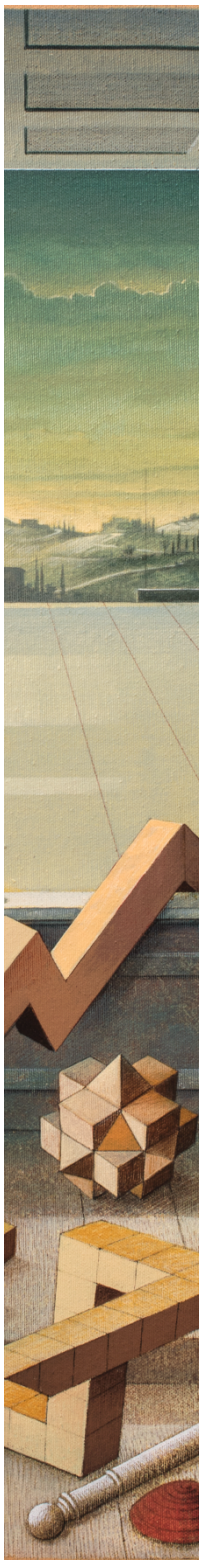
Cultura giuridica e diritto vivente
Rivista on line del Dipartimento di Giurisprudenza
Università di Urbino Carlo Bo
Note e Commenti



I DIRITTI E LE GARANZIE DEGLI INTERESSATI NEL REGOLAMENTO EUROPEO 2016/679

Licia Califano

Abstract
[Rights and guarantees of the data subjects in the General Data Protection Regulation 2016/679] The contribution reconstructs the genesis and development of the right to the protection of personal data, whose recognition at supranational level is due to the General Data Protection Regulation (GDPR) of May 2016, that went into effect on May 25, 2018. After some well-known cases, it became clear how much the circulation of personal data is an huge part of important commercial transactions. Regulation No. 2016/679, which is the last step of a path that at the European level has started a long time ago, represents a concrete opportunity to harmonize the level of protection of people's rights regarding the processing of personal data.

Key Words:
Personal data protection, European integration, privacy, privacy protection

Vol. 10 (2022)

I diritti e le garanzie degli interessati nel regolamento europeo 2016/679

Licia Califano [*]

Se si esce dalla prospettiva di analisi strettamente economicistica, connessa alle quattro libertà fondamentali alla base del processo di integrazione europea (libertà di circolazione di merci, persone, servizi e capitali), è corretto affermare che pochi altri diritti appartenenti alla cosiddetta "nuova generazione" possono vantare l'autentica e solida matrice europea che è propria del diritto alla privacy.

Abbandonata ben presto la più ristretta nozione di riservatezza di matrice anglosassone, la privacy nasce, si sviluppa e si 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 679 del 2016 – ritornare in Europa sotto forma di diritto fondamentale di tutti i cittadini europei, con una disciplina immediatamente applicabile in tutti gli Stati membri.

Esempio concreto ed emblematico, dunque, 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).

In una prima fase storica, influenzato dal modello americano, 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 personale. È questa l'impostazione che, peraltro, in ambito europeo, si ritrova già nel 1950 con la formulazione letterale dell'articolo 8 della Convenzione europea dei

[*] Licia Califano è Professoressa ordinaria di Diritto costituzionale presso il Dipartimento di Giurisprudenza dell'Università degli Studi di Urbino.
Indirizzo mail: licia.califano@uniurb.it

diritti dell'uomo. La tutela offerta dalla Convenzione alla vita privata e familiare dei cittadini viene formulata come una classica libertà negativa, specificando che l'ingerenza delle autorità pubbliche devono essere limitate allo stretto necessario e a pochi casi di necessaria tutela di interessi pubblici prevalenti (sicurezza nazionale, repressione dei reati, pubblica sicurezza ecc.).

Ma, se la dimensione internazionale della Cedu già si abbeverava delle tradizioni costituzionali comuni, anche di paesi con sistemi di *common law* e, per questo motivo, tendeva a riconoscere autonomia alla riservatezza rispetto alle altre libertà civili classiche, il Costituente italiano, immerso nella tradizione civilistica, non aveva esplicitato nel 1948 in una specifica disposizione costituzionale il solo diritto alla riservatezza. Questo, infatti, è stato ricavato in via interpretativa come risultato ermeneutico di altre, ben più classiche, libertà civili quali, significativamente ma non in via esclusiva, la libertà di domicilio e la segretezza della corrispondenza. Questa è la prospettiva di tutte le sentenze della Corte costituzionale degli anni '70, compresa la sentenza della Corte di Cassazione del 1975 sul caso Soraya (Corte cost. sent. n.122/1970 e n. 38/1973, Cassazione sent. n. 2129/1975).

Ad ogni modo, tanto in ambito europeo che in ambito italiano, la parola chiave per questa prima fase è senza dubbio una: riservatezza. Difatti, nel caso italiano la costruzione del diritto è impostata dalla giurisprudenza della Corte costituzionale e, anche più significativamente, da quella della Corte di Cassazione nei termini di un diritto della personalità, imperniato sull'articolo 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 2, Cost.).

Nel 1981 il Consiglio d'Europa elabora una Convenzione internazionale volta a tutelare il trattamento dei dati personali in modalità automatizzata. La Convenzione di Strasburgo – un accordo internazionale ratificato dall'Italia con legge n. 98 del 1989 – rappresenta la prima fonte di diritto internazionale espressamente dedicata alla protezione dei dati personali. La Convenzione, infatti, ricollega espressamente la protezione dei dati personali alla tutela della vita privata e familiare prevista dall'articolo 8 della Cedu, istituendo così, per la prima volta, quel collegamento concettuale tra tutela della riservatezza e tutela dei dati personali. Un collegamento che, da questo momento in poi, verrà riconosciuto e più volte richiamato anche dalla Corte europea dei diritti dell'uomo e che, soprattutto, verrà mutuato dall'ordinamento dell'Unione europea.

Va peraltro osservato che anche la Corte costituzionale italiana coglie, già nel 1990, il nesso esistente tra protezione dati e riservatezza e nella sentenza n. 139 i giudici riuniscono sotto la comune nozione di privacy entrambi i concetti.

Tornando all'ambito europeo, nel 1995 l'UE elabora la prima fonte di diritto derivato europeo in materia di protezione dei dati personali: si tratta della cd. direttiva madre, la n. 95/46/CE, che rappresenta la base del diritto positivo in materia di *data protection* nei principali Paesi europei. Essa ha come base giuridica l'articolo 100 A del Trattato che istituisce la Comunità europea (così come modificato a Maastricht nel 1992), il quale consentiva all'Unione di adottare tutte le misure volte a garantire il riavvicinamento delle disposizioni legislative, amministrative e regolamentari degli Stati membri aventi ad oggetto l'instaurazione e il funzionamento del mercato interno.

Pertanto, ragionando in termini di competenze, a partire da questa clausola, le istituzioni dell'Unione hanno elaborato una normativa di riferimento che, come in seguito riconoscerà la stessa Corte di Giustizia, in realtà è in grado di incidere in ciascun settore della vita pubblica e su ciascuna tipologia di trattamento dati, non solo con quelle categorie

di trattamento direttamente connesse alla regolazione del mercato interno (significativamente in tal senso la *Causa Rundfunk* del 20 maggio 2003).

La direttiva ha fatto propria la logica dell'affiancamento della protezione dati alla riservatezza nella sua dimensione di diritto fondamentale, basandosi proprio sulla elaborazione già avvenuta in sede Cedu. Paesi che non avevano mai avuto specifiche ed organiche norme in materia di protezione dati, come l'Italia, approvano una prima legge in materia di *data protection* che istituisce il Garante per la protezione dati personali e dota il nostro ordinamento dei primi strumenti di tutela in questa materia (l. 675 del 1996). Successivamente, tra il 2001 e il 2002, nonché su ulteriore sollecitazione dell'Unione europea (è del 2002 la Direttiva relativa alla tutela della privacy nel mondo delle comunicazioni elettroniche), il legislatore italiano approva le disposizioni di delega per consentire al Governo di riunire in un unico corpus normativo completo e organico tutte le disposizioni variamente sparse nell'ordinamento in materia di protezione dati. Nasce così il Codice privacy (d.lgs. 196 del 2003), riconosciuto anche dalla Corte costituzionale come corpus organico di norme di derivazione europea (sentenza n. 271 del 2005).

Questa è, dunque, la fase che potremmo definire dell'affiancamento della protezione dati dalla riservatezza e, dunque, della declinazione della privacy sia nella sua accezione più classica che in quella più moderna di tutela dei contenuti informazionali dell'individuo. Il concetto di dignità della sfera personale si affianca man mano a quello di libertà, finora nettamente prevalente nell'ottica classica delle libertà negative (se si accentua la lettura datane dalla Corte costituzionale italiana, come già detto, tradizionalmente più incentrato sul concetto di diritto personale incardinato sull'articolo 2 Cost.).

Un *modus operandi* del diritto stesso che, nel suo progressivo affermarsi, si è vieppiù allontanato dall'originario *right to privacy* quale *right to be let alone*, prima manifestazione dell'esigenza di tutela della sfera privata personale. Non più uno *ius excludendi alios*, una difesa passiva e statica dalle ingerenze altrui, bensì il riconoscimento in capo agli individui di un potere autonomo, attivo e dinamico di scegliere quale ambito di circolazione riconoscere alle informazioni di carattere personale che li riguardano: il cd. potere di autodeterminazione informativa.

Oggi per tutela dei dati personali intendiamo, dunque, il diritto all'autodeterminazione informativa, inteso quale potere del singolo di decidere quale parte di sé, sotto forma di informazioni, far conoscere agli altri, decidendo altresì chi debbano essere i destinatari, per quali fini e con quali modalità e limiti.

Un diritto intimamente connesso alla salvaguardia della dignità della persona intesa quale valore indisponibile fondante lo Stato costituzionale, su cui deve essere costruita ogni operazione di bilanciamento che coinvolga la protezione dei dati personali.

Una evoluzione certamente spinta dall'innovazione tecnologica che, se ha portato all'uomo nuovi orizzonti di sviluppo del benessere, ha prodotto anche nuove e sempre più sofisticate tecniche di raccolta, conservazione, consultazione e manipolazione delle informazioni attraverso sistemi automatizzati di archiviazione e trattamento dati.

Tanti gli interrogativi che questi scenari aprono all'interprete: a rischio sono la lesione della dignità dell'uomo e del principio di non discriminazione.

Alla libertà di pensiero, di scelta e di azione in maniera difforme e non massificata, su cui è costruita la società liberaldemocratica, si contrappongono il controllo, l'omologazione e uniformazione dei comportamenti: il caso Facebook-Cambridge Analytica, solo per citare il caso, forse, più conosciuto, rappresenta una sintesi di come stiano cambiando anzitutto i paradigmi sociali.

È la rete, insomma, unitamente alla enorme diffusione dei *social,* a caratterizzare la circolazione delle informazioni, con una facilità di produzione ed una velocità inimmaginabile anche solo nel recente passato e con le enormi potenzialità future.

Un numero progressivamente crescente di persone fa uso dei *social networks* (in Italia l'ultimo rapporto del Censis ci dice che oltre il 35% della popolazione si informa *online*), divenendo con ciò destinatari di un flusso continuo di notizie ed immagini che scorrono sugli schermi dei dispositivi ma, al contempo, essi stessi produttori e comunicatori. Chiunque, infatti, attraverso il semplice utilizzo di un *personal computer* o di uno *smartphone,* può caricare in rete contenuti capaci di raggiungere un numero incalcolabile, potenzialmente indeterminabile, di utenti.

In questo panorama complesso e dai confini incerti, si può affermare che la privacy nell'era digitale è tutelata soprattutto grazie agli sforzi di due principali circuiti istituzionali, attivi sempre in ambito europeo: da una parte la Corte di Giustizia dell'Unione europea, che nelle sue più recenti decisioni in materia di *data protection* nel mondo digitale ha considerato la tutela della privacy come prevalente rispetto ad una serie di interessi pubblici, costruendo tale prevalenza sugli articoli 7 e 8 della Carta dei diritti fondamentali dell'UE (*Digital rights, Google Spain, Schrems e Tele2 Sverige*); dall'altra le istituzioni che partecipano del procedimento legislativo ordinario ovvero Commissione, Parlamento e Consiglio. Queste hanno non solo approvato il regolamento generale 679/2016, ma anche due nuove direttive in materia di trattamento dati e stanno ripetendo l'operazione già attuata in termini generali sul nuovo regolamento anche in materia di privacy elettronica. Strumenti normativi al passo con i tempi per governare, senza eccessivi appesantimenti burocratici, un mondo nuovo.

Per altro verso le sentenze della Corte di Giustizia emesse tra il 2014 e il 2016 rappresentano uno snodo davvero rilevante nella definizione del diritto alla protezione dati, per una serie di motivi.

In primo luogo si tratta di decisioni in cui prevale la visione di una privacy forte, in grado di prevalere su interessi pubblici anche di notevole portata (la prevenzione e il contrasto del crimine organizzato e del terrorismo) e su interessi privati (la libera attività commerciale svolta dai motori di ricerca), qualora le limitazioni apportate alla privacy stessa non siano improntate al rispetto del principio di proporzionalità e necessità.

In secondo luogo la Corte in tutte queste decisioni sembra accentuare in maniera significativa il ruolo della Carta dei diritti fondamentali dell'Unione europea (va specificato: nella versione consolidata del 2007 e non in quella originaria) come parametro di validità degli atti di diritto derivato. Una valorizzazione che è stata giuridicamente possibile per via di un importante fattore ovvero la scelta di elevare la Carta dei diritti fondamentali al rango dei Trattati istitutivi (nuovo articolo 6 del TUE, così come modificato dal Trattato di Lisbona).

In questo contesto, i giudici di Lussemburgo fondano sul combinato disposto degli articoli 7 e 8 della Carta di Nizza il «diritto fondamentale al rispetto della vita privata con riguardo al trattamento dei dati personali», declinando così assieme i due elementi costitutivi della privacy (Sentenza *Schrems* del 6 ottobre 2015, ma anche, in maniera leggermente diversa, *Digital Rights Ireland* dell'8 aprile 2014, par. 48).

Il secondo rilevante fattore di cambiamento origina anch'esso nelle scelte compiute nel 2007 in merito alla riforma dei Trattati. L'articolo 16 del Trattato sul funzionamento dell'Unione europea (Tfue), così come modificato dal Trattato di Lisbona, prevede espressamente una competenza dell'Unione in materia di disciplina sulla *data protection*. Pur ponendo comunque il limite competenziale «dell'esercizio di attività che rientrano nel campo di applicazione del diritto dell'Unione», l'articolo, inserito nelle disposizioni

generali iniziali, configura chiaramente una competenza legislativa dell'Unione in materia di protezione dati.

È su questa base giuridica – più solida e certamente più ampia del già citato art. 100 A del TCE – che la Commissione europea ha fondato la sua proposta di regolamento generale in materia di protezione dati che va a sostituire e, dunque, ad abrogare per intero, la direttiva del 1995 (*Regolamento n. 679 del 2016*, pubblicato in gazzetta ufficiale il 4 maggio 2016 ma che ha trovato completa applicazione a decorrere dal 25 maggio 2018).

Questo promesso, e prima di entrare nello specifico dell'analisi dei contenuti della disciplina in materia di diritti e garanzie degli interessati, occorre svolgere alcune considerazioni che, sia pur di carattere generale, risultano indispensabili al corretto svolgimento e piena comprensione delle nostre riflessioni.

Anzitutto, non va dimenticato che la direttiva del 1995, calata nel pieno del processo di integrazione europea e di trasformazione delle Comunità in Unione, si poneva quale punto di bilanciamento tra l'esigenza di abbattere gli ostacoli alla libera circolazione all'interno del continente e la necessità di proteggere le persone da una dispersione incontrollata di dati personali. Il Regolamento conferma il binomio circolazione-protezione dei dati personali, scommettendo sulla possibilità di individuare un punto di equilibrio più avanzato, in grado di tenere conto degli scenari tecnologici, economici, commerciali e geopolitici di oggi (e di domani).

E tra gli scenari di cui tiene conto vi è anche il rinnovo dell'intera cornice costituzionale, con la consacrazione della tutela della persona fisica (e della sua dignità) in quanto tale tra gli obiettivi primari dell'Unione e l'abbandono dell'antica visione prettamente legata alla promozione dell'*homo oeconomicus*.

Approdo a un approccio più "umanista" certamente legato anche al fondamentale apporto dato negli anni dalla Corte di giustizia dell'UE, tramite le pronunce che, soprattutto a partire dal 2014, hanno reinterpretato, riscritto e finanche invalidato le regole di diritto positivo: sono le già ricordate sentenze Digital Rights Ireland, Google Spain, Schrems, Weltimmo**,** e Tele2 Sverige e Schrems II che, nello stabilire principi circa la conservazione dei dati di traffico per finalità di giustizia, la deindicizzazione di risultati dai motori di ricerca, l'individuazione di competenze in capo alle Autorità europee su trattamenti transfrontalieri, l'inadeguatezza degli accordi Usa-Ue sui trasferimenti al di fuori dell'Unione, hanno contribuito alla definitiva costituzionalizzazione del diritto alla protezione dei dati personali nel sistema europeo.

Vi è poi la chiara volontà del legislatore europeo nell'orientarsi verso lo strumento regolamentare. Se nel 1995 era sufficiente armonizzare discipline di carattere nazionale, a fronte della frammentazione che tale processo ha provocato, oggi l'esigenza è stata quella di uniformare l'intero *corpus* normativo, ponendo delle regole di immediata e diretta applicazione nei confronti di tutti gli europei, siano essi persone fisiche, imprese od enti pubblici. Purtuttavia, il Regolamento non ha mancato di lasciare consistenti spazi di intervento ai singoli Stati membri, al fine tanto di dare attuazione ad alcuni ambiti tradizionalmente di competenza dello Stato (si pensi alla definizione di apposite sanzioni penali) quanto di specificare o integrare disposizioni di livello più generale, pur nel rispetto di un quadro di limiti e garanzie a presidio del contenuto essenziale del diritto (si pensi alla statuizione per legge di adeguati presupposti di liceità per un'ampia sfera di trattamenti).

Un quadro normativo complesso che muove nella direzione di un rafforzamento importante del piano delle tutele offerte agli interessati.

Il nucleo di questa disciplina aveva rappresentato la vera "rivoluzione" apportata dalla direttiva (CE) 95/46, a partire dall'affermazione del principio del consenso

informato quale strumento cardine per la realizzazione dell'autodeterminazione informativa e dall'introduzione di una serie di diritti (accesso, aggiornamento, integrazione, cancellazione, opposizione) che la persona può direttamente azionare prima nei confronti del titolare del trattamento e poi eventualmente dinanzi al Garante (o al giudice).

Con il Regolamento questi istituti non solo vengono confermati, ma soprattutto sono oggetto di un processo di consolidamento.

Si assiste ad un sensibile ampliamento dei concetti di dato personale (art. 4, n. 1) e di particolare categoria di dato (i vecchi dati sensibili, tra cui oggi si riconoscono anche dati genetici e dati biometrici: art. 9); viene incrementato il livello di trasparenza dei trattamenti (artt. 13 e 14), mentre il consenso si rafforza come presupposto e come garanzia, anche considerando modalità di espressione più chiare, ma anche semplificate, e la possibilità di un consenso autonomo per i minori che si raffrontano con i servizi web (artt. 6-9); aumenta il novero dei diritti dell'interessato, con l'ingresso dei diritti all'oblio e alla portabilità e la declinazione del diritto all'opposizione rispetto ai processi automatizzati (rispettivamente, artt. 17, 20 e 22).

È una impostazione che, peraltro, intende uscire dalla logica del mero adempimento formale agli obblighi di legge, per approdare ad un cambiamento culturale importante, in cui la prima aspirazione per chiunque lavori su dati personali deve essere quella di ridurre, prevenendoli, i rischi di operazioni non consentite, o comunque non conformi.

I titolari dovranno individuare loro stessi le soluzioni maggiormente compatibili con il quadro normativo, svolgendo una valutazione (dinamica) di impatto privacy, rivolgendosi all'Autorità solamente allorché gli effetti sui diritti degli interessati siano connotati da gravità e probabilità.

A muovere le scelte del titolare, sarà sicuramente il suo interesse legittimo, che però dovrà essere necessariamente bilanciato con l'attenzione alla tutela dei diritti e delle libertà delle persone i cui dati utilizza.

Un bilanciamento che il titolare dovrà svolgere nella consapevolezza della responsabilità che porta con sé.

Una tutela, dunque, anticipata ad un momento antecedente all'avvio del trattamento, che chiama in causa direttamente la responsabilità dei titolari in una prospettiva di approccio basato sul rischio, sulla sua valutazione e gestione. Una valutazione dinamica, nel senso che questa non dovrà esaurirsi *una tantum*, ma dovrà accompagnare costantemente l'attività del titolare, aggiornando e rivedendo le fasi del processo di gestione del dato.

Il tutto nella prospettiva della minimizzazione del dato, cioè l'utilizzo di informazioni di carattere personale che sia effettivamente proporzionato alla reale necessità: questo è un principio cardine della *data protection* da quando questa è diventata una cornice valoriale per l'intero continente europeo.

Il concetto di responsabilizzazione del titolare ha dunque una duplice valenza: adottare tutte le misure utili a prevenire atti e comportamenti su dati personali che possano impattare sugli interessati; documentare quanto fatto in chiave probatoria, a fronte di violazioni effettive o comunque di controlli dell'Autorità.

Un profilo speculare alla tutela dei diritti dell'interessato che accentua i doveri del titolare e che risponde al principio di *accountability*.

Occorre poi considerare che le garanzie a tutela del diritto alla protezione dei dati personali diventano applicabili a chiunque fornisca servizi sul territorio europeo. Diventa cioè recessivo il criterio dello stabilimento su cui era costruito il precedente impianto e che già la Corte di Lussemburgo negli ultimi anni aveva riletto in un'ottica più aperturista,

a favore invece del criterio del *targeting,* ossia privilegiando il luogo in cui si trova il destinatario del servizio superando, in questo modo, gli ostacoli causati dall'a-territorialità della rete e dall'extra-territorialità dei più grandi operatori mondiali.

Ciò, peraltro, avendo ben chiara la conferma di un'impostazione finalizzata a incentivare tanto la libera circolazione dei dati personali anche al di fuori dell'Unione – in una logica di libertà di scambio e di mercato senza barriere – quanto la garanzia di un elevato livello di tutela delle persone fisiche presenti del territorio comunitario trattati nel contesto di un'attività economica.

In questo senso, molto più complessa e difficile sarà la riflessione sulla bontà, in termini di efficacia e di effettiva tutela, del punto di bilanciamento proposto dalla nuova disciplina. In altri termini, se le scelte e le innovazioni introdotte dal regolamento rappresentano il più avanzato *point of balance*, sarà compito dell'interprete stabilire fino a che punto le scelte compiute saranno in grado di centrare gli obiettivi indicati, anche alla luce, come già si accennava, dei margini di attuazione lasciati agli Stati membri.

Ciò, ancor più, in un panorama che ha prodotto sbilanciamenti anche significativi a favore della acquisizione/circolazione dei dati rispetto ai soggetti privati, se solo pensiamo alle crescenti emergenze per ragioni di sicurezza.

Lasciando ad un'altra occasione l'approfondimento di aspetti che ci si è limitati a segnalare, occupiamoci di come il legislatore ha scelto di rafforzare le conquiste sul piano delle tutele degli interessati.

Questo è avvenuto in più modi: certamente, ed in primo luogo, ampliando la nozione di dato personale in maniera tale da ricomprendervi sempre più tipologie di trattamento; confermando la centralità dell'istituto del consenso e arricchendone di contenuto la definizione normativa; consolidando la scelta di attribuire alle persone diritti immediatamente azionabili (prima nei confronti del titolare, poi davanti al giudice o all'Autorità di controllo); ampliando il novero dei diritti stessi, tramite una migliore specificazione di diritti già esistenti (ad esempio, con l'opposizione al trattamento) e una decisiva opera di innovazione (pensiamo all'oblio o alla portabilità dei dati); superando una nozione statica di stabilimento; rafforzando, anche in un'ottica di costante coordinamento, il ruolo delle Autorità di controllo dei Paesi membri.

Il perseguimento della garanzia di un elevato livello di tutela e il rafforzamento del sistema dei diritti attraversa, anzitutto, la nozione stessa di dato personale in relazione alle informazioni che identificano o rendono identificabile una persona.

Rispetto ai confini segnati dalla direttiva 95/46/CE, la protezione si estende, infatti, a tutti i dati che di per sé o a seguito di combinazione con altre informazioni possono condurre alla identificazione di una persona fisica, quali i dati relativi all'ubicazione e gli identificativi *online* (art. 4, comma 1, lett. a) GDPR), mutuando e formalizzando così una prassi già da tempo consolidata da parte delle Autorità di protezione dati europee.

Una nozione già così ampia di dato personale, che pure tende ad espandersi ulteriormente se si leggono le indicazioni interpretative – giuridicamente non vincolanti – contenute nei considerando. In questa direzione si rileva che, per determinare se una persona sia identificabile, è opportuno valutare «tutti i mezzi, come l'individuazione, di cui il titolare del trattamento o un terzo può ragionevolmente avvalersi per identificare detta persona direttamente o indirettamente» (*considerando* 26); aggiungendo poi che gli individui potrebbero essere associati con identificativi on line forniti dai loro dispositivi come indirizzi IP, marcatori temporanei (*cookies*) ovvero *tag* di identificazione o radiofrequenza (*Rfid tags*).

Si tratta, dunque, di una nozione con funzione di onnicomprensività e capacità di attrarre nuove situazioni, non prevedibili né previste *ex ante* da parte del legislatore. Poche

materie come questa, d'altra parte, necessitano di una flessibile commistione tra definizioni elastiche e, ove occorre, successivi interventi di dettaglio.

Sempre in quest'ottica viene ridefinita la (categorie particolari di dati personali) categoria dei dati sottoposti a una tutela rafforzata (art. 9).

In primo luogo si riconoscono definitivamente i dati biometrici e genetici quali dati aventi natura sensibile. Il Codice privacy e l'applicazione datane dal Garante italiano nel corso del tempo hanno consentito di elevare il livello delle garanzie che circondano queste tipologie di dati, innalzandoli al di sopra di quelli che vengono solitamente definiti come dati personali "comuni": ci si riferisce, in particolare, all'obbligo di notificazione dei trattamenti al Garante, che accomuna entrambi (art. 37, comma 1, lett. a), del Codice), all'obbligo di sottoporre i trattamenti biometrici a verifica preliminare, nonché alle procedure relative alla autorizzazione del Garante per il trattamento dei dati genetici per finalità di salute e ricerca scientifica (art. 90 del Codice).

Il legislatore europeo riconosce ora la specificità di queste tipologie di informazioni, soprattutto alla luce dei progressi tecnologici che hanno creato sistemi sempre più avanzati e certi di identificazione delle persone, impiegati per le più varie finalità tanto in ambito privato (si pensi all'utilizzo sempre più raffinato di elementi corporei per mere finalità di accesso a luoghi fisici), quanto nel settore pubblico (in particolare si registra un incremento dell'utilizzo del Dna per il contrasto al crimine e al terrorismo nell'ambito dei trattamenti di polizia).

Non solo dati biometrici e genetici assurgono a dati sensibili, ma essi addirittura effettuano un "doppio salto", nel senso che, al pari dei dati sulla salute (dati ormai definiti "supersensibili"), possono essere destinatari di un corredo di garanzie ancora più robuste ad opera delle leggi nazionali, in virtù della clausola di cui al comma 4 dell'art. 9. E per quanto riguarda proprio i dati sulla salute, il Regolamento consegna un ulteriore ampliamento della definizione, e quindi dell'ambito di tutela, laddove fa rientrare nella categoria anche «prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute» (art. 4, comma 1, n. 15): in questo modo, qualsiasi evento che comporti una prestazione di carattere sanitario trova una tutela rafforzata, a prescindere dal fatto che questa riveli una situazione patologica.

Altrettanto rilevante, ma in parte più complessa, la riflessione sulla funzione del consenso, istituto centrale nella costruzione del diritto alla protezione dei dati quale autodeterminazione informativa, riaffermato e rafforzato nella nuova disciplina e, anzi, accompagnato, ai doveri di informazione e trasparenza posti a carico del titolare o responsabile del trattamento e, ancor più, declinato anche con riguardo alla tutela di particolari figure soggettive (così i minori) ed a particolari tipologie di trattamento dati (proprio quelli sensibili e biometrici). Nella stessa logica certamente si inserisce la previsione della revocabilità e dell'esclusione di ogni forma di consenso tacito.

L'interrogativo è quanto consapevolezza e potere di disposizione libera garantiscano un adeguato equilibrio tra le ragioni del soggetto interessato e quelle di chi incide con la propria attività sulla serie degli interessi protetti. Su quanto, in altri termini, lo schema informativa/consenso sia realmente efficace alla protezione dei dati personali, se solo pensiamo alle tecniche di profilazione, al *datamining* e alla *dataveillance*. Dubbi cui il Regolamento (per la verità in assenza di proposte alternative) risponde orientando le proprie scelte sul versante di modalità applicative mirate ad ottenere maggiore effettività ed efficacia dello stesso.

Peraltro, non appare estranea alla ricerca di soluzioni se non alternative certamente compensative delle carenze del consenso, un impianto normativo che, ad un approccio riparatorio, sostituisce una logica di tutela preventiva, che utilizza gli strumenti della

valutazione di impatto sulla protezione dei dati personali e della protezione sin dalla progettazione e per impostazione predefinita.

Venendo ora al piano dei diritti, come già ricordato, le scelte normative compiute dal legislatore europeo si inseriscono nel solco di una particolare attenzione ai diritti e alla necessità di un loro rafforzamento ed ampliamento.

La Direttiva 95/46/CE aveva individuato un meccanismo di tutela dei diritti dell'interessato che, avvicinandosi al modello conciliativo e di risoluzione extragiudiziale delle controversie, ha posto in diretto collegamento i due principali soggetti coinvolti nelle attività di trattamento dati, ovverosia l'interessato e il titolare: l'art. 12 della Direttiva consentiva all'interessato di ricevere dal titolare tutte le informazioni relative al trattamento dei propri dati, nonché richiedere eventuali interventi inibitori o modificativi su di essi ("rettifica", "cancellazione", "congelamento").

Il recepimento di tale indicazione da parte del legislatore italiano aveva così dato vita al procedimento del ricorso all'Autorità, uno strumento che ha dimostrato di assicurare efficacia, immediatezza e funzionalità nella risoluzione delle controversie sui diritti connessi alla protezione dati, fornendo quindi una soluzione alternativa all'ordinario contenzioso davanti al giudice (artt. 7-10 e artt. 145-151 del Codice).

Vi è da dire che lo specifico strumento del ricorso non era previsto nella Direttiva come non è, ad oggi, esplicitato all'interno del Regolamento.

Tuttavia, avendo il Regolamento confermato il principio della interlocuzione diretta tra interessati e titolari (art. 12) e avendo «fatto salvo ogni altro ricorso amministrativo o extragiudiziale disponibile, compreso il diritto di proporre un reclamo ai un'Autorità di controllo ai sensi dell'art. 77» (art. 79), nella fase di attuazione del Regolamento, si sono trovati, nell'ambito del regolamento interno del Garante, termini e modalità procedimentali semplificate che tengono conto della passata esperienza.

Sempre in questa stessa direzione, si ampliano e specificano meglio gli strumenti dell'autodeterminazione informativa.

Vengono anzitutto riaffermati il diritto di accesso ai propri dati (art. 15), il diritto di rettifica (art. 16), il diritto di cancellazione (art. 17), il diritto di limitazione (con una connotazione parzialmente differente rispetto al previgente diritto di chiedere il blocco dei dati: art. 18), il diritto di opposizione (art. 21).

Si introduce per la prima volta il diritto alla portabilità dei dati (art. 20) che sostanzialmente si traduce in due nuove facoltà per l'interessato: il diritto di ricevere un sottoinsieme dei dati personali e il diritto di trasmettere dati personali da un titolare a un altro titolare senza impedimenti. Si tratta di un diritto che in parte ricorda e specifica, per il settore dei servizi, il diritto di accesso ai dati personali; la sua positivizzazione però richiama l'intento dell'UE di facilitare il percorso verso la creazione del mercato unico digitale.

Per altro verso, occorre sottolineare che alla disposizione relativa all'opposizione al trattamento dei propri dati personali si salda la previsione di uno specifico diritto all'opposizione all'attività di profilazione (art. 22), da leggere, peraltro, in connessione logico-sistematica con il diritto alla limitazione al trattamento e al diritto alla portabilità, da intendere correttamente quale declinazione del principio della interoperabilità già adottato nell'ambito delle comunicazioni elettroniche.

Si tratta senza dubbio di una consapevole scelta di ampliamento della tutela legata al progresso tecnologico e informatico e, come già osservato, ad una progressiva espansione e diffusione dell'uso di internet quale strumento essenziale per la vita quotidiana. Una codificazione giusta e opportunamente garantista se si considera che la profilazione online rappresenta una delle principali modalità attraverso cui si alimentano

i *Big data*, per scopi finali che possono attenere alla ricerca di una collocazione professionale, all'individuazione di una fetta di elettorato da convincere, alla classificazione di "buoni" e "cattivi" pagatori, o, più banalmente, a marketing individualizzato.

Ma l'obiettivo dell'autodeterminazione informativa trova una sponda fondamentale nella scelta di positivizzare gli orientamenti della Corte di giustizia. È così che, applicando i principi espressi nella sentenza *Google Spain*, il legislatore europeo ha rielaborato il diritto dell'interessato a controllare e disporre dei propri dati, arricchendolo con l'introduzione del diritto all'oblio all'interno del più generale diritto di cancellazione e, a sua volta, logicamente correlato al diritto di rettifica, precedentemente citati all'interno dell'art. 12, lett. b), della Direttiva 95/46/CE.

La connessione con il diritto alla cancellazione sembrerebbe ampliare i confini del diritto all'oblio così come elaborato dalla giurisprudenza, fuoriuscendo dal recinto della sua originale connotazione di diritto alla deindicizzazione (o alla rimozione della *url*) dai risultati di una ricerca effettuata su un motore di ricerca generalista a partire da parametri di ricerca il nome e cognome di una persona fisica. L'effetto però sarebbe estremamente più impattante sul contrapposto interesse alla memoria collettiva (o alla ricerca storica), poiché deindicizzare dai motori di ricerca generalisti significa che il contenuto rimarrebbe comunque disponibile sul sito fonte, costringendo il ricercatore a effettuare con uno sforzo maggiore un'indagine specificamente al suo interno; al contrario, cancellare tale contenuto direttamente dal sito fonte significa eliminare del tutto dalla rete l'informazione, privando così gli utenti del web di un frammento di conoscenza.

Proprio in ragione di queste implicazioni si può prevedere come l'applicazione del diritto all'oblio di cui all'art. 17 del Regolamento si giocherà – ancora più che in passato quando lo statuto dell'oblio era rimesso alla sola interpretazione giurisprudenziale – sul margine di estensione dei limiti, che sono quelli citati dal comma 3 della medesima disposizione, messi a sistema con quelli indicati dal considerando 73.

Quelle appena richiamate non rappresentano le uniche innovazioni apportate dal Regolamento. Così, sul piano dell'ambito di applicazione territoriale, e sulla scorta della nota giurisprudenza della Corte di giustizia (vedi le sentenze *Google Spain* e *Weltimmo*), il legislatore approda al superamento del criterio di stabilimento posto a fondamento della Direttiva (art. 3). Ora la regola è che vengono disciplinati dal Regolamento, e quindi assoggettati al controllo da parte delle Autorità europee, tutti i trattamenti svolti sui dati di chi si trova in Europa, anche se questi siano effettuati da titolari extra-UE e/o presso sedi extra-UE: ciò purché questi trattamenti attengano l'offerta di beni o la prestazione di servizi, oppure il monitoraggio dei comportamenti. Il principio di stabilimento così ridefinito (cd. principio del *targeting*), opta per una soluzione maggiormente garantista per gli interessati, ponendo al centro gli individui e rendendo, di fatto e di diritto, perseguibili le grandi aziende del web e dell'*Information and communication technologies* (ICT), le quali a fatica potranno, in futuro, celarsi dietro l'a-territorialità della rete.

Tutti i profili finora trattati (il rafforzamento dei diritti e la ridefinizione della territorialità, cui si aggiunge anche la responsabilizzazione dei titolari già richiamata) convergono verso la creazione di un sistema istituzionale in grado di garantire al meglio l'evocato bilanciamento tra circolazione e protezione del dato personale.

La Direttiva madre aveva disposto l'istituzione, all'interno di ciascuno Stato membro, di Autorità di vigilanza sull'effettività della protezione dei dati personali (art. 28). Nel corso degli anni queste si sono rivelate decisive non solo nell'attività di controllo ma anche in una più generale funzione quasi pedagogica di diffusione della cultura dei diritti e del diritto alla protezione dati in particolare.

La considerazione dell'importanza di tali attribuzioni e la buona prova di sé che le Autorità istituite dopo la Direttiva hanno dato, certamente ha contribuito alla scelta di inserire un esplicito riferimento a tali soggetti istituzionali nel *comma* 3 dell'art. 8 della Carta di Nizza (uniche Autorità indipendenti a trovare precisa ed esplicita collocazione all'interno della Carta dei diritti fondamentali dell'Unione europea), ma anche nell'art. 16 TFUE.

Sulla scorta di ciò il legislatore regolamentare era chiamato a fare un passo in più. L'omogeneizzazione in tutta l'UE del sistema di protezione dati richiedeva che anche l'apparato istituzionale che sovrintende tale sistema fosse il più uniforme possibile, altrimenti si sarebbe vanificata la tutela stessa. La direzione intrapresa è stata pertanto quella di una più stretta integrazione e collaborazione tra le Autorità dei singoli Paesi membri.

Su tutti, si pensi al meccanismo dello sportello unico per le imprese (*one-stop-shop*), in base al quale, in caso di trattamenti intercontinentali, un'azienda si rivolge ad una sola Autorità, quella collocata presso la sede di stabilimento principale (art. 56).

Una grande sfida sarà realizzare questo modello di cooperazione, considerato che ci si confronta con panorami giuridici e metodologie di lavoro comunque diversi; ma, risalendo ancora più a monte, da culture non sempre conciliabili, nonché barriere linguistiche da non sottovalutare. Se fino ad ora ci si era abituati a istruire procedimenti tenendo conto di leggi e prassi interne, oltre che delle indicazioni provenienti da ulteriori organismi e giudici di vario livello, ora ci dovremo necessariamente confrontare con procedimenti transnazionali e con approcci ontologicamente diversi, all'interno di un quadro giuridico europeo ancora da decifrare fino in fondo. Si apre l'era del dialogo tra le Autorità come regola.

In ogni caso, questo sistema continuerà a reggersi sul requisito fondamentale ed ineliminabile che appartiene alle Autorità: si tratta cioè dell'indipendenza rispetto al potere politico, e quindi dal potere esecutivo che ne rappresenta la sintesi sul piano dell'indirizzo. La scelta di affidare la *governance* del *data protection* a questo tipo di organismi risale nel tempo, alla Direttiva 95/46: essa affonda le proprie radici nell'esigenza di emancipare il pieno esercizio di un diritto fondamentale, espressione diretta della dignità personale, dalle scelte del vertice politico-amministrativo, considerato che quest'ultimo è il titolare degli archivi, contenenti anche dati sensibili in molti casi, esistenti (si pensi anche solo alle anagrafi, al sistema fiscale-tributario, al servizio sanitario, al casellario giudiziale, alle banche dati di polizia, ecc.). Pertanto, l'indipendenza rimane un cardine cruciale su cui fondare il nuovo quadro europeo della vigilanza.

A ciò si connette la previsione di un quadro sanzionatorio amministrativo comune (art. 83). La costruzione esplicita di un apparato repressivo che abbia al vertice l'Autorità funge da portato fisiologico (o naturale contrappeso) della scelta della responsabilizzazione del titolare. Infatti, lasciare un ampio margine di discrezionalità nelle scelte organizzative e tecnologiche del titolare comporta logicamente che un cattivo uso di tale autonomia debba essere severamente sanzionato. In questo modo l'*accountability* elimina gli alibi: e una corretta rendicontazione delle azioni messe in campo non può che spingere il titolare del trattamento a confrontarsi con l'Autorità nella consapevolezza di essersi comportato in maniera perfettamente *compliant*. L'abbandono della logica dell'adempimento in favore di una meditata tensione verso il risultato (cioè lo svolgimento di trattamenti nella massima garanzia per gli interessati) d'altra parte non può che pretendere una piena assunzione di responsabilità, anche in termini di valutazione delle conseguenze delle scelte effettuate.

Cultura giuridica e diritto vivente

Cultura giuridica e diritto vivente - Rivista scientifica riconosciuta dall'ANVUR ai fini dell'ASN - è espressione del Dipartimento di Giurisprudenza (DiGiur) dell'Università di Urbino. Lo sviluppo e la manutenzione di questa installazione di OJS sono forniti da UniURB Open Journals, gestito dal Servizio Sistema Bibliotecario di Ateneo. **ISSN 2384-8901**