Principi e contenuti del Regolamento UE 2016/679 in materia di protezione dei dati personali

di Licia Califano [*]

Sommario: 1. La matrice europea del diritto alla protezione dei dati personali e la scelta dello strumento *self executing*. – 2. I principi ispiratori e le principali novità contenutistiche del Regolamento. – 2.1. Il rafforzamento del sistema dei diritti e il quadro delle garanzie. – 2.2. La responsabilizzazione del titolare. – 2.3. Il ruolo delle Autorità di controllo. – 2.4. Il regime sanzionatorio e delle responsabilità. – 3. Le sfide presenti e future. Riflessioni conclusive.

1. – La direttiva 95/46/CE nasce, come noto, con l'obiettivo di conciliare due interessi apparentemente contrastanti: da una parte, la rimozione degli ostacoli alla circolazione dei dati personali, necessaria alla piena realizzazione del mercato interno, dall'altra, l'esigenza di apprestare garanzie idonee a salvaguardare i diritti fondamentali della persona. L'eliminazione degli ostacoli alla libera circolazione dei dati personali presuppone la creazione di un livello equivalente di protezione dei diritti delle persone relativamente al trattamento dei dati medesimi.

La collocazione sistematica della tutela dei dati personali nell'alveo dei diritti fondamentali della persona, in coerenza con l'elaborazione dottrinale e giurisprudenziale maturata nei Paesi dell'Unione, si deve alla Carta dei diritti fondamentali dell'Unione europea del 2000 (la c.d. Carta di Nizza), che ricomprende il diritto alla protezione dei dati personali all'art. 8, subito dopo la disposizione dedicata al rispetto della vita privata e familiare (art. 7). Sul piano formale, la successiva incorporazione della Carta di Nizza nei Trattati istitutivi, ad opera del Trattato di Lisbona del 2007, ha attribuito alla prima il medesimo valore giuridico dei secondi, contribuendo al contempo ad innalzare il rango della stessa disciplina contenuta nella direttiva.

Passando invece al piano sostanziale, è la natura giuridica del diritto alla tutela dei dati personali quale diritto del singolo all'autodeterminazione informativa a non poter mai prescindere dalla salvaguardia della dignità della persona intesa quale valore costituzionale (o, forse meglio, supercostituzionale) indisponibile [1].

---

[*] Componente del Garante per la protezione dei dati personali, Professore ordinario di Diritto costituzionale dell'Università degli Studi di Urbino.

[1] Per un approfondimento sulla costruzione del diritto fondamentale alla protezione dei dati personali, mi sia consentito un rinvio al mio *Il Regolamento UE 2016/679 e la costruzione di un modello uniforme di*

Il percorso di costruzione del diritto alla protezione dei dati personali si intreccia con il crescente sviluppo dell'innovazione tecnologica delle comunicazioni elettroniche alla base della nostra società digitale e della globalizzazione delle relazioni interpersonali, economiche, finanziarie e sociali. Sempre di più si pone oggi, e si porrà in futuro, la questione della difesa da una raccolta, utilizzazione e indiscriminata circolazione delle informazioni che ci riguardano. E la complessità e quantità delle problematiche sottese di ordine costituzionale, che il trattamento dei dati personali nel web pongono all'interprete, riguarda non più il solo versante del rapporto fra individuo e potere pubblico, coinvolgendo i protagonisti della rete, a partire dai grandi motori di ricerca [2].

Le profonde innovazioni tecnologiche e il trattamento dati nell'ambito delle comunicazioni elettroniche sono stati oggetto della più recente e rilevante giurisprudenza della Corte di giustizia [3]. Il riferimento è alle pronunce *Digital Rights Ireland* [4], *Google Spain* [5], *Schrems* [6] e *Tele2 Sverige* [7]. Sembra di poter leggere in queste sentenze una evoluzione della tecnica decisoria del bilanciamento giudiziale tra diritti. Difatti, la Corte parte dal presupposto di una centralità della protezione dei dati personali, la cui portata come

---

diritto europeo alla riservatezza e alla protezione dati personali, in 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*, Napoli, Editoriale Scientifica, 2017, 3 ss.

[2] Cfr. F. Balducci Romano, *La protezione dei dati personali nell'Unione europea tra libertà di circolazione e diritti fondamentali dell'uomo*, in *Riv. it. dir. pubbl. com.*, 2015, 1623 ss.

[3] Su tutta questa giurisprudenza, cfr., fra i tanti: G. Finocchiaro, *La giurisprudenza della Corte di giustizia in materia di dati personali da* Google Spain *a* Schrems, in *Dir. inf.*, 2015, 779 ss.; F. Pizzetti, *Le Autorità garanti per la protezione dei dati personali e la sentenza della Corte di giustizia sul caso Google Spain: è tempo di far cadere il "velo di Maya"*, in *Dir. inf.*, 2014, 805 ss.; O. Pollicino, *Diritto all'oblio e conservazione dei dati. La Corte di giustizia a piedi uniti: verso un* digital right to privacy, in *Giur. cost.*, 2014, 2949 ss.; G. Resta-V. Zeno-Zencovich (a cura di), *La protezione transnazionale dei dati personali: dal "Safe Harbour Principles" al "Privacy Shield"*, Roma, Roma TrE-press, 2016; M. Rubechi, *Sicurezza, tutela dei diritti fondamentali e privacy: nuove esigenze, vecchie questioni (a un anno dagli attacchi di Parigi)*, in *www.federalismi.it*, 2016, 23, 18 ss.; L. Scaffardi, *La Data retention va in ascensore*, in *Forum Quad. cost.*, 28 luglio 2017.

[4] CGUE 8 aprile 2014, C-293/12 e C-594/12, *Digital Rights Ireland*, con cui è stata dichiarata l'invalidità dell'intera direttiva 2006/24/CE sulla conservazione dei dati di traffico telefonico e telematico, dei dati relativi all'ubicazione e quelli necessari all'identificazione dell'abbonato (*data retention*), poiché lesiva del principio di proporzionalità.

[5] CGUE 13 maggio 2014, C-131/12, *Google Spain*, con la quale la Corte ha accordato a un cittadino spagnolo il diritto di richiedere e ottenere dal motore di ricerca Google, con riferimento alle ricerche ivi effettuate, la rimozione delle pagine ricavate a partire dal proprio nome e cognome.

[6] CGUE 6 ottobre 2015, C-362/14, *Schrems*, con la quale il giudice europeo ha invalidato l'accordo *Safe Harbour* del 2000, con cui la Commissione europea aveva riconosciuto la legittimità del trasferimento dei dati personali di cittadini europei da parte delle filiali europee delle grosse multinazionali statunitensi (come Facebook, nella vicenda in oggetto) verso le rispettive società madri, situate in territorio americano: in questo modo, tali dati si erano resi pienamente disponibili alle attività di sorveglianza continua da parte delle forze di sicurezza degli Usa, come lo scandalo c.d. *Nsa* ha dimostrato.

[7] Il tema del *data retention* ha ricevuto un secondo giudizio con CGUE 21 dicembre 2016, C-203/15 e C-698/15, *Tele2 Sverige*, quando ha inibito gli Stati membri dallo stabilire un obbligo generale e indifferenziato di conservazione dei dati di traffico degli utenti nei confronti dei fornitori di servizi di comunicazione elettronica.

diritto fondamentale può essere limitata solo in presenza di modalità strettamente proporzionali e necessarie al raggiungimento di fini legittimi di rilevante interesse pubblico [8].

Nello sviluppo logico-giuridico delle sentenze citate, i giudici si soffermano con decisione sulla collocazione sistematica della Carta dei diritti fondamentali, proprio alla luce della citata parificazione ai Trattati. La Corte pone così le premesse di un'opera di piena costituzionalizzazione del diritto alla protezione dei dati personali nel sistema UE, sempre più attento ai valori personalisti e ormai sempre più distante dalla logica economicista che ne aveva caratterizzato l'origine [9].

Il baricentro del diritto si sposta così sulla difesa della libertà e dignità della persona a fronte della espansione del controllo sull'acquisizione delle informazioni legate alle innovazioni tecnologiche che, come già detto, hanno introdotto tecniche di raccolta, conservazione e consultazione delle informazioni attraverso sistemi automatizzati di archiviazione e trattamento dati.

Tanti gli interrogativi che questi scenari aprono all'interprete: primo tra tutti l'impatto sull'insieme dei diritti e dei valori fondamentali dell'uomo. A rischio sono la lesione della dignità dell'uomo e del principio di non discriminazione; al controllo e all'omologazione e uniformazione dei comportamenti si contrappone la libertà di pensiero, di scelta e di azione in maniera difforme e non massificata [10].

È andata così maturando, in siffatto contesto storico, sociologico e, non da ultimo, giuridico la consapevolezza che fosse necessario ammodernare la disciplina *privacy*, con uno sforzo di omogeneizzazione ulteriore tra le normative statali che solo un atto regolamentare poteva assicurare.

La consapevolezza che fosse giunto il tempo di uniformare in Europa la disciplina *privacy*, superando i difetti del passato, veniva avvertita distintamente e il rafforzamento della base giuridica della *data protection* a seguito dell'entrata in vigore del Trattato di Lisbona ha costituito, al contempo, il presupposto e il volano dell'intervento riformatore.

Si giunge così al Regolamento UE 2016/679 in materia di protezione dei dati personali [11], approvato il 27 aprile 2016, pubblicato nella Gazzetta Ufficiale dell'UE il 4 maggio, ma che inizia ad esplicare pienamente i suoi effetti solamente a partire dal 25 maggio 2018 (art. 99, par. 2): due anni di sospensione dell'efficacia per consentire a

---

[8] In proposito, cfr. le riflessioni di V. Fiorillo, *Il principio di proporzionalità da parametro di validità a fondamento del diritto alla protezione dei dati personali nella recente giurisprudenza della Corte di giustizia dell'Unione europea*, in *www.federalismi.it*, 2017, 15, 16 ss.

[9] Come rilevato da M. Bassini, *La svolta della privacy europea: il nuovo pacchetto sulla tutela dei dati personali*, in *Quad. cost.*, n. 3/2016, 588, l'approccio delle istituzioni europee è passato «da una configurazione prevalentemente *market-driven* a una *fundamental rights-oriented*»; *amplius*, sul punto, O. Pollicino, *Un digital right to privacy preso (troppo) sul serio dai giudici di Lussemburgo? Il ruolo degli artt. 7 e 8 della Carta di Nizza nel reasoning di Google Spain*, in *Dir. inf.*, 2014, 573.

[10] Cfr. S. Rodotà, *Il diritto di avere diritti*, Bari, Laterza, 2013; G. Resta, *Dignità, persone, mercati*, Torino, Giappichelli, 2014.

[11] La dicitura completa è *Regolamento UE 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 (sulla tutela delle persone fisiche con riguardo al trattamento dei dati personali e alla libera circolazione di tali dati che abroga la Direttiva 95/46/CE).*

Stati, istituzioni, amministrazioni, imprese e cittadini di prendere confidenza con il nuovo impianto. Parimenti, a partire dalla medesima data è abrogata la direttiva del 1995, ormai interamente sostituita dal novello quadro regolamentare (art. 94) [12].

Il Regolamento, come ricordato anche nei primissimi *Considerando*, è stato concepito per dare attuazione alle disposizioni fondamentali contenute nelle fonti originarie, tanto nella Carta dei diritti fondamentali quanto nel TFUE. Vi è, dunque, una innegabile coerenza, tra la costituzionalizzazione del diritto alla protezione dati in ambito europeo (art. 8 della Carta) e il rafforzamento delle competenze dell'Unione (art. 16 TFUE) da un lato, e la scelta dello strumento regolamentare dall'altro. L'attuazione di un diritto fondamentale alla protezione dei dati personali non poteva che avvenire attraverso un atto legislativo in grado di raggiungere direttamente e indistintamente tutti gli individui che si trovano nell'Unione.

Un'opera di uniformazione normativa che, nella sua fase attuativa, lascia ambiti e spazi di manovra in capo ai singoli Stati membri, liberi così di «mantenere o introdurre norme nazionali, al fine di specificare ulteriormente l'applicazione del presente Regolamento», così come «di stabilire condizioni per specifiche situazioni di trattamento, anche determinando con maggiore precisione le condizioni alle quali il trattamento di dati personali è lecito» (*Considerando* n. 10).

Lo stesso testo del Regolamento può essere fonte di molti riferimenti utili da tenere presenti in fase di intervento statale, a partire dai numerosi *Considerando* che fungono da preambolo al testo regolamentare. Essi, infatti, vanno a configurarsi come contenuti di principio privi di carattere giuridico vincolante ma dotati di funzione ermeneutica, in grado di orientare l'applicazione dei precetti nel senso più conforme ai principi statuiti [13].

In altre parole, vi sono esplicite previsioni che mettono in evidenza non solo la liceità ma anche la necessità di taluni interventi correttivi da parte degli Stati membri, per rendere più effettiva la tutela del diritto e senza nulla togliere alla diretta applicabilità delle disposizioni contenute nel Regolamento, rispetto a quelle contenute nel corpus normativo proprio dei singoli Stati membri.

Una delle disposizioni più rilevanti in tal senso è rinvenibile all'interno dell'art. 6, par. 3, ove si statuisce che «il diritto dell'Unione o degli Stati membri persegue un obiettivo di interesse pubblico ed è proporzionato all'obiettivo legittimo perseguito».

---

[12] È doveroso aggiungere che il Regolamento fa parte di un "pacchetto *privacy*" che ricomprende anche la *Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio del 27 aprile 2016 (relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio)*; contestualmente il legislatore europeo ha approvato altresì la *Direttiva (UE) 2016/681 del Parlamento europeo e del Consiglio del 27 aprile 2016 sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi*.

[13] Per esempio: nel *Considerando* n. 8 si prevede la possibilità per gli Stati di integrare parti del Regolamento nel diritto interno, qualora il Regolamento stesso lo preveda; nel *Considerando* n. 41 si parla esplicitamente di un intervento legislativo dei singoli Stati, configurato come non necessario, ma comunque ragionevolmente auspicabile per rendere più chiara la misura legislativa da applicare nel caso di specie.

Tale disposizione di carattere generale, inserita nel quadro dei presupposti di liceità del trattamento, impone espressamente ai legislatori nazionali di considerare, tra i criteri ispiratori della propria azione, il principio di proporzionalità del trattamento, che rappresenta uno dei pilastri non solo dell'intero Regolamento ma ormai, ampiamente, anche nel ragionamento ermeneutico della Corte di giustizia dell'Unione europea [14].

Sul piano legislativo italiano, si pone la questione delle ricadute che il Regolamento ha sul Codice in materia di protezione dei dati personale [15]. È infatti possibile che si riscontrino antinomie tra le disposizioni regolamentari e quelle del Codice. In questo caso la strada della disapplicazione per via giudiziale delle norme interne in contrasto con quelle europee direttamente applicabili è ormai regola certa e da tempo definita dalla Corte costituzionale [16].

Nella direzione di intraprendere un percorso volto ad apportare interventi correttivi mirati, si è mosso il Parlamento italiano, che ha rimesso al Governo, tramite delega legislativa (art. 13 legge 163/2017, Legge di delegazione europea 2016-2017), il compito di individuare le parti del testo del Codice da modificare e i nuovi contenuti da introdurre [17].

---

[14] Cfr. V. Fiorillo, *op. cit.*, 23 s.

[15] Il d.lgs. 196/2003, che aveva sostituito la prima legislazione organica in materia, la legge 675/1996.

[16] Tuttavia, sarà interessante capire quale incidenza avrà, su tale consolidato orientamento, la recente sent. 269/2017 con cui la Corte costituzionale, al termine di un ragionamento piuttosto innovativo, ritiene che «laddove una legge sia oggetto di dubbi di illegittimità tanto in riferimento ai diritti protetti dalla Costituzione italiana, quanto in relazione a quelli garantiti dalla Carta dei diritti fondamentali dell'Unione europea in ambito di rilevanza comunitaria, debba essere sollevata la questione di legittimità costituzionale, fatto salvo il ricorso al rinvio pregiudiziale per le questioni di interpretazione o di invalidità del diritto dell'Unione, ai sensi dell'art. 267 del TFUE» (par. 5.2).

[17] Ecco il testo della delega: «1. Il Governo è delegato ad adottare, entro sei mesi dalla data di entrata in vigore della presente legge, con le procedure di cui all'articolo 31 della legge 24 dicembre 2012, n. 234, acquisiti i pareri delle competenti Commissioni parlamentari e del Garante per la protezione dei dati personali, uno o più decreti legislativi al fine di adeguare il quadro normativo nazionale alle disposizioni del 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 95/46/CE.

2. I decreti legislativi di cui al comma 1 sono adottati su proposta del Presidente del Consiglio dei ministri e del Ministro della giustizia, di concerto con i Ministri degli affari esteri e della cooperazione internazionale, dell'economia e delle finanze, dello sviluppo economico e per la semplificazione e la pubblica amministrazione.

3. Nell'esercizio della delega di cui al comma 1 il Governo è tenuto a seguire, oltre ai principi e criteri direttivi generali di cui all'articolo 32 della legge 24 dicembre 2012, n. 234, anche i seguenti principi e criteri direttivi specifici:

a) abrogare espressamente le disposizioni del codice in materia di trattamento dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196, incompatibili con le disposizioni contenute nel regolamento (UE) 2016/679;

b) modificare il codice di cui al decreto legislativo 30 giugno 2003, n. 196, limitatamente a quanto necessario per dare attuazione alle disposizioni non direttamente applicabili contenute nel regolamento (UE) 2016/679;

c) coordinare le disposizioni vigenti in materia di protezione dei dati personali con le disposizioni recate dal regolamento (UE) 2016/679;

Va detto che appare al contempo comprensibile e condivisibile la scelta del legislatore delegato di aver previsto una delega che non portasse al superamento per intero del Codice – un testo che ha sempre dato un'ottima prova di sé in termini di chiarezza ed efficacia – ma ad una sua riscrittura alla luce delle istanze maggiormente garantiste del Regolamento, pur in una linea di continuità con il percorso europeo del diritto [18]. In questo caso, a differenza di quanto va rilevato per il sistema delle fonti europee dove la forma (la scelta dello strumento regolamentare) è anche sostanza, nell'applicazione a livello nazionale la vera innovazione sta nei contenuti piuttosto che nella forma.

Il d.lgs. 10 agosto 2018, n. 101 attua la delega e modifica in larga parte il Codice, oltre a prevedere una serie di disposizioni che, pur non entrando a far parte del corpus del Codice stesso, rivestono fondamentale importanza per la disciplina della fase transitoria (in particolare articoli da 18 a 21).

Pur non essendo questa la sede per una completa trattazione del contenuto del decreto legislativo, va detto che il legislatore delegato si è mosso nell'ottica di estensione delle tutele, avvalendosi appieno di una serie di facoltà, tra cui, in primis, quella prevista dall'art. 9, par. 4 GDPR la quale consente agli Stati membri di estendere le garanzie per le particolari categorie di dati (genetici, biometrici e sanitari).

L'art. 2 *septies* del Codice novellato (che peraltro tiene conto di alcuni rilievi formulati dal Garante nel proprio parere reso il 22 maggio 2018) rappresenta un'importante ed ulteriore fonte di garanzia per quelle tipologie di dati che più da vicino sono connessi al nucleo fondante della personalità, non solo perché ne rappresentano caratteristiche fisiche (dati biometrici) o momenti di sofferenza e bisogno (dati sanitari) ma anche perché posseggono una portata "narrativa" (sul passato, sulla storia famigliare) e "predittiva" (sul futuro, si pensi alla medicina predittiva ma anche a possibili applicazioni "deviate" di tali strumenti), come i dati genetici.

L'art. 2 *septies* del Codice, come modificato dal legislatore delegato, affida al Garante il compito di adottare ogni due anni un provvedimento prescrittivo generale che stabilisca le misure di garanzia per il trattamento di tali dati; tramite tale provvedimento il Garante può reintrodurre il consenso – secondo il Regolamento, il consenso, infatti, non è esclusiva base legale del trattamento per tali dati – quale misura di

---

d) prevedere, ove opportuno, il ricorso a specifici provvedimenti attuativi e integrativi adottati dal Garante per la protezione dei dati personali nell'ambito e per le finalità previsti dal regolamento (UE) 2016/679;

e) adeguare, nell'ambito delle modifiche al codice di cui al decreto legislativo 30 giugno 2003, n. 196, il sistema sanzionatorio penale e amministrativo vigente alle disposizioni del Regolamento (UE) 2016/679 con previsione di sanzioni penali e amministrative efficaci, dissuasive e proporzionate alla gravità della violazione delle disposizioni stesse.

4. Dall'attuazione del presente articolo non devono derivare nuovi o maggiori oneri a carico della finanza pubblica e ad essa si provvede con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente».

[18] Cfr. M. Rubechi, *La transizione verso il nuovo sistema delle fonti europee di protezione dei dati personali*, in 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*, Napoli, Editoriale Scientifica, 2017.

protezione per il trattamento di genetici che comportino un elevato livello di rischio.

Vi è da dire che sui dati genetici e i dati biometrici – finalmente parificati dal legislatore europeo ai dati sensibili – il Garante nel corso degli anni aveva costruito delle specifiche garanzie, pur in assenza dell'attuale quadro regolamentare. La scelta di avvalersi di questa "riserva" è, dunque, in linea con un preciso percorso che l'Autorità ha fatto nel corso degli anni e non rappresenta un appesantimento ulteriore, bensì una conferma di un quadro di garanzie, ora pienamente supportato anche dal dato normativo.

Occorre però fare riferimento ad un'ultima e importante fonte di regolazione. Il Regolamento lascia spazio da un lato alla *soft law* delle Autorità di vigilanza, nonché del Comitato europeo per la protezione dati [19], dall'altro incentiva il ricorso a codici di condotta (art. 40), da adottarsi nei settori di volta in volta ritenuti opportuni: fonti regolatorie autoprodotte da parte degli stessi soggetti che sono poi chiamati a rispettarle, nella consapevolezza che il coinvolgimento nel processo normogenetico assicuri un maggior livello di conformazione [20].

2. – Si può sostenere che il Regolamento si costruisce su quattro pilastri fondamentali che incarnano, in termini generali, i principi ispiratori dell'intervento normativo. Su tali principi si innestano poi i vari istituti e le tante regole specificamente contenute, in alcuni casi rafforzando gli strumenti di tutela e i presupposti generali già contenuti nella direttiva; in altri, anche innovando significativamente quanto stabilito in precedenza, proprio alla luce del necessario ammodernamento degli strumenti di tutela.

2.1. – Non si può non partire dalla constatazione del rafforzamento del sistema dei diritti. Il riconoscimento di un catalogo di diritti azionabili in capo all'interessato rappresenta una delle principali conquiste poste dalla direttiva 95/46/CE e successivamente consolidate dalla giurisprudenza europea, oggi pienamente inscritte nella cornice costruita dai Trattati europei come rivisti a Lisbona e dalla Carta dei diritti fondamentali.

Si tratta di un modello che ha mostrato tutti i suoi pregi, e che funziona soprattutto grazie a due elementi: da una parte, l'affermazione di alcuni precisi diritti, come il diritto di accesso ai propri dati personali, di conoscenza delle caratteristiche del trattamento, di aggiornamento, cancellazione o modificazione dei dati, di opposizione al trattamento. Dall'altra parte, la delineazione di un meccanismo di tutela che prevede un primo tentativo di risoluzione in via conciliativa, cioè l'esercizio dei diritti direttamente nei confronti del titolare del trattamento; in caso di riscontro mancato o insoddisfacente, l'esperimento di apposita azione di fronte all'istituzione competente [21].

---

[19] Cioè il consesso europeo delle Autorità, che sostituisce il precedente Gruppo di lavoro "Articolo 29".

[20] Sottolinea questo processo di «abdicazione dell'*hard law*» P. Passaglia, Privacy e *nuove tecnologie, un rapporto difficile. Il caso emblematico dei social media, tra regole generali e ricerca di una specificità*, in *Consulta online*, n. 3/2016, 335.

[21] Su quest'ultimo versante, occorre riconoscere che il legislatore italiano ha ideato un meccanismo di

I benefici del modello costruito dal combinato Direttiva-Codice sono stati così evidenti da portare il legislatore europeo a confermarlo. Già di per sé questa scelta rappresenta una chiara presa di posizione: sui diritti non si arretra, il patrimonio di questi anni mantiene una sua piena validità ed efficacia.

La principale valutazione da compiere a tal proposito riguarda gli strumenti a disposizione dell'interessato per esercitare i propri diritti. Lo strumento paragiurisdizionale del ricorso, che così bene aveva funzionato nel contesto dell'ordinamento italiano, non era espressamente previsto dalla direttiva, così come non è disciplinato dal Regolamento. Quest'ultimo, infatti, prevede esclusivamente – come già faceva la direttiva – il reclamo come mezzo a disposizione dell'interessato attivabile dinanzi un'Autorità di controllo (art. 77 GDPR). Eppure se si guarda alle disposizioni relative ai diritti (artt. 15-22) ci si rende conto che queste sono costruite in modo da coinvolgere il titolare del trattamento: è quest'ultimo, infatti, a dover assicurare *prima facie* il soddisfacimento del diritto di cui l'interessato è titolare. Permane, dunque, la logica di una richiesta rivolta in prima istanza al titolare da parte dell'interessato, che poi potrà comunque rivolgersi all'Autorità di controllo tramite lo strumento del reclamo. Va detto che neanche il d.lgs. n. 101/2018 contiene traccia della necessaria procedimentalizzazione di questi passaggi, in grado di assicurare una copertura normativa al procedimento dei ricorsi così come conosciuti finora.

Il Regolamento non si limita ad un approccio meramente conservativo. Infatti, il progresso tecnologico e informatico e l'utilizzo sempre più massiccio della rete hanno reso necessario un adeguamento alle nuove sfide che l'uomo (digitale) deve affrontare: in altre parole, il citato catalogo dei diritti doveva essere arricchito.

Tra i nuovi diritti entrati nella disciplina positiva particolare attenzione va riservata al diritto all'oblio, quale sottoinsieme del più generale diritto alla cancellazione, in quanto istanza di cancellazione di dati personali trattati lecitamente ma diventati non più attuali a causa del trascorrere del tempo (art. 17). 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 dell'*url*) dai risultati di una ricerca effettuata su un motore di ricerca generalista a partire da parametri di ricerca quali il nome e cognome di una persona fisica [22]. Si tenga però conto delle possibili conseguenze, soprattutto sul contrapposto interesse alla memoria collettiva (o alla ricerca storica), poiché deindiciz-

tutela ancora più efficace, affiancando, ai tradizionali ricorsi in via amministrativa (tramite segnalazione o reclamo) e in via giurisdizionale (adendo il giudice civile), una speciale procedura di ricorso di carattere "paragiurisdizionale" dinanzi all'Autorità (artt. 141 e 145-151); si tratta di una soluzione, sostanzialmente unica nel panorama europeo, che consente una tutela rapida ed efficace.

[22] Si trattava del classico caso della pubblicazione da parte di testate giornalistiche di notizie contenenti informazioni personali sui soggetti di cui si parla (perlopiù, vicende giudiziarie che li hanno coinvolti) le quali, a distanza di tempo, e in presenza di sviluppi della vicenda (come un'assoluzione in giudizio) o di altri elementi (il ruolo non più pubblico della persona, la scarsa gravità delle accuse), meriterebbero di non ricevere più la medesima diffusione.

zare 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.

Non si può dimenticare il diritto alla portabilità dei dati personali da un titolare del trattamento ad un altro (art. 20), preordinato a facilitare il percorso verso la creazione del mercato unico digitale [23]. Inoltre, il tradizionale diritto di opposizione (art. 21) trova una sua specifica declinazione nell'ambito della profilazione (art. 22) che, nell'era dei *big data*, rappresenta uno dei trattamenti più diffusi e utilizzati da operatori pubblici e privati, ma ad alto tasso di pervasività della nostra sfera privata oltre che di ridefinizione automatizzata e involontaria della nostra identità personale [24].

Altrettanto rilevante, ma in parte più complicata, 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. Vanno altresì in questa medesima direzione la declinazione del consenso con riguardo alla tutela di particolari figure soggettive come i minori ed a particolari tipologie di trattamento dati. Nella stessa logica certamente si inserisce la previsione espressa della possibilità di revoca e dell'esclusione di ogni forma di consenso tacito.

2.2. – La vera novità del Regolamento risiede nel profilo speculare alla tutela dei diritti dell'interessato: quello cioè dell'accentuazione dei doveri del titolare, che risponde al principio di *accountability*, oggi incluso espressamente all'art. 5 tra i principi che governano il sistema della protezione dati, accanto a quelli ormai noti [25]. Il nuovo quadro normativo infatti è disseminato di numerosi istituti che si iscrivono in una prospettiva di carattere chiaramente responsabilizzante [26].

Questa logica di maggior responsabilizzazione dei *data controllers* a primo impatto

---

[23] Come sostenuto all'interno delle *Linee-guida sul diritto alla "portabilità dei dati"* (WP 242 del 5 aprile 2017), che forniscono indicazioni utili proprio sull'esercizio di questo diritto riconosciuto dal Regolamento.

[24] Ecco alcuni esempi recenti dove il Garante italiano è intervenuto con provvedimenti di divieto: un progetto di banca dati privata per la misurazione del "rating reputazionale", consistente nell'incrocio di dati personali caricati volontariamente sulla piattaforma dagli stessi utenti con dati recuperati, invece, dalla rete tramite dubbie operazioni di *webcrawling* (Provv. Garante 24 novembre 2016, doc. web n. 5796783); l'elaborazione e aggregazione automatizzata dei dati personali, caricati per altri scopi dagli utenti sui social network dedicati alla valorizzazione del proprio profilo professionale, al fine di creare profili personalizzati da mettere a disposizione di datori di lavoro che reclutino personale (cfr. Relazione annuale 2016 del Garante, 109 s.).

[25] Seguendo la nuova dicitura, si tratta cioè dei principi di: liceità, correttezza e trasparenza; limitazione della finalità; minimizzazione dei dati; esattezza; limitazione della conservazione.

[26] Le Autorità europee di protezione dati avevano posto la necessità di accedere ad una valorizzazione della responsabilità del titolare già nel 2010 con il *Parere 3/2010 sul principio di responsabilità* (WP 173 del 13 luglio 2010).

potrebbe apparire come un appesantimento degli oneri. In realtà l'obiettivo è più ambizioso: infatti, se gli adeguati accorgimenti gestionali, procedimentali e tecnologici vengono adottati in fase di progettazione, se affidi ad una persona competente il compito di monitorare costantemente la loro idoneità e di mediare con le richieste provenienti dalle Autorità di vigilanza, se riesci ad ottenere un marchio di garanzia, se aderisci ad un codice di condotta riconosciuto, e così via, allora sarà più difficile incorrere in violazioni, e quindi in prescrizioni, divieti o sanzioni.

Ci si può attendere, dunque, che la responsabilizzazione produca grandi benefici sugli interessati e contemporaneamente possa risultare alla lunga più conveniente per i titolari stessi (pur riconoscendosi qualche alleggerimento in favore delle piccole e medie imprese: *Considerando* n. 13), che potranno ammortizzare nel tempo i maggiori costi patiti in fase di progettazione.

È ipotizzabile che le imprese potranno godere di ricadute positive anche per altre ragioni connesse alla percezione della *privacy* come valore aggiunto da parte di cittadini e consumatori. Le imprese virtuose in termini di *privacy* alimentano un clima di fiducia e questo può accrescere la competitività sui mercati.

Con l'impostazione del Regolamento si 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 e dovranno rivolgersi all'Autorità solamente allorché gli effetti sui diritti degli interessati siano connotati da gravità e probabilità: questa può certamente essere una semplificazione degli adempimenti, altra naturale ricaduta positiva della responsabilizzazione [27].

Il concetto di responsabilizzazione del titolare ha una duplice valenza (art. 24): quella di adottare tutte le misure utili a prevenire atti e comportamenti su dati personali che possano impattare sugli interessati; nonché quella di documentare quanto fatto in chiave probatoria, a fronte di violazioni effettive o comunque di controlli dell'Autorità.

In questo contesto possiamo quindi leggere le principali novità introdotte dal Regolamento.

In primo luogo, va precisato che la sicurezza dei sistemi e delle reti in cui si conservano e fluiscono dati personali non costituisce più un semplice elemento tecnico: con la sua elevazione a livello di principio fondamentale (art. 5, par. 1, lett. *f*)), essa diventa un presupposto vero e proprio dei trattamenti, che ogni titolare deve considerare quale elemento prioritario ineliminabile.

I principali strumenti di responsabilizzazione sono tuttavia sintetizzati dall'approccio

[27] Pone l'accento sulla responsabilizzazione e sulla "filosofia" che vi sta dietro anche A. Mantelero, *La riforma della data protection in Europa: un'opportunità per le imprese*, in *www.giustiziacivile.com*, 3 marzo 2014.