciò si verifica sia nell'ipotesi in cui la condivisione del dato personale è lo scopo diretto dell'utente sul *web*, come nel caso delle piattaforme social (Instagram, X o Facebook), sia quando la condivisione è invece strumentale all'accesso ad un servizio, come nel caso dei servizi 'gratuiti' di cui fruiamo quotidianamente attraverso internet dando in cambio in nostri dati (dalla galassia dei servizi Google ai software Microsoft, fino ai più recenti sistemi di intelligenza artificiale generativa come Chat-GPT o Gemini). Nonostante ciò, il grado di consapevolezza dell'effetto «sorveglianza» (Zuboff 2018) che questa fruizione gratuita produce rimane molto scarso e, oggi, la privacy, intesa tradizionalmente come «riservatezza», sembra essere divenuta un problema meno percepito di un tempo.

L'evoluzione dei costumi sociali è così 'ruotata' intorno al concetto di privacy, che sul piano giuridico è però rimasto per lungo tempo ancorato alla cultura proprietaria che lo aveva ispirato.

Volendo scandire le tappe essenziali di questo percorso, prima di affermazione e poi di affrancamento dal modello proprietario, possiamo – sul piano del diritto internazionale ed europeo – indicare questa prima sequenza di atti: la Convenzione Europea dei Diritti dell'Uomo (del 1950), la Convenzione sulla protezione delle persone rispetto al trattamento automatizzato dei dati di carattere personale (c.d. Convenzione n. 108 del 1981), la Direttiva 95/46/CE, la Carta dei Diritti Fondamentali dell'Unione Europea (c.d. Carta di Nizza, 2001), il Reg. UE 2016/679 (il Regolamento Generale sulla Protezione dei Dati Personali; d'ora in avanti: GDPR) e, da ultimo, il corposo pacchetto di atti con i quali l'Unione Europea ha disciplinato il fenomeno digitale (a partire dal febbraio 2020).

In via di sintesi: il citato modello proprietario ha prodotto sul piano normativo l'affermazione del diritto al rispetto della vita privata e familiare, postulato in ambito convenzionale dall'art. 8 della CEDU e ribadito all'art. 7 della Carta di Nizza. A questo si è affiancato, dapprima con la Direttiva 95/46/CE, poi con l'art. 8 della Carta di Nizza, l'art. 16 del TFUE e infine con il GDPR, il paradigma del 'controllo' e della 'protezione dei dati', non più inteso in senso assolutistico quale proiezione di un diritto di proprietà, ma quale punto di caduta del bilanciamento tra l'esigenza di tutelare un diritto fondamentale della personalità e l'opposta esigenza di garantire quanto più possibile la 'circolazione' dei dati, personali e non personali.

E così, il GDPR ha rappresentato un compromesso tra le esigenze del mercato dei dati e quello della tutela dei diritti, delineando uno statuto giuridico dei dati personali, da una parte, strumentale alla *garanzia* delle libertà fondamentali dell'Unione e, dall'altra, anche *funzionale* al consolidamento del mercato unico.

Dopodiché, il processo non si è arrestato e il concetto giuridico di 'dato' ha iniziato ad essere disciplinato in un'ottica sempre più funzionale all'integrazio-

ne del mercato unico. A partire dal 2017, l'Unione Europea ha avviato un ampio processo di riforma che si è incentrato sui temi della «apertura dei dati» e del «riutilizzo delle informazioni» del settore pubblico (favorendo flussi di dati *Government to Government*, c.d. G2G, e *Government to Business*, c.d. G2B), in particolare con l'approvazione della Direttiva *Open Data*. Dopodiché, le tappe sono state scandite dall'approvazione, nel 2018, del Regolamento sulla circolazione dei dati non personali e poi dalla pubblicazione della *Strategia europea per i dati* del febbraio 2020, che ha gettato le basi, tra gli altri, per il *Data Governance Act* (che per primo definisce il 'dato' in quanto tale) e il *Data Act*. In particolare, l'Unione ha annunciato la creazione di spazi comuni europei di dati in alcuni settori strategici, non rinunciando ad incoraggiare lo sblocco di flussi di dati dal settore privato a quello pubblico (*Business to Government*, c.d. B2G) e tra privati (*Business to Business*, c.d. B2B, e *Business to Consumer,* c.d. B2C).

In definitiva, la linea tracciata descrive un processo di allontanamento dal paradigma proprietario che ha caratterizzato la prima (*right to be let alone*) e, in parte, la seconda stagione (*protezione e controllo*) della normativa privacy, per un approdo ad una terza fase regolatoria caratterizzata da un accento sul tema della 'condivisione', che mira a 'liberare' enormi quantità di dati a beneficio del mercato unico e della collettività.

2. L'ordinamento multilivello delle fonti in materia di dati personali

Come ormai avviene in molti settori dell'ordinamento, la disciplina in materia di protezione dei dati personali è distribuita su più livelli normativi: vi sono le fonti di diritto internazionale (la CEDU, la Convenzione 108 e le sentenze della Corte EDU); le fonti di diritto europeo (i Trattati, il GDPR, le sentenze della Corte di Giustizia, le Linee guida e i provvedimenti del Comitato europeo per la protezione dei dati); le fonti di diritto interno (la Costituzione, il codice privacy, alcuni atti del Garante per la protezione dei dati personali); le fonti di diritto privato (i codici di condotta, i contratti).

Tutte queste fonti – che analizzeremo separatamente nei paragrafi seguenti – concorrono tra loro, pur avendo un diverso grado gerarchico, diversi ambiti di competenza ed essendo state adottate in tempi diversi.

Per comporre a sistema, dunque, questa pluralità di fonti, occorre anzitutto saper bene governare i criteri di risoluzione delle possibili antinomie, ovvero: il criterio gerarchico, il criterio della competenza e il criterio cronologico.

Il criterio gerarchico prevede che le fonti di grado superiore prevalgano su quelle di grado inferiore. Queste ultime – se in contrasto con la fonte di grado superiore – sono affette da un vizio di validità e debbono essere disapplicate o annullate. Ad esempio, una norma del codice privacy (dunque di diritto italiano) che fosse in contrasto con il GDPR (dunque un regolamento europeo direttamente applicabile) sarebbe invalida. Il che significa che il giudice italiano dovrebbe non applicarla nel caso concreto o che la Corte costituzionale italiana, se investita della questione, dovrebbe annullarla attraverso una dichiarazione di incostituzionalità per violazione degli articoli 11 e 117 della Costituzione,

che impegnano l'Italia al rispetto del diritto europeo (secondo il principio del 'primato' del diritto europeo, affermato a partire dalla sentenza della Corte di Giustizia nel caso 15 luglio 1964, C-6/64, e poi ancora nella sentenza, 9 marzo 1978, C-106/77).

Il criterio della competenza prevede invece che l'eventuale contrasto tra fonti – di eguale grado gerarchico – sia risolto in favore della fonte cui è attribuita la competenza per materia, mentre il criterio cronologico prevede che, in caso di contrasto tra fonti di eguale grado gerarchico ed entrambi competenti, la norma successiva abroghi la precedente, e cioè la sostituisca dal momento in cui entra in vigore.

Nelle pagine che seguiranno, dunque, tutte le fonti che saranno passate in rassegna dovranno ritenersi 'contemporaneamente' applicabili, ogniqualvolta non si ravvisi un'ipotesi di antinomia, che quindi dovrà essere risolta alla luce dei criteri appena indicati.

3. Il diritto internazionale: la Convenzione Europea dei Diritti dell'Uomo e la Convenzione 108

L'articolo 8 della Convenzione Europea dei Diritti dell'Uomo (CEDU) e la Convenzione 108 del Consiglio d'Europa sono due pilastri fondamentali nella tutela di diritto internazionale del diritto alla privacy e alla protezione dei dati personali. La CEDU e la Convenzione 108 sono state approvate nell'ambito del Consiglio d'Europa, una organizzazione internazionale fondata nel 1949 – che conta oggi 46 stati membri – con l'obiettivo di promuovere i diritti umani, la democrazia e lo stato di diritto. In particolare, dal punto di vista giuridico, la CEDU, adottata nel 1950, è un trattato internazionale che garantisce una serie di diritti e libertà fondamentali agli individui e che ha istituito un giudice appositamente dedicato: la Corte Europea dei Diritti dell'Uomo.

La Convenzione 108, adottata nel 1981, è stata invece il primo trattato internazionale vincolante dedicato esclusivamente alla protezione dei dati personali e alla privacy. Con il protocollo di modifica adottato nel 2018, noto come Convenzione 108 *plus*, sono state ampliate e rafforzate le misure di protezione al fine di raccogliere le nuove sfide poste dalla digitalizzazione e dalla globalizzazione.

In Italia, entrambe queste convenzioni hanno un valore normativo rilevante. La CEDU, ratificata dall'Italia con la legge n. 848 del 1955, è applicabile e vincolante per il nostro ordinamento (Corte cost. 24 ottobre 2007, nn. 348 e 349). La Convenzione 108 è stata ratificata dall'Italia nel 1985, nella sua versione originaria, e nel 2021, nella sua versione aggiornata.

Entrando nel merito dei due testi normativi, vediamo che l'articolo 8 della CEDU stabilisce il diritto al rispetto della vita privata e familiare, del domicilio e della corrispondenza, tutelando la sfera privata delle persone da ingerenze arbitrarie da parte dello Stato (le uniche giustificazioni ammesse di tali 'interferenze' sono relative alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà

altrui). La Corte Europea dei Diritti dell'Uomo ha sviluppato nel corso degli anni un'ampia giurisprudenza sull'applicazione dell'articolo 8, chiarendo che qualsiasi interferenza nella vita privata e familiare deve essere giustificata, proporzionata e basata su una norma chiara e anteriormente conoscibile.

La Convenzione 108 integra la disciplina di principio contenuta nella CEDU, dettagliando maggiormente quali debbono essere gli obblighi degli stati aderenti in tema di protezione delle persone rispetto al trattamento automatizzato dei dati personali. In particolare, si prevede: i) che sia assicurata la trasparenza nelle modalità di trattamento dei dati e la qualità del dato e siano garantiti i diritti degli individui, come il diritto di rettifica; ii) che siano previste rigorose misure di sicurezza per proteggere i dati personali da accessi abusivi non autorizzati; iii) che sia assicurata la collaborazione tra le autorità di protezione dei dati dei vari paesi per affrontare le violazioni transfrontaliere.

4. Il diritto europeo

4.1. La Carta di Nizza e il TFUE

Nel sistema delle fonti relative alla protezione dei dati personali, il ruolo centrale è assunto senz'altro dal diritto dell'Unione Europea. Le fonti rilevanti sono tre: gli artt. 7 e 8 della Carta dei diritti fondamentali dell'Unione Europea (Carta di Nizza), l'art. 16 del Trattato sul funzionamento dell'Unione Europea (TFUE) e, soprattutto, il Regolamento Generale sulla Protezione dei Dati (GDPR), che ne dà compiuta disciplina. Tutte queste fonti sono immediatamente applicabili all'interno dell'ordinamento italiano (in attuazione del principio dell'*effetto diretto* affermato dalla Corte di Giustizia a partire dalla sentenza *Van Gend en Loos* del 1963). Come detto, inoltre, esse prevalgono sul diritto interno in caso di antinomia, in ossequio al principio del *primato* del diritto europeo sugli ordinamenti nazionali, incluso il diritto costituzionale, salvi i principi fondamentali (c.d. controlimiti).

Muovendo dalla Carta di Nizza, proclamata nel 2000 e divenuta giuridicamente vincolante con il Trattato di Lisbona nel 2009, possiamo ancora rilevare le due diverse anime di questa materia: quella della privacy intesa come 'riservatezza', come diritto di escludere altri dalla propria sfera personale, e quella della privacy intesa come diritto ad avere il 'controllo' sui propri dati personali, senza necessariamente accedere ad una logica esclusiva ed escludente.

In particolare, l'articolo 7 della Carta di Nizza riprende il contenuto dell'articolo 8 della CEDU che abbiamo toccato nel paragrafo precedente, stabilendo che «ogni individuo ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni». Ancora una volta, il diritto alla privacy viene garantito *contro* ingerenze arbitrarie da parte dello Stato e di terzi. La Corte di Giustizia ha interpretato questo diritto in modo ampio, includendovi ogni forma di comunicazione e interazione di carattere privato.

L'articolo 8 è invece specificamente dedicato ai dati personali, prevedendo che ogni persona abbia diritto alla protezione dei dati di carattere personale

che la riguardano. La norma individua già alcuni princìpi fondamentali legati al trattamento dei dati, che ritroveremo anche nel GDPR, ovvero che i dati debbano essere trattati secondo il principio di lealtà, per scopi specifici e sulla base del consenso dell'interessato o su altra legittima base prevista dalla legge. Ogni persona ha altresì il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica. Pure si prescrive che il rispetto di tali regole sia soggetto al controllo di un'autorità indipendente.

L'articolo 16 del Trattato sul funzionamento dell'Unione Europea (TFUE) stabilisce il quadro giuridico per la protezione dei dati personali, fissando la competenza delle istituzioni europee (Parlamento e Consiglio) alla adozione della normativa in materia e prevedendo altresì che tale disciplina sia, da una parte, funzionale alla protezione dei diritti fondamentali e, dall'altra, che sia funzionale a garantire comunque la circolazione dei dati all'interno dell'Unione.

4.2. Il Regolamento Generale sulla Protezione dei Dati n. 679/2016 (GDPR)

In questa logica di compromesso, tra esigenze di tutela dei diritti fondamentali ed esigenze di circolazione dei dati in funzione di promozione del mercato, l'Unione Europea ha varato il Regolamento Generale sulla Protezione dei Dati (GDPR) n. 679/2016, entrato in vigore il 25 maggio 2018, che rappresenta l'evoluzione e il rafforzamento della precedente Direttiva 95/46/CE sulla protezione dei dati personali. Tale direttiva infatti, adottata nel 1995, aveva già stabilito i primi standard a livello europeo per la protezione dei dati personali e introdotto alcuni concetti fondamentali come il consenso dell'interessato, il diritto di accesso e rettifica dei dati personali; tuttavia, proprio perché si trattava di una direttiva, richiedeva il recepimento da parte degli stati membri tramite leggi nazionali, determinando così una frammentazione del sistema della protezione dei dati personali all'interno dell'UE.

Il GDPR, essendo un regolamento, è invece direttamente applicabile in tutti gli Stati membri senza bisogno di recepimento (salvo che per alcune parti che espressamente prevedono l'adozione di normative da parte degli ordinamenti nazionali), garantendo così finalmente un livello uniforme di protezione dei dati personali.

L'articolo 2 del GDPR stabilisce l'ambito di applicazione materiale, individuando cioè le situazioni in cui il Regolamento si applica. In linea generale, il GDPR si applica al trattamento di dati personali di un soggetto «interessato» effettuato da un «titolare del trattamento» o da un «responsabile del trattamento» nell'Unione Europea (tali definizioni saranno affrontate nel dettaglio nei capitoli seguenti), con alcune eccezioni relative ad esempio ad attività non rientranti nell'ambito di applicazione del diritto dell'Unione (come la sicurezza nazionale), ad attività svolte da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico (come la gestione delle proprie rubriche di contatti o la corrispondenza privata) o ad attività di prevenzione, in-

dagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali (che sono disciplinate dalla Direttiva UE 2016/680).

Tale regolamento ha, poi, un ambito di applicazione territoriale particolarmente ampio. Ai sensi dell'art. 3, esso si applica su tutto il territorio dell'Unione, non solo ai trattamenti di dati di cittadini europei da parte di soggetti europei, ma anche ai trattamenti di dati effettuati da società con sede extra-europea che svolgano una attività effettiva e stabile sul territorio europeo (*establishment criterion*) e ai trattamenti che riguardano soggetti interessati che si trovino all'interno dell'Unione (*targeting criterion*).

Con riferimento al primo criterio di applicazione, è opportuno precisare che non rileva la forma giuridica assunta (sia essa, ad esempio, una succursale o una filiale di una società con sede all'estero) quanto piuttosto l'effettivo legame tra l'attività svolta sul territorio europeo in maniera stabile e il trattamento dei dati personali, indipendentemente dal fatto che quest'ultimo avvenga o meno sul territorio dell'Unione.

Il secondo criterio, quello dell'indirizzamento (*targeting*) del trattamento, è invece preordinato ad assicurare la piena applicabilità del GDPR a prescindere dalla cittadinanza, dalla residenza o da altri elementi propri della condizione giuridica del soggetto interessato, in applicazione di quanto previsto dall'art. 8 della Carta di Nizza, in forza del quale ogni 'persona' ha diritto alla protezione dei dati personali che lo riguardano. Sul punto, l'*European Data Protection Board* ha raccomandato di applicare tale criterio secondo un approccio 'bifasico' volto a determinare, *in primis*, se il trattamento si riferisce a dati personali di interessati che si trovano nell'UE e, in secondo luogo, se riguarda l'offerta di beni o la prestazione di servizi o il monitoraggio del comportamento di soggetti interessati all'interno dell'Unione Europea.

Non solo. Vale la pena evidenziare che il GDPR ha avuto una significativa influenza anche a livello globale. Infatti, dopo la sua adozione, sono molti gli stati che hanno adottato normative simili (dal Brasile, alla California, al Cile, al Giappone) secondo quello che è stato definito come *Brussels Effect* (Bradford 2020), ovvero la capacità dell'Unione di fissare standard normativi globali.

Il GDPR rappresenta il principale testo normativo che sarà esaminato nei capitoli che seguiranno. In linea generale, può sin qui osservarsi che le principali novità introdotte dal GDPR riguardano:

1. il rafforzamento dei diritti dei soggetti interessati, introducendo – tra gli altri – il diritto alla portabilità dei dati, e novellando, ad esempio, il diritto alla cancellazione (c.d. diritto all'oblio) e il diritto di opposizione al trattamento;
2. la previsione di un principio generale di responsabilizzazione (*accountability*), in virtù del quale i titolari del trattamento devono adottare misure tecniche e organizzative adeguate a garantire e dimostrare la conformità al regolamento. Il che implica che i titolari del trattamento non solo devono rispettare le norme del regolamento, ma devono anche essere sempre in grado di dimostrare di aver adottato idonee misure tecniche e organizzative;
3. l'introduzione di un obbligo per alcune organizzazioni di nominare un responsabile della protezione dei dati (*Data Protection Officer*), che svolge un

ruolo cruciale nel garantire la conformità al GDPR all'interno dell'organizzazione e funge da punto di contatto per le autorità di controllo e gli interessati;
4. la previsione di sanzioni elevate per le violazioni, fino a 20 milioni di euro o il 4% del fatturato globale annuo, allo scopo di assicurare l'efficacia delle sue disposizioni;
5. la regolamentazione rigorosa dei trasferimenti di dati personali verso paesi terzi, richiedendo adeguate garanzie come decisioni di «adeguatezza» da parte della Commissione Europea, clausole contrattuali standard, o norme vincolanti d'impresa (*Binding Corporate Rules*).

4.3. Le sentenze della Corte di Giustizia dell'Unione Europea

Anche se non si tratta di vere e proprie fonti normative, le sentenze della Corte di Giustizia dell'Unione Europea (CGUE) sono altrettanto importanti nel sistema di disciplina della protezione dei dati personali. Infatti, le sentenze della CGUE forniscono l'interpretazione autentica del diritto europeo e vincolano i giudici nazionali al rispetto di quella interpretazione. La CGUE ha emesso numerose sentenze che hanno avuto un impatto significativo sull'applicazione delle norme sulla protezione dei dati personali.

Ad esempio, con la sentenza resa nel caso *Google Spain* (CGUE, Grande Sezione, 13 maggio 2014, C-131/12), la Corte ha per la prima volta riconosciuto il c.d. diritto all'oblio, che è stato poi inserito due anni dopo all'art. 17 del GDPR. In quella vicenda, un cittadino spagnolo aveva presentato un reclamo all'Agencia Española de Protección de Datos (AEPD) contro Google Spain e Google Inc., chiedendo che Google rimuovesse dai risultati di ricerca i *link* ad un articolo di un giornale spagnolo del 1998, che riguardava un'asta immobiliare per il recupero di alcuni crediti insoluti, in cui veniva menzionato il suo nome. Il reclamo sosteneva che l'articolo fosse ormai irrilevante e che il continuo collegamento a esso attraverso il motore di ricerca fosse lesivo del diritto alla privacy. L'Autorità spagnola accolse la richiesta e Google impugnò la decisione, sostenendo che – essendo un 'mero' motore di ricerca – non aveva responsabilità sui contenuti pubblicati da terze parti e che l'articolo in questione fosse stato pubblicato legittimamente. La Corte, investita della questione, riconobbe invece la prevalenza del diritto all'oblio, stabilendo che i motori di ricerca sono «titolari del trattamento» dei dati personali che appaiono nelle pagine *web* che indicizzano e che, pertanto, gli individui hanno sempre il diritto di chiedere la rimozione dei *link* che contengono informazioni personali quando sono obsolete o non più rilevanti.

Altre importanti decisioni sono state quelle note come *Schrems I* (CGUE, 6 ottobre 2015, C-362/14) e *Schrems II* (CGUE, 16 luglio 2020, C-311/18), dal nome del cittadino austriaco, attivista della privacy, che aveva intentato i due giudizi. In entrambi i casi, la CGUE ha annullato gli accordi – denominati *Safe Harbor* e *Privacy Shield* – per il trasferimento dei dati personali dall'UE agli USA, così imponendo l'adozione di più elevati standard di tutela a tutte le imprese (ad esempio le grandi piattaforme digitali stabilite negli Stati Uniti) che

'importavano' i dati relativi ai cittadini europei (in tema v. cap. *La regolamentazione di diversi rapporti che riguardano i dati personali*).

O ancora, si ricordi la sentenza resa nel caso *Meta Platforms Ireland Limited* (già *Facebook Ireland Limited*) contro *Bundeskartellamt* (l'Autorità antitrust tedesca) nel 2023, in cui si discuteva della condotta di Facebook consistente nella raccolta e nella combinazione di dati personali raccolti su diverse piattaforme in assenza di uno specifico consenso (CGUE, C-252/21, 4 luglio 2023). In quel caso, la Corte di Giustizia ha affermato che il mancato rispetto delle norme in materia di protezione dei dati personali può essere valutato per capire se una pratica commerciale costituisce o meno un abuso di posizione dominante. In altre parole, se una piattaforma che detiene una posizione dominante sul mercato, come Facebook, impone condizioni che violano le norme sulla protezione dei dati, ciò può essere rilevante anche per l'irrogazione di una sanzione antitrust.

Questa decisione riconosce che le pratiche di trattamento dei dati possono avere un impatto significativo anche sul grado di concorrenza nel mercato, specialmente nel contesto di piattaforme digitali che basano il proprio *business model* sulla raccolta di enormi quantità di dati degli utenti.

4.4. Le Linee Guida dell'European Data Protection Board

Nel quadro generale delle fonti, particolare importanza è rivestita dalle linee guida fornite dall'European Data Protection Board (EDPB), un organismo indipendente dell'Unione Europea responsabile di garantire l'applicazione coerente del GDPR in tutta l'UE. Queste linee guida offrono chiarimenti e orientamenti su vari aspetti della materia della protezione dei dati personali, aiutando sia i titolari del trattamento che gli interessati a comprendere meglio gli adempimenti necessari al rispetto del regolamento (*compliance*), le responsabilità e i diritti. Questi documenti sono il risultato di un processo di consultazione pubblica e della collaborazione tra le autorità nazionali di protezione dei dati.

Ad esempio, tra le principali Linee Guida dell'EDPB, si rammentano quelle sul diritto di accesso dell'interessato (1/2022), sulle notificazioni di *data breach* (9/2022), sul *targeting* degli utenti dei social media (8/2020), sull'esercizio del diritto all'oblio (5/2019), sui requisiti per la prestazione del consenso al trattamento (5/2020).

5. Il diritto costituzionale italiano

5.1. Il diritto alla riservatezza

Anche se il diritto alla privacy non ricorre espressamente nel testo della Costituzione italiana, la sua disciplina ha una sua dimensione propriamente 'costituzionale', per due ordini di ragioni. La prima è rappresentata, come abbiamo visto, dal livello delle fonti che regolano la materia. Le fonti internazionali e le fonti del diritto europeo si collocano su di un piano gerarchico superiore alle

fonti primarie (leggi e atti aventi forza di legge) ed entrano nell'ordinamento italiano proprio grazie agli artt. 11 e 117 della Costituzione.

Tale dimensione costituzionale, però, deriva anche dalla natura di diritto fondamentale che nel tempo – attraverso una interpretazione evolutiva di alcune disposizioni del testo costituzionale – è stata riconosciuta al diritto alla privacy.

Sebbene infatti inizialmente la giurisprudenza della Corte di Cassazione avesse escluso l'ammissibilità di una protezione autonoma del diritto al rispetto della vita privata (Cass. 22 dicembre 1956, n. 4487), a partire dal 1975 l'orientamento mutò, individuando in particolare nell'art. 2 della Costituzione la principale norma di copertura costituzionale della materia.

L'art. 2 Cost., infatti, afferma il principio «personalista», riconoscendo e garantendo i diritti inviolabili dell'uomo, ed è considerato una norma a fattispecie aperta, suscettibile – a certe condizioni – di incrementare il catalogo dei diritti costituzionalmente tutelati, ancorché non espressamente nominati.

Anche grazie all'intervento della dottrina (in particolare, Rodotà 1973), la giurisprudenza di legittimità e costituzionale iniziò ad individuare via via gli ulteriori interessi costituzionalmente rilevanti coinvolti nella tutela del diritto alla privacy.

Oltre alla funzione di promozione del pieno sviluppo della persona umana promossa dall'articolo 3, comma 2, Cost., le norme costituzionali rilevanti sono state individuate nell'articolo 13, che garantisce l'inviolabilità della libertà personale proteggendo il singolo da ingerenze indebite nella sfera fisica e psichica, nell'articolo 14, che sancisce l'inviolabilità del domicilio proteggendo la casa come luogo privilegiato della vita privata, nell'articolo 15, che tutela la libertà e la segretezza della corrispondenza e delle comunicazioni da intrusioni non giustificate e, infine, nell'articolo 21, che, regolando la libertà di manifestazione del pensiero e di informazione, tutela anche il diritto di non vedere divulgate informazioni di carattere personale. A completare il sistema di tutela della vita privata, vanno richiamati anche gli articoli 19 (diritto di professare la propria fede religiosa), 16 (libertà di circolazione), 17 (diritto di riunirsi pacificamente) e 18 (libertà di associazione), tutti rilevanti per la protezione della 'personalità' dell'individuo.

Come è dunque evidente, la giurisprudenza della Corte costituzionale non ha ricondotto il diritto alla vita privata a un unico parametro costituzionale. Ad esempio, nella sentenza 12 aprile 1974, n. 38, la Corte ha collegato i diritti inviolabili dell'uomo, come decoro, onore, rispettabilità, riservatezza, intimità e reputazione, all'articolo 2 della Costituzione, in combinato con gli articoli 3, comma 2, e 13, comma 1.

La Corte ha inoltre evidenziato che il diritto alla tutela della vita privata è un corollario della dignità della persona. Nella sentenza 19 dicembre 1991, n. 467, la Corte ha affermato che la sfera intima e personale deve essere considerata il riflesso giuridico più profondo della dignità della persona umana e merita una tutela proporzionata al suo livello di priorità e al suo carattere fondante nella scala dei valori espressa dalla Costituzione italiana.

5.2. Il diritto all'identità personale

A fianco del diritto al rispetto della vita privata, ma parimenti ricompreso nella dimensione costituzionale del diritto alla privacy in virtù della stretta correlazione con il diritto alla riservatezza (come accennato *supra* nel cap. I, § 1), vi è il c.d. diritto all'identità personale, ovvero l'interesse del soggetto ad «essere se stesso» e a esprimere una «verità» attinente alla propria persona nella vita di relazione.

Il diritto all'identità personale si è differenziato dagli altri diritti della personalità, avendo per oggetto la proiezione sociale della personalità complessiva dell'individuo, garantendo la rappresentazione della sua vera identità nella vita di relazione, senza alterazioni del patrimonio intellettuale, ideologico, politico, etico, religioso o professionale (Cass. 7 febbraio 1966, n. 978). Il travisamento dell'identità può consistere sia nell'attribuzione di qualità inesistenti che nell'omissione di elementi esistenti, siano essi migliorativi o peggiorativi. Anche un'alterazione migliorativa può essere illegittima se incide sulla personalità, indipendentemente dalla lesione di altri diritti.

La Corte costituzionale, con la sentenza 3 febbraio 1994, n. 13, ha riconosciuto che il diritto all'identità personale rientra nella tutela prevista dall'art. 2 della Costituzione, contribuendo a formare il patrimonio inviolabile della persona umana. I fondamenti normativi della tutela dell'identità personale si trovano nelle disposizioni relative al nome, all'immagine e, ancora una volta, nell'art. 2 della Costituzione.

Naturalmente, il diritto all'identità personale – come tutti i diritti di rango costituzionale – può entrare in bilanciamento con altri diritti. Ad esempio, il diritto all'identità personale incontra un limite necessario nei diritti di cronaca, critica, satira e creazione artistica, riconducibili all'art. 21 della Costituzione. Il diritto di cronaca prevale infatti se sorretto dall'utilità sociale della notizia, dalla verità dei fatti divulgati e dalla continenza dell'esposizione.

6. Il Codice in materia di protezione dei dati personali

Il codice in materia di protezione dei dati personali, noto come codice privacy (d.lgs. n. 196/2003 che ha abrogato la precedente disciplina rappresentata dalla l. 675/1996), ha rappresentato per anni il principale riferimento per la protezione dei dati personali in Italia.

Con l'entrata in vigore del GDPR nel 2018, il Codice Privacy è stato significativamente novellato ad opera del d.lgs. n. 101/2018 che ne ha abrogato molte disposizioni, in virtù della attrazione della disciplina al livello regolamentare europeo, apportando altresì molte modifiche e integrazioni alle disposizioni residue.

Il Codice Privacy italiano è dunque una fonte gerarchicamente inferiore al GDPR e contiene solamente una disciplina di carattere attuativo (per le materie nelle quali il legislatore europeo non può intervenire, come le sanzioni penali)

e integrativo (per previsioni di dettaglio che lo stesso GDPR ha rimesso alla legislazione degli stati membri).

Essenzialmente, oggi il Codice Privacy fornisce: 1) i principi relativi al trattamento dei dati in situazioni specifiche (come quelli relativi al perseguimento di un compito di interesse pubblico o quelli relativi ai minori, alla sanità e alla giustizia); 2) la disciplina dei trattamenti in ambito pubblico, con particolare riferimento alle strutture socio-sanitarie, all'istruzione, alla ricerca, al lavoro e ai servizi di comunicazione elettronica; 3) la disciplina della composizione, del funzionamento e dei poteri del Garante per la protezione dei dati personali e degli strumenti di tutela amministrativa e giurisdizionale a disposizione dei soggetti interessati; 4) la disciplina del sistema sanzionatorio, amministrativo e penale.

7. La co-regolazione pubblico-privata: codici di condotta, certificazioni e Binding Corporate Rules

Uno degli aspetti più significativi del GDPR, di particolare interesse per quanto attiene al sistema delle fonti analizzato in questo capitolo, è l'approccio di forte incoraggiamento verso forme di co-regolazione pubblico-privata, nelle quali gli attori privati contribuiscono alla individuazione di regole e prassi conformi alle norme di protezione dei dati. Tale approccio si manifesta attraverso diversi strumenti, tra cui codici di condotta, certificazioni, *Binding Corporate Rules* (BCR), tutti orientati a fornire pratiche settoriali specifiche, aumentare la trasparenza e facilitare la *compliance* al Regolamento.

Analizziamoli singolarmente. I codici di condotta, ai sensi dell'art. 40 del GDPR, sono strumenti di autoregolamentazione che le associazioni e altri organismi rappresentativi possono sviluppare per facilitare l'applicazione del GDPR in contesti specifici. Il processo di adozione di un codice di condotta prevede che il testo sia sottoposto all'autorità di controllo nazionale competente per la revisione e l'approvazione. Una volta approvato, il codice viene pubblicato e ulteriori organizzazioni di settore possono aderirvi volontariamente. I soggetti promotori del codice di condotta devono altresì istituire organismi di monitoraggio, che debbono essere accreditati dall'autorità di controllo, per verificare il livello di adesione al codice e per gestire eventuali violazioni.

Le certificazioni sono invece strumenti che attestano la conformità di un'organizzazione alle norme del GDPR. L'art. 42 del GDPR incoraggia la creazione di meccanismi di certificazione, sigilli e marchi per dimostrare che i trattamenti di dati personali da parte di titolari e responsabili del trattamento sono conformi al regolamento. Tali certificazioni sono rilasciate da organismi accreditati deputati alla redazione di norme tecniche (*standard*). Ad esempio, una delle principali certificazioni è la ISO 27001 (rilasciata dalla International Organization for Standardization), che rappresenta lo standard internazionale che descrive le *best practices* per un sistema di gestione della sicurezza delle informazioni (SGSI).

Le *Binding Corporate Rules* (BCR) sono uno strumento volto a consentire il trasferimento di dati personali dal territorio dello Stato verso Paesi terzi (extra-

UE) tra società facenti parti dello stesso gruppo d'impresa. Ai sensi dell'art. 47 del GDPR, le BCR si concretizzano in una serie di regole, di natura contrattuale, che fissano i principi vincolanti al cui rispetto sono tenute tutte le società appartenenti ad uno stesso gruppo, allo scopo di semplificare gli oneri amministrativi a carico delle società multinazionali con riferimento ai flussi infra-gruppo di dati personali (art. 47 GDPR).

Sempre al fine di agevolare la *compliance* al GDPR, le BCR sono sottoposte alla revisione dell'autorità di controllo nazionale competente, che può coinvolgere anche altre autorità di controllo europee. Una volta approvate, le BCR sono applicate in tutte le entità del gruppo e il loro rispetto deve essere costantemente monitorato attraverso meccanismi di sorveglianza. Molte grandi aziende tecnologiche, come Google e Microsoft, hanno adottato BCR per gestire i trasferimenti di dati personali tra le loro filiali globali.

Riferimenti bibliografici

Bradford, Anu. 2020. *The Brussels Effect: How the European Union Rules the World*. Oxford: Oxford University Press.

Colapietro, Carlo, e Antonio Iannuzzi. 2017. "I principi generali del trattamento dei dati personali e i diritti dell'interessato." In C.C. Licia Califano (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, 85-136. Napoli: Editoriale scientifica.

Rodotà, Stefano. 1973. *Elaboratori elettronici e controllo*. Bologna: Il Mulino.

Ryngaert, Cedric, e Mistale Taylor. 2020. "The GDPR as Global Data Protection Regulation?." *AJIL Unbound* 114: 5-9.

Warren, Samuel D., e Louis D. Brandeis. 1890. "The Right to Privacy." *Harvard Law Review* 4, 5: 193-200.

Zuboff, Shoshana. 2019. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: Public Affairs.