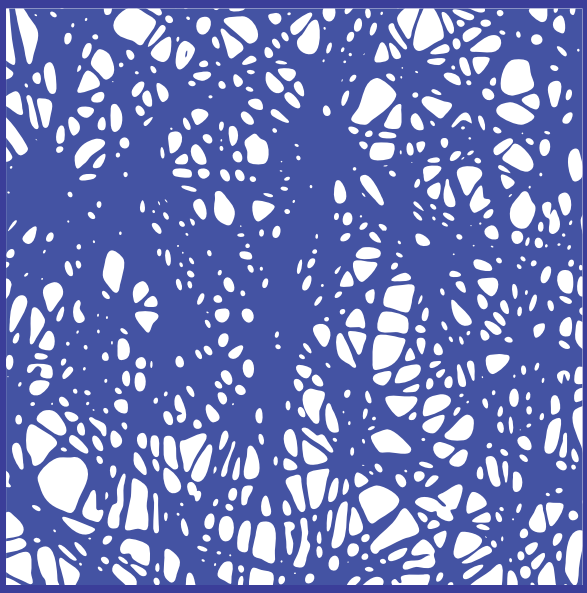
STUDI IN TEMA DI
INTERNET
ECOSYSTEM

Alessandro Mantelero, Dianora Poletti
(a cura di)

Regolare la tecnologia: il Reg. UE 2016/679 e la protezione dei dati personali. Un dialogo fra Italia e Spagna



Collana diretta da Paolo Passaglia e Dianora Poletti

PISA
UNIVERSITY
PRESS

Alessandro Mantelero, Dianora Poletti
(a cura di)

Regolare la tecnologia: il Reg. UE 2016/679 e la protezione dei dati personali. Un dialogo fra Italia e Spagna

PISA
UNIVERSITY
PRESS

Regolare la tecnologia: il Reg. UE 2016/679 e la protezione dei dati personali : un dialogo fra Italia e Spagna / a cura di Alessandro Mantelero, Dianora Poletti. - Pisa : Pisa university press, 2018. - (Studi in tema di internet ecosystem)

342.240858 (WD)
Mantelero, Alessandro II. Poletti, Dianora 2. Dati personali - Diritto alla riservatezza – Regolamenti comunitari

CIP a cura del Sistema bibliotecario dell'Università di Pisa

Opera sottoposta a peer review secondo il protocollo UPI

Titolo collana:
Studi in tema di Internet Ecosystem

Società con socio unico Università di Pisa
Capitale Sociale € 20.000,00 i.v. – Partita IVA 02047370503
Sede legale: Lungarno Pacinotti 43/44 – 56126 Pisa
Tel. + 39 050 2212056 Fax + 39 050 2212945
press@unipi.it
www.pisauniversitypress.it

ISBN 978 88 6741 8718

impaginazione: Ellissi

Sommario

Profili del contesto europeo

Regolare le tecnologie

Scenari applicativi

Premessa

Il tema della regolamentazione della tecnologia ed in specie delle tecnologie digitali ha trovato di recente un importante punto di svolta nell'adozione ed implementazione del Regolamento UE 679/2016 in materia di protezione dei dati personali.

È questo un ambito connotato da rilevanti interessi che devono essere opportunatamente considerati e bilanciati, come dimostrato dai più noti casi (Snowden, Google Spain, Cambridge Analytica, solo per citare i principali) e dalle importanti ripercussioni che gli stessi hanno generato *in primis* sul sistema regolatorio, ma anche sui modelli di business e sugli equilibri geo-politici.

In tal contesto, il tema del nuovo Regolamento non può essere affrontato unicamente da una prospettiva nazionale, ma necessita di un più ampio dialogo fra culture giuridiche ed esperienze differenti. È in quest'ottica che nei giorni 8 e 9 giugno 2018 si è tenuto presso l'Università di Pisa il primo incontro di studi italo-spagnolo su "L'entrata in vigore del Regolamento (UE) 2016/679: la riforma alla prova della prassi in Italia e in Spagna", organizzato dal Master in Internet Ecosystem: Governance e Diritti e dal Dipartimento di Giurisprudenza dell'Università di Pisa, in collaborazione con il Dipartimento di Ingegneria Gestionale del Politecnico di Torino. L'incontro ha costituito una delle prime occasioni di confronto tra esperti e studiosi all'indomani dell'entrata in vigore del Regolamento, con il coinvolgimento diretto dei rappresentanti sia dell'autorità italiana per la protezione dei dati personali, sia di quelle spagnole e catalana.

La varietà degli interventi tenutisi durante l'incontro ed il dialogo stimolante fra i relatori, nonché il fruttuoso esito della messa a confronto dei modelli italiano e spagnolo, ci hanno indotti a non concludere questa proficua esperienza nel contesto del convegno ed

a dar vita al presente volume. In questo libro trovano, dunque, più compiuto sviluppo e meditata analisi i temi discussi nel corso delle giornate di studi, ora raccolti attorno a quattro nuclei principali che guardano alle novità, alle sfide e ai limiti del GDPR, ai profili del contesto europeo, alla più generale regolamentazione delle tecnologie ed, infine, agli scenari applicativi.

Dall'insieme dei contributi, molti dei quali frutto di una *call for papers* che ha coinvolto giovani studiosi, trova conferma come il nuovo quadro normativo, passato dall'armonizzazione all'uniformazione, necessiti di un opportuno confronto fra le varie esperienze nazionali, a partire da quelle che per cultura giuridica e valori sociali mostrano maggiore affinità.

Da ciò l'interesse ad analizzare l'attuazione del Regolamento nei due Paesi qui considerati, onde verificare le soluzioni dettate. L'intento che ha mosso la raccolta di saggi è stato quello di riflettere sulle linee di politica del diritto tracciate dal legislatore europeo, con lo sguardo volto alle concrete modalità operative con cui il GDPR ha inteso perseguire tali scelte.

Il lettore italiano troverà inoltre, nei contributi relativi al contesto nazionale, richiami specifici al d.lgs n. 101/2018, emanato successivamente allo svolgimento del convegno che ha ispirato questo lavoro, ma di cui gli autori hanno tenuto conto nei loro scritti.

Gli autori spagnoli non hanno mancato di fare riferimento alla recentissima *Ley Orgánica 3/18, de 5 de diciembre, de Datos Personales y garantía de los derechos digitales*, promulgata proprio mentre il presente *e-book* era in bozze.

Pisa, dicembre 2018

I curatori
Alessandro Mantelero
Dianora Poletti

Comprendere il Reg. UE 2016/679: un'introduzione

Dianora Poletti

Sommario: 1. Lo scenario e l'intento del GDPR – 2. Una risposta complessa per un problema complesso – 3. *Accountability* e *compliance*: la "procedimentalizzazione" dell'adeguamento al GDPR – 4. La riforma alla prova della prassi (e del d.lgs. n. 101/2018) – 5. Il necessario recupero della priorità dei diritti

1. Lo scenario e l'intento del GDPR

Il Regolamento UE 679/2016 (GDPR) relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali mette definitivamente in soffitta la Direttiva 95/46/CE. Quest'ultima ha segnato l'avvio degli sforzi dell'Unione Europea volti a disciplinare la specifica materia in un momento in cui il trattamento dei dati personali ancora era considerato un "affare" sostanzialmente privato, posto che lo scambio dei dati avveniva dall'interessato al titolare, operando in una dimensione relazionale binaria o almeno in una sfera soggettivamente circoscrivibile[1].

Il significativo passaggio dall'armonizzazione all'uniformazione è stato imposto da uno scenario profondamente mutato sotto molteplici risvolti. Dall'epoca della c.d. direttiva-madre la tematica ha dovuto confrontarsi con trasformazioni tumultuose e neppure im-

[1] Parla di modello normativo che «individuava un unico scambio di dati: dall'interessato al titolare del trattamento», G. Finocchiaro, *Introduzione al Regolamento Europeo sulla protezione dei dati*, in *Le nuove leggi civ. comm.*, 2017, 1.

maginabili, dipendenti soprattutto dalla facilitazione della circolazione delle informazioni e dalla crescente apertura dei mercati. La penetrazione della tecnologia, che ormai si fonde con lo stesso corpo fisico, ha consentito la raccolta massiccia di dati, spesso operata "a strascico", con il conseguente loro impiego per finalità altre da quelle della raccolta e con la loro detenzione – fattore tanto decisivo quanto inquietante – non già da parte di autorità pubbliche ma di soggetti privati. Le espressioni "società datificata" o *quantified self* ("io quantificato") scolpiscono con efficacia la situazione e pongono con prepotenza il problema del valore non solo personale ma economico delle informazioni.

Nella consapevolezza di questo diverso contesto e delle nuove sfide dallo stesso prodotte, come è reso esplicito dal *Considerando* 6 del GDPR, l'Unione europea interviene rafforzando internamente e esternamente il suo diritto.

Sul primo versante, la dichiarata ragione di una persistente frammentazione normativa nei singoli Stati, conseguenza di un recepimento non del tutto uniforme della Direttiva 95/46/CE, ha costituito una delle ragioni dell'adozione dello strumento regolamentare, volto proprio a superare le asimmetrie tra gli ordinamenti (*Considerando* n. 9) e a dettare una disciplina analitica, espressa nei 99 articoli del Regolamento.

Sul secondo versante, il tentativo dell'Europa di emanciparsi dalla dimensione riduttiva del mercato interno emerge con chiarezza da due passaggi normativi. Anzitutto, dall'art. 3, dedicato all'ambito di applicazione territoriale (art. 3), che – a determinate condizioni – estende le disposizioni regolamentari anche al trattamento effettuato fuori dell'Unione o da titolari non stabiliti nell'Unione, qualora essi offrano beni o servizi agli individui ivi residenti o ne controllino il comportamento[2]. Il tentativo di espandere al di là dei confini geografici le guarentigie offerte dal diritto europeo (in buona sostanza, di arginare la legge americana, vera regolatrice della Rete) è attuato superando il principio della cittadinanza quale parametro per il rico-

[2] Sull'ambito di applicazione territoriale del GDPR cfr. L. Bolognini-E. Pelino, in L. Bolognini-E. Pelino-C. Bistolfi (a cura di), *Il Regolamento Privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, Milano, Giuffrè, 2016, 2 ss.

noscimento e l'esercizio del diritto alla protezione dei dati. È evidente in questo l'onda della sentenza della Corte di Giustizia dell'Unione Europea relativa al caso Schrems[3], le cui argomentazioni mostravano contezza dell'impossibilità di discriminare gli utenti di una realtà globale come quella digitale in ragione della loro nazionalità. In aggiunta, anche il trasferimento dei dati verso Paesi terzi viene condizionato (come si evince in particolare dall'art. 44) al rispetto delle condizioni dettate dallo stesso regolamento nell'intero Capo V, al fine di evitare che il livello di protezione non risulti pregiudicato: questa valutazione è riservata alla Commissione europea.

L'intento del Regolamento resta quello di garantire il rispetto dei diritti in un mercato aperto alla circolazione, anche transfrontaliera, delle persone e delle loro informazioni e dunque di conciliare libertà di trattare i dati[4] con il limite rappresentato dalla effettività dei diritti spettanti all'interessato. In questo l'intento del Regolamento non è dissimile da quello della abrogata Direttiva, anche se il faro di questa era rappresentato dalla Convenzione europea dei diritti dell'uomo, mentre quello del Regolamento è rappresentato dall'art. 7, che ripropone il diritto al rispetto della vita privata e soprattutto dall'art. 8 della Carta di Nizza, che riconosce espressamente il diritto alla protezione dei dati personali, oltre che dall'art. 16 del TFUE.

La Direttiva ricordava che uno degli obiettivi della Comunità europea era la promozione della democrazia basata «sui diritti fondamentali sanciti dalle Costituzioni e dalle leggi degli Stati membri nonché dalla Convenzione europea di salvaguardia dei diritti dell'uomo e delle libertà fondamentali». La chiave di comprensione del Regolamento è sintetizzata nei suoi primi *Considerando*, che esplicitano come lo scopo dello stesso sia quello di incentivare l'economia digitale, che vive e si nutre della circolazione dei dati, garantendo il diritto fondamentale alla protezione di questi, all'insegna della creazione di un clima di fiducia e di collaborazione. Molto

[3] Sentenza 6 ottobre 2015, C-362/14, sulla quale cfr. AA.VV., *La protezione transnazionale dei dati personali. Dal "Safe Harbour Principle" al "Privacy Shield"*, G. Resta-V. Zeno Zencovich (a cura di), Roma, RomaTrePress, 2016.

[4] Per una ricostruzione volta a porre l'accento sul potere del titolare di svolgere l'attività di trattamento v. F. Bravo, *Il "diritto" a trattare dei dati personali nello svolgimento dell'attività economica*, Milano, Cedam, 2018.

chiaro al riguardo è il *Considerando* 7, che punta alla creazione di un «quadro più solido e coerente in materia di protezione dei dati dell'Unione, affiancato da efficaci misure di attuazione, data l'importanza di creare il clima di fiducia che consentirà lo sviluppo dell'economia digitale in tutto il mercato interno».

2. Una risposta complessa per un problema complesso

Il legislatore attua questo difficile ma necessario contemperamento, proprio di un contesto rinnovato, operando uno spostamento di prospettiva rispetto al passato. Se un tempo il passaggio epocale era stato quello dal "vecchio" diritto alla riservatezza al nuovo diritto al controllo sui propri dati, in una realtà fortemente tecnologica, affamata di informazioni, il primo diritto persiste, salva la necessità di definirne meglio i confini con il diritto alla protezione dei dati personali, ma si riduce, fino quasi a scomparire del tutto, la possibilità di mantenere il controllo sul flusso di informazioni che riguardano gli interessati.

Da qui, l'esigenza di adottare un registro diverso, sintetizzabile con una certa dose di approssimazione in una serie di passaggi: dall'osservanza di specifiche misure di sicurezza (anche legislativamente previste) alla scelta e all'applicazione di quelle che risultino più adeguate in ogni specifico contesto; dall'adempimento di una dettagliata normativa ad un vero e proprio sistema di gestione del rischio; dalla responsabilità alla "responsabilizzazione"; dalla riparazione del danno alla prevenzione dello stesso. Inusuale è anche lo stesso linguaggio adoperato dal legislatore, che risente di una terminologia mutuata in parte dalla dimensione aziendale in parte dall'ambiente tecnologico, come comprovano concetti come la valutazione del rischio, il *Data Protection Impact Assessment*, il regime del *Data Breach*, l'anonimizzazione e la pseudonimizzazione dei dati personali.

Parallelamente, per operare l'opportuno bilanciamento, il legislatore amplia il catalogo dei diritti dell'interessato, anche se, a ben vedere, i nuovi diritti introdotti (in specie, il diritto alla portabilità, il diritto alla limitazione del trattamento, ma anche il "diritto all'oblio", qualora lo si voglia connotare in termini diversi dal già noto diritto alla cancellazione dei dati) altro non sono che specificazioni

del diritto alla protezione dei dati, che non riceve una esplicita definizione nel Regolamento.

Deriva da tutto questo un provvedimento complesso, che tenta di dare risposte ad un problema la cui complessità già si è accresciuta a fare data dal periodo (non breve) di gestazione dello stesso, che – per esempio – ha visto emergere con ancora maggiore risalto le problematiche legate alla crescente diffusione dell'intelligenza artificiale e dei *Big Data analytics*[5], ma anche quelle legate a forme più penetranti dei tradizionali controlli a distanza, come le tecniche di geolocalizzazione o i *wearable devices*.

Il GDPR non è inoltre un corpo normativo autosufficiente, ma reclama l'aiuto di molteplici soggetti per assicurare un adeguato livello di protezione agli interessati: la Commissione europea, alla quale l'art. 12 paragrafo 8 e l'art. 43 paragrafo 8 attribuiscono il potere di adottare atti delegati, ma anche "atti di esecuzione per stabilire norme tecniche riguardanti i meccanismi di certificazione e i sigilli e i marchi di protezione dei dati"; gli stati nazionali, cui è demandata l'adozione di norme più specifiche per adeguare l'applicazione del Regolamento, a partire dalle categorie particolari di dati personali; le autorità di controllo, anche riunite nel Gruppo europeo dei Garanti (EDPB).

La molteplicità dei soggetti complica inevitabilmente il quadro delle fonti, rendendolo sempre più multilivello. A dispetto dei non scarsi rinvii operati dal Regolamento alle legislazioni nazionali, risulta inevitabilmente ridimensionamento il ruolo di queste ultime, a causa della crescente importanza del ruolo delle autorità garanti, i cui provvedimenti solo descrittivamente possono essere ancora definiti in chiave di *soft law*. Il richiamo al *soft law* evoca a sua volta la crescita destinata ai codici di condotta, che assumeranno un ruolo molto rilevante, specie per adeguare l'applicazione del GDPR alle micro, piccole e medie imprese.

[5] Sul tema v., tra la crescente letteratura: F. Pizzetti, *a protezione dei dati personali e la sfida dell'Intelligenza Artificiale*, in F. Pizzetti (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Torino, Giappichelli, 2018, 145 ss.; A. Mantelero, *Regulating big data. The guidelines of the Council of Europe in the context of the European data protection framework*, in *Computer Law and Security Review*, 2017, 584.

Il Regolamento, infine, non è un corpo normativo destinato a rimanere invariato o a conservare immutabile la sua struttura: la stessa idea del GDPR come di una legge *in progress* (alla quale già la disciplina nazionale previgente in materia aveva subito abituato l'interprete) è proiettata nella formulazione dell'art. 97, che prevede un riesame con cadenza quadriennale del GDPR, consentendo alla Commissione la possibilità di proporre modifiche del Regolamento tenuto conto, «in particolare, degli sviluppi delle tecnologie dell'informazione e dei progressi della società dell'informazione».

3. *Accountability* e *compliance*: la "procedimentalizzazione" dell'adeguamento al GDPR

Il carattere di effettiva novità del Regolamento va individuato, come è stato rilevato, più che nel dato normativo (in alcuni casi proiezione del WP29 o della giurisprudenza europea), nello spostamento di prospettiva che coloro che trattano dati altrui (*in primis*, istituzioni e imprese) dovranno adottare[6].

Non vi è dubbio che l'approccio del Regolamento sia incentrato sul principio di "accountability" e della "compliance" dei trattamenti. A dispetto della sua comparsa nel regolamento solo nel paragrafo 2 dell'art. 5, l'*accountability* è l'espressione che più ha attirato l'attenzione degli studiosi, anche per la sua difficoltà di una specifica traduzione, resa in genere con il termine "responsabilizzazione"[7], atto anche ad esprimere la stessa capacità di "rendere conto" dell'efficacia delle misure organizzative e tecniche concretamente impiegate.

Al principio di *accountability* è tenuto in primo luogo il titolare del trattamento, la cui responsabilità è definita dall'art. 24. Non vi è dubbio che il GDPR definisca un sistema di adeguamento al GDPR fortemente accentrato sulla figura del titolare. La riconosciuta difficoltà di esercizio dei diritti dell'interessato (spesso propenso a rila-

[6] G. Busia-L. Liguori-O. Pollicino, *Nota introduttiva*, in G. Busia-L. Liguori-O. Pollicino (a cura di), *Le nuove frontiere della privacy nelle tecnologie digitali. Bilanci e prospettive*, Roma, Aracne, 2017, 12.

[7] Discute sul significato e sulla traduzione del termine "accountability" E. Lucchini Guastalla, *Il nuovo Regolamento europeo sul trattamento dei dati personali: i principi ispiratori*, in *Contratto e impr.*, 2018, 120.

sciare i suoi dati con leggerezza o con totale carenza di consapevolezza) e il ruolo sempre più declinante del consenso e del controllo affidato alla persona fisica sposta il baricentro sul titolare del trattamento e sulla necessità che le operazioni del trattamento siano "GDPR *compliant*". La stessa centralità della gestione del rischio mostra, in definitiva, una visuale appuntata più sulla circolazione che non sulla protezione dei dati.

Si è già detto che il rispetto della normativa dettata dal GDPR non è garantito dall'osservanza di norme puntuali, posto che lo stesso non compie una scelta predeterminata, ma la rimette al titolare del trattamento, che è chiamato a scegliere le misure più adeguate a prevenire i rischi, ad assumere le debite decisioni e a provare di aver adottato misure proporzionate ed efficaci.

Il risultato che consegue è chiaramente quello di un approccio di tipo procedimentale, lontano da iniziative estemporanee o adottate in unica soluzione, che muove dalla valutazione di impatto, passa per l'individuazione dei responsabili del trattamento (interni ed esterni) e dalla considerazione dell'opportunità di procedere alla nomina di un responsabile della protezione dei dati (*Data Protection Officer*), continua, ad esempio, con il periodico aggiornamento dei registri del trattamento e con il costante monitoraggio delle misure organizzative e tecnologiche volte non solo ad allontanare il pericolo di trattamenti illeciti o comunque non conformi alla normativa ma anche dirette ad assicurare e facilitare l'adempimento delle richieste degli interessati basate sull'esercizio dei loro diritti.

Si pone in questa stessa direzione il passaggio da una tutela in chiave prevalentemente rimediale e riparatoria, come quella prevista dalla Direttiva 95/46/CE, a una tutela – quella su cui è incentrato il GDPR – di stampo essenzialmente preventivo, fondata sulla valutazione del rischio e sul suo contenimento attraverso tecniche di protezione fin dall'avvio del trattamento e per impostazione predefinita. I declamati principi di "privacy by default" e di "privacy by design"[8], espressioni efficaci per sintetizzare l'innesto della regola sulla tecnica, sono essi stessi una concretizzazione dell'*accountability*. Fin dal momento della progettazione dei servizi occorre infatti tenere

[8] G. D'Acquisto-M. Naldi, *Big Data e Privacy By Design*, Torino, Giappichelli, 2018, specie 33 ss.

in considerazione la minimizzazione dell'uso dei dati personali e la necessità di integrare o, se si vuole, di incorporare nell'architettura e nell'uso delle tecnologie la loro necessaria protezione.

La conclusione è che il GDPR non è rigido ma dotato della flessibilità necessaria per adattarsi dinamicamente alle differenti situazioni nelle quali si opera il trattamento, non impone direttamente una prescrizione ma sollecita scelte e verifiche delle stesse, anche se il tutto è presidiato da un sistema sanzionatorio di tipo amministrativo non predeterminato nei massimi e minimi ma parametrato al fatturato aziendale mondiale, con uno specifico, evidente riguardo per i *Big Players* della Rete.

4. La riforma alla prova della prassi (e del d.lgs. n. 101/2018)

Il tempo trascorso dall'emanazione del Regolamento ha segnato dapprima un sostanziale disinteresse per le novità e per gli obblighi previsti, seguito, nell'imminenza della sua entrata in vigore, da una corsa all'adeguamento, sospinta dal timore delle sanzioni.

Nel diritto italiano, il periodo è stato caratterizzato dallo sforzo di pervenire all'adeguamento tempestivo della normativa interna, che ha fatto registrare, non senza un certo ritardo e con un iter alquanto tribolato, l'emanazione del d.lgs. n. 101/2018.

L'entrata in vigore di questo provvedimento ha tratteggiato un regime nel quale le disposizioni del d.lgs. n. 196/2003 novellato dovranno essere interpretate ed applicate in conformità al Regolamento, in quanto parte integrante di un unico sistema normativo a due livelli[9].

[9] Chiarisce la Relazione al decreto che la "clausola di salvaguardia" contenuta nell'art. 22, comma 1°, che impone di applicare e interpretare le disposizioni del decreto e dell'ordinamento nazionale alla luce della normativa euro-unitaria in materia – «esplicita un canone interpretativo desumibile anche dalla gerarchia delle fonti del diritto», che «mira ad evitare ogni possibile controversia o antinomia in sede applicativa, garantendo alle norme dell'ordinamento coerenza e conformità al quadro giuridico europeo». In argomento cfr. F. Pizzetti, *I consigli per leggere e applicare bene il decreto 101/2018 dal 19 settembre*, in *www.agendadigitale.eu*, 14 settembre 2018.

Il dato che colpisce più immediatamente l'interprete è la presenza di un codice che, a dispetto del mantenimento della sua denominazione (neppure puntuale peraltro)[10] ha perso il suo ruolo di corpo normativo centrale[11]. La disciplina in materia è oggi ripartita su più piani: la fonte primaria del Regolamento, il Codice privacy novellato, il decreto legislativo di adeguamento della normativa nazionale (per la parte che non incide sul Codice), la residua normativa nazionale in materia di protezione dei dati personali, con un assetto complessivo di non sempre facile impiego per gli operatori.

La perdita di centralità del Codice privacy si deve anche all'ulteriore ispessimento del ruolo delle autorità di controllo, rispetto all'ampliamento già avvenuto a livello europeo. L'Autorità Garante ha svolto un ruolo essenziale in chiave di concretizzazione dei precetti di rango legislativo, dando un operoso contributo alla effettività della tutela dei dati personali: ha sviluppato una propria "giurisprudenza", ha proceduto alla redazione di linee guida, autorizzazioni, provvedimenti, prescrizioni. I Garanti nazionali e il Gruppo dei Garanti europei tanto hanno fatto per orientare e incoraggiare quella che oggi chiamiamo la responsabilizzazione, per molti versi anticipando gli indirizzi contenuti nella nuova legislazione europea. L'Autorità garante continuerà ad avere un ruolo da protagonista nell'attuazione e nell'implementazione del nuovo quadro normativo[12]. Gli indici sono numerosi: senza alcuna pretesa di completezza,

[10] Infatti la ridenominazione del d.lgs. n. 196/2003 "Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 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", lascia intendere che sia il d.lgs. 196/ 2003 ad avere adeguato il diritto interno al GDPR, quando tale adeguamento è stato operato dal d.lgs. n. 101/2018.

[11] Emblematico è il titolo del commento a prima lettura di questa normativa che si deve a V. Cuffaro, *Quel che resta di un codice: il d.lgs. 10 agosto 2018, n. 101 detta le disposizioni di adeguamento del codice della privacy al Regolamento sulla protezione dei dati*, in *Corr. giur.*, 2018, 1181 ss.

[12] V. Cuffaro, *Il diritto europeo sul trattamento dei dati personali*, in *Contr.e impresa*, 2018, 1098 ss., specie 1114, sottolinea come il rafforzamento del ruolo dell'Autorità Garante sia imposto dall'esigenza di rendere effettiva la tutela dei diritti dell'interessato, che necessita di una gestione di stampo pubblicistico.

oltre alla previsione di regole deontologiche (art. 2-*quater*), si pensi alle misure di garanzia per il trattamento dei dati genetici, biometrici e relativi alla salute di cui all'art. 2-*septies*, ai provvedimenti di carattere generale relativi a trattamenti che comportano rischi elevati per l'esecuzione di compiti di interesse pubblico di cui all'art. 2-*quinquiesdecies* (che riconosce all'autorità di controllo la possibilità di emanare inediti "provvedimenti di carattere generale adottati d'ufficio"), alle autorizzazioni generali per la disciplina dei dati appartenenti a "categorie particolari", alle linee guida di indirizzo, ma anche ai nuovi e rilevanti poteri assegnati al Garante nella delicata materia dell'accreditamento (art. 2-*septiesdecies*).

5. Il necessario recupero della priorità dei diritti

I limiti e le difficoltà di operare del Regolamento – non a torto – sono già stati individuati, specie di fronte alla dimensione della raccolta delle grandi quantità di dati personali, la cui regolamentazione sfugge al rapporto binario interessato-titolare e allo stesso impiego del principio di finalità del trattamento. Tranne un richiamo alla contitolarità del trattamento contenuto nell'art. 26 GDPR, nuovo rispetto alla direttiva, che apre a un modello di co-gestione dei dati, il profilo della tutela collettiva fa difetto, come è stato prontamente sottolineato[13].

Il lavoro compiuto è significativo, ma quello da compiere è ancora molto. Più che imputare al regolamento manchevolezze o di tacciarlo di non essere riuscito nell'intento divisato, pare necessario raccogliere e provare a perseguire le nuove sfide poste da questo atto normativo, giungendo quando ciò si renda necessario a interpretazioni anche estensive e ragionevoli della normativa.

Su questo tema si gioca una delle più importanti sfide identitarie dell'Europa. Perdere terreno sul piano dei diritti umani per il vecchio continente equivale a perdere la battaglia più decisiva che oggi si sta combattendo: quella contro l'imbarbarimento. L'Europa ha il compito di attuare un modello di crescita e di evoluzione che faccia perno sui diritti e che tuteli la dignità umana.

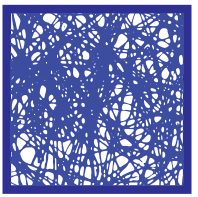
[13] Soprattutto A. Mantelero, *Responsabilità e rischio nel reg. UE 2016/679*, in *Le nuove leggi civ. comm.*, 2017, 144.

Occorre prendere atto, con visione realistica, che la libertà non può essere salvaguardata oscurando (se mai sia possibile nella struttura della Rete) i dati personali o revocando il consenso al trattamento, come i recenti e recentissimi fatti di cronaca ci hanno confermato.

Per proseguire il cammino verso la realizzazione di un'idea democratica e personalista del diritto, l'interprete dovrà spostare il baricentro, per tornare all'art. 1 del Regolamento, da quanto sancito al suo paragrafo terzo («La libera circolazione dei dati personali nell'Unione non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali»), alla prospettiva di una circolazione nella quale la tutela dei diritti sia effettivamente garantita[14]. In questa direzione la scomparsa del riferimento al diritto alla protezione dei dati personali nella norma di apertura del codice novellato, più che prestare il fianco a critiche, può essere compensata dal richiamo operato al rispetto «della dignità umana, dei diritti e delle libertà fondamentali della persona» che compare nell'art. 1 del novellato codice. Quella dignità che il Regolamento richiama un'unica volta, a proposito del trattamento dei dati relativi ai lavoratori (art. 88).

Adeguarsi al Regolamento (essere, come si dice oggi, *compliant* allo stesso) costa, per imprese e istituzioni, più che in termini economici, in termini di consapevolezza, maturità e serietà. Proprio la *compliance* – presa sul serio – è termine che è forse possibile usare anche per gli studiosi, chiamati a uno sforzo molto significativo per impiegare al meglio la normativa e dare risposte adeguate al tema della protezione dei dati personali.

[14] Per una lettura critica sul ridimensionamento del diritto alla *privacy* e del diritto alla protezione dei dati personali operato dal GDPR: F. Piraino, *Il Regolamento generale sulla protezione dei dati personali e i diritti dell'interessato*, in *Le nuove leggi civ. comm.*, 2017, specie 403 ss.



Novità, sfide e limiti del GDPR

Il diritto europeo sulla protezione dei dati personali e la sua applicazione in Italia: spunti per un bilancio

Vincenzo Cuffaro

Sommario: 1. Tre spunti di riflessione sul trattamento dei dati personali – 2. La costruzione del sistema – 3. La realizzazione delle regole e l'effettività del sistema – 4. Il ruolo dell'interprete

1. Tre spunti di riflessione sul trattamento dei dati personali

Cercando di schematizzare una riflessione che richiederebbe un impegno certo maggiore delle mie forze, credo che la sintesi di quanto è accaduto nei venti anni trascorsi dell'emanazione della legge n. 675/96 possa essere affidata a tre ordini di considerazioni riguardanti rispettivamente: la costruzione del sistema, l'effettività del sistema, il ruolo dell'interprete.

Il riferimento al sistema appare una notazione obbligata quando si esamini il complesso delle disposizioni elaborate nell'arco di tempo che ci separa dalla prima legge in materia; disposizioni non a caso raccolte nel testo che, messo a punto nel 2003 sotto l'ambiziosa ma eloquente norma di Codice per la protezione dei dati personali, è ora in corso di smantellamento. Ma analoga notazione vale per il Regolamento che anch'esso aspira a delineare un corpo organico di regole destinate, ed è rilievo nel segno dell'ovvio, a non essere astrette nei confini nazionali.

2. La costruzione del sistema

La disciplina sul trattamento dei dati costituisce un osservatorio privilegiato là dove consente di osservare un fenomeno non usuale nell'esperienza del diritto, costituito dal formarsi di regole la cui trama non è tessuta su un ordito precedente.

Certamente l'interesse intorno al quale si coagula la disciplina giuridica dei dati personali è interesse che appartiene all'individuo in quanto tale e può quindi ricondursi al novero dei diritti dei quali la persona fisica è titolare[1], ma è innegabile che alla messa a fuoco di tale diritto – del diritto che nella formula dell'art. 1 del Codice del 2003 e nel titolo del Regolamento del 2016 è focalizzato sulla 'protezione dei dati personali'- concorrono un complesso di disposizioni che ne determina il contenuto *ex novo*, nel senso che, a differenza di quanto è ad esempio avvenuto per la disciplina del consumatore, le diverse regole non si innestano su una precedente regolamentazione, ma enunciano una disciplina del tutto nuova, come è del resto nuova la realtà che si intende disciplinare.

L'esigenza di approntare una regolamentazione dell'attività di trattamento dei dati personali, che è avvertita quasi contestualmente al determinarsi del fenomeno e ne segue costantemente gli sviluppi, nasce su impulso del legislatore comunitario.

La messa a punto delle regole sul trattamento dei dati personali è infatti attribuibile principalmente se non esclusivamente alla fonte comunitaria a partire da quando, rimasti inattuati i progetti precedenti[2], la disciplina del trattamento dei dati irrompe, per così dire, nell'ordinamento statuale con la legge n. 675/1996 che vede l'Italia tra i primi paesi europei a dare attuazione alla direttiva 95/46/CE. A tale direttiva sono poi seguite le direttive 2002/21/CE in materia di reti e servizi di comunicazione elettronica e la direttiva 2002/58/CE sul trattamento dei dati personali a tutela della vita privata nel settore delle comunicazioni elettroniche, che hanno entrambe trovato

[1] Non a caso è ormai abbandonata l'impostazione originaria di cui all'art. 1 della legge n. 675/1996 che annoverava anche la persona giuridica e ogni altro ente e associazione tra gli interessati al trattamento dei dati.

[2] Sui quali v. S. Niger, *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali*, Padova, Cedam, 2006, 109 ss.

attuazione con l'emanazione del d.lgs. 30 giugno 2003, n. 196 recante il Codice in materia di protezione dei dati personali[3]. Una articolata disciplina domestica rispetto alla quale viene ora a porsi come fonte sovraordinata il Regolamento UE 2016/679, tramite il quale il legislatore europeo abbandona la strada della armonizzazione e adotta direttamente le regole che sovrintendono il trattamento dei dati in vista della realizzazione degli obiettivi, tra loro complementari, della protezione delle persone fisiche e della libera circolazione dei dati personali.

Della matrice comunitaria la disciplina reca i tratti caratteristici in misura tale che l'esame di alcuni di questi può costituire un'utile traccia per svolgere una necessariamente sommaria ricognizione di quanto è accaduto in questi anni.

Dovendo procedere per esemplificazioni, l'analisi può essere circoscritta ad alcuni profili: il ruolo dei 'considerando', il contenuto delle 'definizioni', la tecnica di formulazione delle regole.

Rispetto ai 'considerando' che precedono l'articolato delle norme per spiegarne la *ratio*, può innanzi tutto constatarsi come per la materia del trattamento dei dati personali la novità del fenomeno cui è rivolta la regolamentazione assegna ai considerando una peculiare funzione.

Già mettendo a confronto il considerando 3 della direttiva del 1995 «l'instaurazione e il funzionamento del mercato interno, nel quale conformemente all'articolo 7A del trattato, è assicurata la libera circolazione delle merci, delle persone, dei servizi e dei capitali, esigono non solo che i dati personali possano circolare liberamente da uno Stato membro all'altro, ma che siano altresì salvaguardati i diritti fondamentali della persona», con il considerando 4 del Regolamento del 2016

> «il trattamento dei dati dovrebbe essere al servizio dell'uomo. Il diritto alla protezione dei dati di carat-

[3] Non è forse inutile ricordare che proprio in occasione dell'emanazione della legge n. 675/96 era stata inaugurata la tecnica di filatura mobile del tessuto normativo, essendo espressamente prevista la delega ad emanare «decreti legislativi, recanti disposizioni integrative della legislazione in materia di tutela della persona e di altri soggetti rispetto al trattamento dei dati personali» (così art. 1, legge n. 676/1996).

> tere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità. Il presente regolamento rispetta tutti i diritti fondamentali e osserva le libertà e i principi riconosciuti dalla Carta, sanciti dai trattati, in particolare il rispetto della vita privata e familiare, del domicilio e delle comunicazioni, la protezione dei dati personali. la libertà di pensiero, di coscienza e di religione, la libertà di espressione e d'informazione, la libertà d'impresa il diritto a un ricorso effettivo e a un giudice imparziale, nonché la diversità culturale, religiosa e linguistica»,

l'interprete è in grado di cogliere un significativo mutamento di *ratio*, che nel testo più recente rende esplicita l'esigenza di contemperamento tra gli interessi in gioco rispetto all'attività del trattamento dei dati. Una realtà che ormai è segnata dalla ineliminabile pervasività delle tecnologie informatiche nell'uso dei dati personali e che impone una regolamentazione che con tale pervasività deve confrontarsi.

Certo, il linguaggio del legislatore è significativo del mutamento di *ratio*. Nel testo più recente è resa esplicita l'esigenza di contemperamento tra gli interessi in gioco rispetto all'attività del trattamento dei dati europeo anche se con l'uso di termini, come il riferimento alla 'funzione sociale' riferita al diritto alla protezione dei dati personali, che non possono non apparire singolari all'interprete consapevole del significato che tale espressione assume nel nostro sistema costituzionale quale connotato del diritto di proprietà. Parole[4] che tuttavia confermano come il sistema che si è andato costruendo in questi anni è indirizzato ad una disciplina che abbandona l'idea della protezione esclusiva, della 'prerogativa assoluta', e intende coniugare l'esigenza di tutela della persona con la inevitabile realtà della circolazione dei dati personali.

[4] Sulle quali riflette A. Ricci, *Sulla «funzione sociale» del diritto alla protezione dei dati personali*, in *Contr. Impr.*, 2017, 596 ss.

Il rilievo assegnato al profilo della circolazione dei dati personali, trova conferma nel considerando n. 6 del Regolamento

> «la rapidità dell'evoluzione tecnologica e la globalizzazione comportano nuove sfide per la protezione dei dati personali. La portata della condivisione e della raccolta di dati personali è aumentata in modo significativo. La tecnologia attuale consente tanto alle imprese private quanto alle autorità pubbliche di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività. Sempre più spesso, le persone fisiche rendono disponibili al pubblico su scala mondiale informazioni personali che li riguardano. La tecnologia ha trasformato l'economia e le relazioni sociali e dovrebbe facilitare ancora di più la libera circolazione dei dati personali all'interno dell'Unione e il loro trasferimento verso paesi terzi e organizzazioni internazionali, garantendo al tempo stesso un elevato livello di protezione dei dati personali»,

e mostra come il modello di regolamentazione adottato per la disciplina del trattamento dei dati sia significativamente mutato per tener conto di quanto è accaduto contestualmente al porsi delle regole.

Non è inutile ricordare, nella cronaca del vissuto di questi anni, che la prima direttiva comunitaria ora abrogata è del 1995, ma la Google Inc., il più grande motore di ricerca al mondo, è stata fondata il 4 settembre 1998, o ancora che il codice italiano in materia di protezione dei dati è del 2003, ma nel 2004 è stata fondata Facebook Inc. (che nel 2012 ha acquistato Instagram e nel 2014 ha acquisito Whatsapp) e nel 2006 è stato lanciato Twitter. Ma è parimenti interessante osservare come, anche in ragione di tali accadimenti, la disciplina del trattamento si sia andata progressivamente costruendo secondo la logica del rapporto, cui è immanente il principio di bilanciamento degli interessi[5], che vuole la condotta di tutti

[5] Condivisibili così i rilievi di F. Piraino, *Il regolamento generale sulla protezione dei dati personali e i diritti dell'interessato*, in *Nuove Leggi civ. comm.*, 2017, 369 ss.

i soggetti coinvolti nel trattamento improntata alla regola della reciproca correttezza.

Nel testo del Regolamento 2016/679/UE sono, del resto, presenti numerose disposizioni che appaiono espressione del modello sopra indicato.

Ad esempio quando, nell'art. 6, la liceità del trattamento è commisurata, tra l'altro, anche al perseguimento di un legittimo interesse del titolare o di terzi; ovvero quando, nell'art. 7, è precisato che la richiesta di consenso all'interessato deve essere esposta in maniera facilmente intellegibile; o ancora quando, nell'art. 21, al titolare è riconosciuto il diritto di dimostrare che esistono motivi legittimi per procedere al trattamento malgrado l'opposizione dell'interessato; soprattutto quando, nell'art. 25 e negli artt. 32 e ss., è imposto al titolare l'approntamento di misure idonee per garantire la protezione dei dati personali rispetto a potenziali rischi.

Certamente una disciplina legale improntata al modello del rapporto si espone all'obiezione che in tal modo viene ad essere ignorata l'enorme sperequazione delle posizioni delle parti e tuttavia non può omettersi di rilevare come il legislatore europeo non sia ignaro del problema ed abbia preferito affrontarlo non con gli strumenti del divieto ma con quelli più duttili della responsabilità e della vigilanza affidata alle Autorità che con maggior efficacia possono realizzare una tutela dei diritti dei singoli.

Ancora rilevante per comprendere come si è andato modificando il disegno complessivo della disciplina è riflettere sulla tecnica delle definizioni; una tecnica nella specie giustificata dalla indubbia novità della materia sin dal momento in cui iniziò ad essere oggetto di regolamentazione e dalla necessità di adeguare successivamente le regole ad una realtà in continua evoluzione.

Il numero della definizione è progressivamente aumentato, ma non si tratta solo di un aspetto quantitativo, giacché l'esame dei termini presenti nelle liste permette di percepire come si è andata mutand la disciplina. Dalla lettura sinottica degli elenchi definitori risultano, infatti, mappe non perfettamente sovrapponibili, nelle quali le aree della regolamentazione presentano confini in continua espansione.

Le definizioni di cui alla legge n. 675/96 contengono termini elementari se messi a confronto con quelli, ben più analitici, di cui al Codice del 2003 e addirittura superati rispetto a quelli contenuti ora nel Regolamento del 2016.

Ad esempio, la definizione di 'banca dati' presente nella legge n. 675/1996 e ripetuta nel Codice del 2003, scompare dal Regolamento, sostituita dal vocabolo 'archivio', che identifica «qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico». Un termine dunque più snello, ma maggiormente ricco di indicazioni, proiettate a considerare con maggiore precisione la attuale realtà fenomenica che conosce la rete di internet come un archivio di archivi[6].

Il mutamento del lessico riflette, del resto, il mutamento della *rationes* sottese alla disciplina del trattamento dei dati, rispetto alla quale l'attenzione alla costituzione della banca dati, espressione della legislazione "di prima generazione"[7], cede il passo alla necessità di attuare una più ampia protezione dei diritti dell'interessato quale che sia il luogo nel quale sono "custoditi", "depositati", i dati che lo riguardano.

Ancor più significativo dell'evoluzione che la disciplina è andata registrando in questi quattro lustri è rilevare come nel novero delle definizioni della legge n. 675/1996 e del Codice del 2003 mancasse una definizione di 'consenso', anche se tale mancanza non è stata d'ostacolo alla comprensione della disciplina dell'atto i cui requisiti erano enunciati in disposizioni specifiche[8].

[6] Come sottolineano F. Di Ciommo e R. Pardolesi, *Dal diritto all'oblio in Internet alla tutela dell'identità dinamica. È la rete, bellezza!*, in *Danno e resp.*, 2012, 701 ss.

[7] Sulla quale v. N. Matteucci (a cura di), *Privacy e banche dati. Aspetti giuridici e sociali*, Bologna, il Mulino, 1981. Ripercorre le varie fasi degli interventi legislativi A. Mantelero, *Il nuovo approccio della valutazione del rischio nella sicurezza dei dati*, in G. Finocchiaro (diretto da) *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, Zanichelli, 2017, 290.

[8] *Ex multis*, sull'art. 11 della legge n. 675/96, v. P. Manes, *Il consenso al trattamento di dati personali*, Padova, Cedam, 2001; A. Fici-E. Pellecchia, *Il consenso al trattamento*, in R. Pardolesi (a cura di) *Diritto alla riservatezza e circolazione dei dati personali*, Milano, Giuffrè, 2003, vol. I, 469 ss.; sull'art. 23 del Codice del 2003, v. S.M. Meloni, *Il trattamento dei dati da parte di soggetti privati: la disciplina del consenso*, in V. Cuffaro-R. D'Orazio-D. Ricciuto (a cura di), *Il codice del trattamento dei dati personali*, Torino, Giappichelli, 2007, 197 ss. e S. Mazzamuto, *Il principio del consenso e il problema della revoca*, in R. Panetta (a cura di), *Libera circolazione e protezione dei dati personali*, Milano, Giuffrè, 2006, vol. I, 1029 ss.

Nel Regolamento i tratti del consenso, espresso «mediante dichiarazione o azione positiva inequivocabile», sono invece direttamente esposti nella definizione di cui al punto 11) dell'art. 4 che vuole la «manifestazione di volontà libera, specifica, informata e inequivocabile», con una formula che viene in tal modo ad assumere un significato immediatamente precettivo, fissando i requisiti ricorrendo i quali il consenso sussiste. Il luogo nel quale sono espresse le regole consente così di rimarcare sul piano diacronico il valore di una disciplina che abbandona il formalismo e privilegia l'esigenza di assicurare la concreta consapevolezza della persona circa il trattamento dei dati.

Nel segno della evidenza quanto alla emersione di contenuti che si aggiungono a caratterizzare la disciplina del trattamento dei dati, è poi la presenza di definizioni nuove.

È già stato ricordato come la stessa nozione di 'dato personale' risulti nel Regolamento arricchita di significative integrazioni, ma di maggior rilievo è certamente la definizione di 'profilazione' che indica «qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica». La definizione, nel richiamare un aspetto del trattamento non nuovo, in quanto già l'art. 14 del Codice del 2003 contiene una regola che attiene alla profilazione[9], dà risalto ad una modalità del trattamento particolarmente rilevante e particolarmente invasiva.

L'uso della profilazione non soltanto per attività di marketing ma nei più diversi settori, lavorativo, commerciale, sanitario, del credito, spiega la particolare attenzione che ad essa riserva il Regolamento, nell'ambito del quale due specifiche disposizioni disciplinano il diritto di opposizione dell'interessato rispetto al processo decisionale automatizzato conseguente la profilazione. Segno, questo, del rilievo

[9] V. L. Bozzi, *Le regole generali per il trattamento dei dati*, in V. Cuffaro-R. D'Orazio-D. Ricciuto (a cura di), *Il codice del trattamento dei dati personali*, cit., 96 ss.

che è venuta ad assumere l'esigenza di protezione dell'individuo di fronte a quei trattamenti dei dati che vengono ad incidere in misura più marcata sulla sfera personale.

Ulteriore tratto caratteristico della (e derivante dalla) disciplina di fonte comunitaria attiene, infine, alla tecnica di formulazione delle disposizioni.

Nel codice del 2003 ed ora nel Regolamento del 2016, la norma che individua il precetto legale è sovente accompagnata da un elenco di eccezioni che non soltanto ne delimitano la portata ma ne modificano il senso, rendendo meno agevole la intelligenza della regola.

Ad esempio, nel codice del 2003, l'enunciazione perentoria circa la necessità del consenso quale si trae dalla lettura del comma 1 dell'art. 23 «il trattamento di dati personali da parte di privati o di enti pubblici economici è ammesso solo con il consenso espresso dell'intermediario» è subito smentita dal dettato del successivo art. 24 che enumera nove casi nei quali il trattamento può essere effettuato senza il consenso.

Analogamente, per quanto inerisce a quei dati che nel Codice del 2003 sono qualificati «sensibili», la norma dell'art. 9 par. 1 del Regolamento 2016/679 vieta il trattamento di «categorie particolari di dati personali», di ma nel successivo par. 2 elenca i numerosi casi nei quali il divieto non si applica. Ancora, la articolata previsione dei primi quattro paragrafi dell'art. 14 del Regolamento circa il novero delle informazioni da fornire qualora i dati personali non siano stati ottenuti dall'interessato, è corretta dall'enunciato del paragrafo 5 del medesimo articolo, nel quale sono indicati i casi nei quali le informazioni possono essere omesse.

La esatta attribuzione di significato dei precetti risulta in tal modo più complessa.

Rimanendo sulle precedenti esemplificazioni tratte dall'esame del Regolamento, è agevole constatare come dalla lettura dell'ipotesi di cui alla lett. a) del par. 2 dell'art. 9, si ricavi la regola che il trattamento dei dati sensibili è consentito, tra l'altro, quando l'interessato abbia prestato il proprio esplicito consenso per una o più finalità specifiche. Regola che dunque ribalta il precetto sul divieto perentorio e supera l'impostazione di cui al Codice del 2003 – che invece condizionava il trattamento dei dati sensibili al consenso scritto dell'interessato e soprattutto alla previa autorizzazione del

Garante – sicché in definitiva, in forza dell'ulteriore condizione dettata nella medesima proposizione normativa[10], finisce per affermare un precetto di diverso tenore: il trattamento dei dati sensibili è consentito quando, tra l'altro, l'interessato abbia prestato il proprio consenso per una o più finalità specifiche, a meno che il diritto europeo o nazionale non vietino comunque esplicitamente il trattamento.

Ancora, mentre i primi quattro paragrafi dell'art. 14 elencano il novero delle informazioni che il titolare del trattamento deve fornire all'interessato quando i dati non siano stati ottenuti direttamente, nel paragrafo successivo della medesima disposizione è precisato che l'obbligo non sussiste in un complesso di casi la cui disamina vale in parte a rimodellare il ruolo del precetto. L'enunciato per cui le informazioni non sono dovute quando l'interessato già ne dispone ovvero quando comunicarle implicherebbe uno sforzo sproporzionato, vale non soltanto ad attenuare la portata del precetto circa la doverosità dell'informazione, ma altresì a delineare una regola nel segno del necessario contemperamento tra il diritto dell'interessato a conoscere la sorte dei dati che altri sta trattando avendoli ottenuti *aliunde* ed il diritto di un titolare ad effettuare il trattamento senza appesantire la propria attività con adempimenti sproporzionati rispetti al tipo di dati utilizzati[11].

Resta così confermato il rilievo precedentemente svolto circa i connotati caratterizzanti la più recente disciplina che, con solido realismo, prende atto della dimensione che è venuto ad assumere il fenomeno della circolazione dei dati e cerca di fornire risposte adeguate privilegiando tecniche di tutela più efficienti rispetto a quelle affidate alla sola iniziativa del singolo.

[10] Espressa con una formula poco felice: «salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al paragrafo 1».

[11] Di recente, viene suggerita una lettura del sistema che dà rilievo al potere del titolare a svolgere l'attività di trattamento: v. F. Bravo, *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, Milano, Cedam, 2018.

3. La realizzazione delle regole e l'effettività del sistema

Il complesso delle regole che sovrintendono il trattamento dei dati personali, segnate per come si è detto da un vigoroso tratto di novità, pone in primo piano il tema delle effettività della regolamentazione di questo settore dell'esperienza giuridica.

A tale riguardo, non può omettersi di considerare come la dimensione nella quale si svolge il trattamento dei dati abbia determinato un significativo mutamento di prospettiva che si riflette sulla stessa conformazione delle regole del trattamento.

Innanzi tutto, la dimensione geografica.

Nel momento in cui l'interprete prende atto che i dati raccolti o depositati circolano in una rete tendenzialmente globale, risulta evidente che la prescrizione di regole dettate per essere efficaci nello spazio geopolitico europeo mostra il limite intrinseco, giacché il modello europeo di regolamentazione deve necessariamente misurarsi con altri modelli che, come è noto, presentano un minor livello di protezione.

Di ciò mostra consapevolezza il Regolamento quando, nell'art. 3, delinea l'ambito di applicazione territoriale delle regole con riferimento allo stabilimento del titolare o del responsabile nel territorio dell'Unione, ma «indipendentemente dal fatto che il trattamento si effettuato o meno nell'Unione», affrancando così la nozione di stabilimento dal luogo fisico (ammesso che sia in qualche modo individuabile) nel quale il titolare organizza il trattamento dei dati.

In termini ancor più incisivi, il medesimo articolo precisa che le regole devono essere rispettate altresì quando, pur non sussistendo lo stabilimento del titolare nell'Unione, l'attività di trattamento inerisca a offerte di beni o servizi ovvero riguardi il monitoraggio del comportamento degli interessati.

Rispetto a quest'ultimo, specifico novero di trattamenti, opportunamente ritenuti più invasivi e quindi potenzialmente pregiudizievoli per la persona, è dunque disegnata una rete protettiva più ampia di quella immediatamente riferibile ai confini geografici dell'Unione, nel dichiarato intento di evitare che le tutele approntate possano risultare in concreto vanificate.

A tale riguardo, il Capo V del Regolamento disciplina le condizioni per il trasferimento di dati personali verso paesi terzi fissando, nell'art. 44, il principio per cui «qualunque trasferimento di dati personali oggetto di trattamento…ha luogo soltanto se il titolare del trattamento e il responsabile del trattamento rispettano le condizioni di cui al presente capo», ulteriormente precisando che «tutte le disposizioni del presente capo sono applicate al fine di assicurare che il livello di protezione delle persone fisiche garantito dal presente regolamento non sia pregiudicato», e quindi demandando direttamente alla Commissione europea la valutazione se il paese terzo garantisca un livello di protezione adeguato.

Previsioni, queste, che costituiscono una precisa presa di posizione sul tema dei flussi di dati transfrontalieri, dopo che la sentenza della Corte di Giustizia dell'Unione europea sul caso Shrems[12] ha ribadito la superiorità del modello europeo di protezione dei dati personali, sottolineando il ruolo ed il valore degli artt. 7 e 8 della Carta dei diritti fondamentali dell'Unione europea, del resto già richiamati nella altrettanto nota sentenza Google Spain[13].

Ancora, la dimensione tecnologica.

La quantità e la complessità delle operazioni di trattamento, realizzate da software in grado di captare ed elaborare i dati, mostra la necessità di un adeguamento delle regole. Il modello europeo di disciplina al quale dà rilievo la giurisprudenza della Corte di Giustizia[14] viene ora, nel Regolamento, arricchito di ulteriori valenze, segnatamente là dove sono dettate nuove prescrizioni circa gli obblighi che incombono sul titolare del trattamento.

Senza che sia qui possibile una lettura di dettaglio, merita sottolineare come il novero di prescrizioni individuate e riassunte nelle formule *privacy by default* e *privacy by design*, valga ad imporre al

[12] Per una ricca ed articolata riflessione sulla sentenza 6 ottobre 2015, C-362/14, v. G. Resta-V. Zeno-Zencovich (a cura di), *La protezione transnazionale dei dati personali. Dai 'Safe Harbour principles' al "Privacy Shied"*, Roma, Roma TrE-Press, 2016.

[13] Al cui commento la Rivista *Dir. Inf*., ha dedicato il numero speciale 4/5 del 2014, senza che sia qui necessario richiamare nel dettaglio tutti gli interessanti e perspicui contributi ivi raccolti.

[14] Puntualmente richiamate in F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali, personali – Dalla Direttiva al nuovo Regolamento e*uropeo, Torino, Giappichelli, 2016, 240 ss.

titolare del trattamento di mettere in atto sin dal momento dell'approntamento dell'attività «misure tecniche e organizzative adeguate» per «attuare in modo efficace i principi di protezione dei dati» a tutela dei diritti degli interessati (art. 25) e successivamente ad adottare le medesime misure per «garantire un livello di sicurezza adeguato al rischio» di pregiudizi per i diritti e le libertà delle persone fisiche (art. 32).

In tal modo, il Regolamento segna una significativa frattura rispetto al modello precedentemente adottato, nella legge 675/96 e quindi del Codice del 2003, che, come è noto, seguendo esplicitamente lo schema di cui all'art. 2050 cod. civ., consente di valutare l'adeguatezza dei mezzi impiegati ad evitare il danno soltanto dopo che il pregiudizio si è verificato[15].

La prescrizione di obblighi specifici, e specificamente sanzionabili ai sensi dell'art. 83 del Regolamento, viene a spostare il baricentro della disciplina mettendo l'accento sulla necessità di limitare preventivamente il rischio insito nel trattamento dei dati personali. La necessaria adozione di misure preventive, dirette a realizzare il rispetto delle regole di trattamento ed insieme a ridurre il rischio di pregiudizi, determina così una sorta di positivizzazione degli obblighi di protezione, ma appare scelta opportuna e opportunamente diretta a rimarcare l'esigenza di tutela cui è improntata la disciplina del trattamento.

Al tema della protezione e quindi della sicurezza dei dati appartiene altresì il complesso di disposizioni che pongono a carico del titolare l'obbligo di dare avviso prontamente delle violazioni dei dati (artt. 33 e 34); l'obbligo di compiere una preventiva valutazione dei possibili rischi, anche consultando preventivamente l'autorità di controllo (artt. 35 e 36); l'obbligo di designare, in relazione a trattamenti effettuati da soggetti pubblici ovvero aventi ad oggetto particolari categorie di dati, un responsabile della protezione dei dati (art. 37), del quale il Regolamento individua (art. 39) i compiti in maniera dettagliata.

A questo novero di obblighi si aggiunge poi un ulteriore complesso di regole che, sul piano volontario, prevedono l'adesione a codici

[15] Su tali profili v. F. Gritti, *La responsabilità civile nel trattamento dei dati personali*, in V. Cuffaro-R. D'Orazio-D. Ricciuto (a cura di) *Il codice del trattamento dei dati personali*, cit., 107 ss.

di condotta elaborati autonomamente dalle associazioni di categoria (art. 40), la eventuale sottoposizione ad un organismo di vigilanza indipendente, con procedure di certificazione delle misure adottate per la protezione dei dati, affidate ad autonomi organismi di certificazione (artt. 42 e 43) accreditati, al pari degli organismi di vigilanza, presso l'Autorità garante.

A riassumere il sistema risultante da siffatte disposizioni, è diffuso il riferimento al principio di *accountability*[16] ed alla *compliance* dei trattamenti[17].

L'uso di termini mutuati dall'esperienza delle organizzazioni aziendali e societarie rende così avvertiti del mutamento di prospettiva del più recente intervento normativo e consente di registrare la peculiare valenza che è venuta ora a segnare la regolamentazione di questo ormai non marginale ambito dell'attività giuridica.

La normativa di ultima generazione, della quale il Regolamento 2016/679 costituisce il più recente ma non ultimo esempio[18], tende dunque a focalizzare l'attenzione sulla struttura dell'attività di trattamento dei dati, seguendo quasi inconsapevolmente il medesimo percorso che in altri settori di rilievo economico, quali quello bancario e assicurativo, ha portato ad irrobustire l'approntamento di regole di condotta cui devono attenersi gli operatori, il rispetto delle quali vale in qualche misura a conformare l'attività di trattamento dei dati.

Nella medesima direzione, la disciplina europea sul trattamento dei dati personali si atteggia allora a disciplina del mercato dei dati, sollecitando a comportamenti virtuosi gli operatori del trattamento,

[16] Cfr., ad esempio, G. Finocchiaro, *Il quadro d'insieme sul regolamento europeo sulla protezione dei dati personali*, in G. Finocchiaro (diretto da) *Il nuovo regolamento europeo sulla privacy*, cit., 14 ss; L. Califano, *Il Regolamento UE 2016/679 e la costruzione di un modello uniforme di diritto europeo alla riservatezza e alla protezione dati personali*, in L. Califano-C. Colapietro, *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel regolamento UE 2016/679*, Napoli, Editoriale Scientifica, 2018, 14 ss.

[17] V. F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla direttiva 95/46 al nuovo Regolamento europeo*, cit., 283.

[18] È infatti avviata la discussione sulla proposta di Regolamento relativo al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettroniche e che abroga la direttiva 2002/58/CE (regolamento sulla vita privata e le comunicazioni elettroniche).

incoraggiati a condotte coerenti con i principi di protezione in vista del conseguimento di una maggiore affidabilità agli occhi dei fornitori di dati, cioè, in definitiva, delle stesse persone i cui dati sono oggetto di trattamento.

Il riferimento al mercato dei dati non intende certo dimenticare che la disciplina del trattamento tocca direttamente i valori della persona ed avverte espressamente l'esigenza di tutela delle libertà fondamentali, ma vuole rimarcare che la circolazione dei dati ha ormai da tempo assunto un rilievo sul piano economico che sarebbe ingenuo se non ipocrita ignorare.

Né il richiamo all'idea di mercato come possibile chiave di lettura del sistema potrebbe essere inteso come un indebolimento del grado di tutela rispetto al trattamento dei dati personali, giacché nel nostro ordinamento il dettato dell'art. 41 Cost., sotto la cui egida si colloca la disciplina dell'attività economica, reca anch'esso quei riferimenti alla libertà ed alla dignità della persona che valgono sul piano assiologico a determinare la portata delle regole.

Il riferimento[19] consente piuttosto una consapevole lettura del sistema quale risulta conformato all'esito della pluriennale disciplina di settore. Un sistema che, anche per effetto del Regolamento, presenta chiari connotati economici in precedenza meno avvertiti non per disattenzione, ma in quanto diverse erano le esigenze e differenti i contesti di riferimento con i quali aveva dovuto confrontarsi la disciplina 'di prima generazione'. Merita del resto considerare come la crescita esponenziale delle tecnologie informatiche quanto alla possibilità di immagazzinamento e trattamento dei dati, accompagnata dall'espansione costante della rete di Internet e dall'affermarsi di piattaforme e motori di ricerca, abbiano determinato situazioni che da tempo suggeriscono e ora impongono un approccio economico alla studio del trattamento dati[20].

[19] Che avverte le suggestioni del dibattito da tempo avviato sui nuovi beni: v. P. Perlingieri, *L'informazione come bene giuridico*, in *Rass. dir. civ.*, 1990, 326 ss.; V. Zeno-Zencovich, *Cosa*, voce del *Dig. Civ.*, *IV*, Torino, 1990; D. Messinetti, *Circolazione dei dati personali e dispositivi di regolazione dei poteri individuali*, in *Riv. crit. dir. priv.*, 1998, 339 ss.; v. Zeno-Zencovich, *Sull'informazione come «bene» (e sul metodo del dibattito giuridico)*, in *Riv. crit. dir. priv*., 1999, 485 ss.

[20] V. A. Acquisti, *L'economia della privacy*, in V. Cuffaro-R. D'Orazio-D. Ricciuto (a cura di), *Il codice del trattamento dei dati personali*, cit., 907 ss.

Mutamento strutturale, questo ora sommariamente descritto, che ha quale necessario corollario la conferma del ruolo centrale da attribuire all'Autorità di controllo indipendente cui demandare, anche se in via non esclusiva, il governo degli interessi che gravitano nel mercato dei dati personali. Infatti, proprio nella figura del Garante sembra di poter individuare lo strumento più idoneo per conseguire una maggiore affettività del complesso sistema delineato.

Al riguardo, non è infatti senza significato che nel Regolamento venga espressamente ribadito che l'Autorità di controllo «è elemento essenziale della protezione delle persone fisiche con riguardo al trattamento dei loro dati personali»[21].

La funzione del Garante per la protezione dei dati personali, figura istituita in Italia fin dalla legge n. 675/1996 che in questi anni ha svolto l'apprezzabile compito di vigilanza e controllo, integrando con i propri provvedimenti il disegno regolamentare, è in effetti centrale nell'economia di una disciplina nella quale l'esigenza di tutela dei diritti e delle libertà fondamentali della persona deve confrontarsi con il numero e la complessità delle operazioni di trattamento dei dati e soprattutto con la presenza di una pluralità di operatori privati, molti dei quali assurgono a dimensioni economiche neanche immaginabili quando è iniziata l'era di Internet.

D'altronde, proprio la dimensione rivestita dalle imprese operanti nel settore è, a ben vedere, sottesa al nuovo e per molti versi rigoroso regime delle sanzioni che il Garante può irrogare. La previsione dell'art. 83, par. 4 del Regolamento, là dove individua quale parametro delle sanzioni amministrative il "fatturato mondiale", vale in effetti a dimostrare la avvertita consapevolezza della posizione economica ora rivestita dagli operatori del mercato.

Se per le normative di prima generazione la figura del Garante quale Autorità indipendente era stata probabilmente, anche se non esclusivamente, individuata come strumento di garanzia dei diritti delle persone rispetto al trattamento dei dati da parte dei soggetti pubblici, l'evolversi vorticoso degli apparati e delle tecnologie digitali, con la presenza di soggetti imprenditoriali privati che operando a livello globale basano la propria attività sul trattamento dei dati,

[21] Così il considerando n. 117.

determina la necessità di una Autorità indipendente, quale soggetto strutturalmente e funzionalmente idoneo a poter svolgere un controllo efficace sull'attività di trattamento ed un altrettanto efficace intervento a tutela degli interessati.

Autorità indipendente che dunque ha motivo di essere apprezzata in chiave di (ed in vista del) conseguimento del principio di effettività del novero delle regole approntate.

La centralità della figura del Garante quale perno intorno al quale ruota la disciplina della circolazione dei dati personali è del resto ribadita nel Regolamento in una duplice prospettiva. Da un lato, nell'art. 58, sono riepilogate le funzioni delle quali è titolare il Garante, con riferimento a poteri di indagine, correttivi, autorizzativi e consultivi, e con il significativo riconoscimento della legittimazione ad «intentare un'azione o agire in sede giudiziale o, ove del caso, stragiudiziale in caso di violazione del presente regolamento per far rispettare le disposizioni dello stesso». Dall'altra, negli artt. 60 e ss., è delineata una articolata disciplina di cooperazione tra i garanti dei singoli Stati, affidata alla Autorità di controllo capofila ed al Comitato europeo per la protezione dei dati.

Nel rafforzamento del ruolo dell'Autorità Garante deve dunque leggersi una precisa risposta ai problemi determinati dalla dimensione raggiunta dalla circolazione dei dati; dimensione tale per cui il riconoscimento di diritti in capo all'interessato non è più garanzia sufficiente ad una effettiva tutela, mentre è necessario che alla gestione di interessi che pur rimangono privati provveda anche un soggetto pubblico ma indipendente[22].

In tale prospettiva, la gestione pubblica di interessi privati della quale è investito il Garante appare sul piano sistematico la risposta idonea a rafforzare ed a rendere efficiente l'esigenza di tutela del singolo, non essendo ragionevole che tale tutela resti affidata alla sola iniziativa dell'interessato ovvero alla sola determinazione dei soggetti che esercitano il potere di trattare i dati personali.

[22] Sul significato che viene ad assumere il connotato della "indipendenza" proprio della Autorità, v. A. Patroni Griffi, *L'indipendenza del Garante*, in L. Califano-C. Colapietro (a cura di), *Innovazione tecnologica e valore della persona*, cit. 267 ss.

4. Il ruolo dell'interprete

Resta da considerare l'ultimo punto: il ruolo riservato all'interprete nella costruzione e ricostruzione del sistema.

Dobbiamo riconoscerlo. Rispetto alla materia del trattamento dei dati personali si assiste ad un radicale mutamento nel percorso seguito dalla tradizione giuridica nazionale (e forse non solo da questa) per lo studio dei diritti della persona.

Se vogliamo, e dobbiamo, fermare l'attenzione sul termine divenuto eponimo della disciplina, è agevole osservare che la privacy – declinata nell'accezione di diritto alla riservatezza che più direttamente rispecchia il lemma d'oltreoceano cui William Faulkner legava il 'sogno americano' – era stata una scoperta del giurista.

Sembra in effetti di poter osservare che nella nozione di privacy, o meglio nel mutamento di significato che il termine è venuto assumendo, l'interprete può leggere una sorta di parabola della ricerca giuridica e del ruolo di giurista.

Espressione prima di una aspirazione, poi di una pretesa, in Italia la privacy è affidata per larga parte del XX secolo al formante giurisprudenziale[23]; a quei giudici ed a quei giuristi particolarmente sensibili ai valori della persona, cui una intelligente lettura della norme costituzionali aveva consentito di delineare un diritto che si colloca su un terreno diverso da quello patrimoniale, un diritto radicato nel più generale diritto della personalità che non si esaurisce nella pretesa ad essere lasciati soli[24]. La privacy, nelle varie accezioni del diritto alla riservatezza che lo studioso municipale trae dai testi e dalle esperienze di altri ordinamenti, appare in effetti una sorta di scoperta del giuri-

[23] In una enumerazione necessariamente sommaria devono almeno essere indicate, quali tappe di un percorso molto più ricco seguito dalla giurisprudenza di merito, Cass. 20 aprile 1963, n. 990 in *Foro It*., 1963, I, 879 e in *Giur. It*., 1964, I, 1, 469 con nota di G. Pugliese, *Diritto alla libertà di autodeterminazione e tutela della riservatezza*; Cass. 22 maggio 1975, n. 2129 in *Foro It*., 1976, I, 2895.

[24] Le linee di sviluppo dell'articolata riflessione sul tema sono tracciate da P. Perlingieri, *La personalità umana nell'ordinamento giuridico*, Napoli – Camerino, Edizioni Scientifiche Italiane, 1972; D. Messinetti, *Personalità (diritti della)*, voce della *Enc. del Dir*., XXXIII, Milano, s.d. ma 1983; V. Zeno-Zencovich, *I diritti della personalità*, in N. Lipari-P. Rescigno (a cura di), *Diritto civile*, Milano, Giuffrè, 2009, vol. I, 495 ss.

sta il quale dall'uso accorto dello strumentario ermeneutico giunge ad affermarne l'esistenza anche in mancanza di un sufficientemente preciso riscontro normativo[25]. Una scoperta che rivendica alla scienza giuridica ed alla scienza pratica un ruolo non di mera esegesi delle disposizioni legislative, bensì di costruzione del diritto ancorata al riconoscimento dei valori costituzionali, di guida dell'esperienza giuridica per la realizzazione del valore della persona.

Tuttavia, nel momento in cui l'esito della 'scoperta' si consolida nell'opinione dei giuristi e nelle proposizioni della giurisprudenza e consente di affermare senza tentennamenti che sussiste ed è meritevole di tutela il diritto alla riservatezza[26], la nozione stessa di privacy è stata costretta a confrontarsi con una nuova realtà, quella della tecnologia informatica, che cambia radicalmente la prospettiva di analisi e, sulla scorta di un ricco apparato normativo, determina un radicale mutamento di significato della parola che tuttavia continua ad essere usata come eponimo della disciplina legale.

Senza che sia qui possibile riepilogare in che modo e secondo quali criteri la messa a fuoco del diritto alla riservatezza sia stata determinata dal confronto con il diritto all'informazione esercitato dai mezzi di comunicazione di massa, merita solo segnalare come la situazione giuridica soggettiva individuata come privacy venga ora ad assumere una diversa consistenza quando muti il punto di riferimento oggettivo e soggettivo della tutela.

Sul piano oggettivo la privacy, ormai metabolizzata come diritto alla riservatezza o ancora come diritto all'identità personale[27], muta significato ed acquista una diversa connotazione al termine del XX secolo, quando deve confrontarsi con una diversa realtà tecnologica che vorticosamente sviluppata nell'arco di pochi anni, non soltanto consente la raccolta massiva di un più vasto novero di informazioni ricavabili dall'esperienza quotidiana di ciascun individuo, ma soprattutto permette di organizzare le informazioni raccolte così da

[25] A. Cataudella, *La tutela civile della vita privata*, Milano, Giuffrè, 1974; T. Auletta, *Riservatezza e tutela della personalità*, Milano, Giuffrè, 1978.

[26] G. Giacobbe, *Riservatezza (diritto alla)*, voce della *Enc. del Dir*., XL, Milano, s.d. ma 1989.

[27] Come messo a fuoco nelle ampie e documentate voci di V. Zeno-Zencovich, *Identità personale* in *Dig. It. Sez. civ*., IX, Torino, 1995 e di G. Finocchiaro, *Identità personale (diritto alla)*, in *Dig. It. Sez. civ.*, *Agg.*, Torino, 2010.

ricostruire la vita privata come sommatoria di dati personali che divengono appetibili da parte degli operatori economici del mercato. La diffusione dei calcolatori elettronici, la digitalizzazione delle informazioni con la creazione di banche dati, l'avvento di Internet con la diffusione dei motori di ricerca e la proliferazione dei *social network* sono accadimenti che hanno determinato una sostanziale modifica dell'angolo prospettico per ciò che hanno portato al centro dell'attenzione non più quelle informazioni sulla persona che potevano rivestire interesse per la cronaca e che, in quanto notizie, riguardavano un numero ristretto di individui, bensì tutte quelle informazioni, anche minute e di per sé scarsamente significative, che riguardano ognuno e che necessariamente e costantemente vengono messe in circolazione in un sistema economico e sociale che affida all'informatica e ad Internet lo svolgimento delle attività pubbliche e private.

Sul piano soggettivo, non vengono più (solo) in considerazione le intrusioni nella vita privata poste in essere dai mezzi di informazione, cui si contrappone l'interesse del singolo fatto oggetto di notizia, quanto le utilizzazioni dei dati da parte degli operatori, economici e non, presenti sul mercato, cui si contrappone l'interesse di tutti a conoscere l'uso che dei dati vien fatto.

Sul piano strutturale, al modello proprio del diritto alla riservatezza che muove dalla individuazione di un bene appartenente al soggetto per delineare, secondo il paradigma della responsabilità da fatto illecito, la forma di tutela in caso di lesione, si sostituisce il modello che muovendo dalla relazione tra chi fornisce e chi utilizza i dati personali segue il paradigma del rapporto obbligatorio che, in quanto tale, richiama il principio della correttezza nel trattamento dei dati ed il parametro del bilanciamento degli interessi delle parti del rapporto.

Sul piano sostanziale, al profilo della informazione sulla persona che in quanto prima raccolta e poi diffusa diviene notizia, si contrappone il profilo delle informazioni che la persona fornisce di sé e produce come dati che, più o meno consapevolmente, divengono oggetto di un trattamento affidato ad apparati informatici che ne consentono l'elaborazione.

I rilievi svolti permettono quindi di comprendere come il mutamento della stessa organizzazione sociale che il linguaggio rende esplicito quando usa l'espressione 'dati personali', sia stato dunque

accompagnato da un radicale mutamento di rotta: la privacy da frutto di una costruzione teorica come diritto della persona della cui elaborazione il giurista può rivendicare la paternità, diviene invece materia di un apparato normativo elefantiaco che nel breve volgere di anni ha visto il susseguirsi di una pluralità di testi segnati da una insistente e progressiva analiticità quasi al punto di mortificare il compito dell'interprete.

Sembra allora che proprio intorno alla privacy si compia il singolare destino del giurista il quale, nel momento in cui giunge a rivendicare il ruolo di protagonista dell'esperienza, in grado di elaborare concetti ed individuare, anche in assenza di un esplicito enunciato normativo, situazioni giuridiche soggettive aventi la consistenza di diritti, facendosi così interprete di avvertite e condivise esigenze a tutela della persona, viene in qualche misura respinto indietro al ruolo di esegeta.

A far data dalla emanazione della legge 31 dicembre 1996, n. 675, l'interprete è infatti costretto a misurarsi con una fitta trama di disposizioni nelle quali sono espressamente enunciati diritti e obblighi inerenti l'attività di trattamento dei dati personali, ma soprattutto sono espressamente indicati quei diritti la cui individuazione era stata in precedenza affermata all'esito di una faticosa elaborazione dogmatica.

Di tale aspetto della vicenda il Regolamento 2016/673/UE offre significativa testimonianza in quanto non soltanto ribadisce e ulteriormente precisa il novero delle pretese e dunque dei diritti dell'interessato, quali sono ora ricavabili dai principi che sovrintendono il trattamento (artt. 5, 6 e 9), ma soprattutto espressamente enuncia i diritti dei quali è titolare l'interessato, quali il 'diritto di accesso' (art. 15), il 'diritto di rettifica' (art. 16), il 'diritto all'oblio' (art. 17), il 'diritto di limitazione del trattamento' (art. 18), il 'diritto alla portabilità dei dati' (art. 20), il 'diritto di opposizione' (art. 21) il 'diritto a non essere sottoposto a decisioni automatizzate' (art. 22).

Parallelamente, il Regolamento riformula gli obblighi a carico del titolare quanto alle modalità di trattamento ed alle informazioni da fornire all'interessato, e ancora prescrive nuovi ed ulteriori 'adempimenti' quanto all'adozione di misura tecniche e organizzative per la sicurezza dei dati ed alla preventiva valutazione del rischio.

Il complesso di disposizioni, per un verso, dà concretezza sul piano positivo alle situazioni giuridiche che vengono in considerazio-

ne nella disciplina di settore, per altro verso, rischia di confondere l'interprete che, frastornato dalla enunciazione di una miriade di diritti ed obblighi, potrebbe essere indotto a compiere una lettura frammentaria, venendo in qualche misura a ripetere la risalente esperienza circa il novero dei diritti della personalità[28].

Suggestione della quale occorre essere consapevoli e che occorre tuttavia sforzarsi di superare, cercando di ricostruire ad unitarietà la posizione giuridica del soggetto cui i dati si riferiscono.

In tale prospettiva, un utile ausilio può essere trovato nel mutato quadro di riferimento delle norme apicali del sistema.

Mentre per la individuazione del diritto alla riservatezza l'interprete si confrontava con il dettato dell'art. 2 Cost. che esprime con formula aperta la garanzia della personalità, rispetto al trattamento dei dati personali l'interprete è ora quasi affrancato dal compito in quanto in termini espliciti la norma nell'art. 8 della Carta dei diritti fondamentali dell'Unione Europea e la norma dell'art. 16 del Trattato sul funzionamento dell'Unione Europea, enunciano con analoga formula il principio per cui «ogni persona ha diritto alla protezione dei dati personali che la riguardano»; una formula che nell'ordinamento interno è altresì recepita nell'art. 1 del Codice del trattamento dei dati personali[29].

La pluralità di enunciati presenti già nelle norme apicali dell'Unione europea, da un lato, solleva l'interprete dalle necessità di ricercare il fondamento positivo del diritto, dall'altro, messa a confronto con la vasta normativa, rende avvertiti del mutamento di significato che è venuto ad assumere il termine epigono della disciplina. Se anche la formula 'protezione dei dati personali' sembra evocare l'idea di appartenenza di beni alla persona che può pretenderne la protezione, la lettura complessiva del sistema di disposizioni dedicato al trattamento dei dati rende avvertiti della fallacia di una lettura del principio in termini di pretesa *ad excludendum*, così come avveniva in precedenza per la privacy, nell'accezione risalente del termine.

[28] Una efficace sintesi in D. Messinetti-F. Di Ciommo, *Diritti della personalità*, in S. Martuccelli-V. Pescatore (a cura di), *Diritto Civile*, Milano, Giuffrè, 2011, 599 ss.

[29] Al riguardo, se si vuole, v. V. Cuffaro, *Il principio di protezione dei dati*, in V. Cuffaro-R. D'Orazio-D. Ricciuto (a cura di), *Il codice del trattamento dei dati personali*, cit., 3 ss.

Al contrario la disciplina, come ora ribadisce l'art. 1 del Regolamento, coniuga il principio di protezione dei dati personali con la regola della libera circolazione dei dati. Ed è al riguardo significativo che nel medesimo art. 1 del Regolamento UE/2016/679 sia poi ribadito, nel comma 2, il diritto alla protezione dei dati personali ed insieme affermato, nel comma 3, che la libera circolazione dei dati personali dell'Unione non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali.

Per la nozione di privacy non è dunque più sufficiente il richiamo all'idea del rispetto dell'intimità della vita privata perché il complesso delle disposizioni affidate alla pluralità dei testi normativi, e da ultimo al Regolamento UE 2016/679, impongono di prendere atto di una disciplina improntata all'esigenza della circolazione dei dati personali, in relazione alla quale sono dettate regole precise dirette a tutelare l'interesse della persona rispetto al fenomeno inarrestabile e incontenibile della circolazione di dati.

La formula «diritto al controllo sul flusso di informazioni riguardanti la persona» della quale siamo debitori allo studioso che prime e più degli altri ha approfondito il tema[30] conferma la sua efficacia perché esprime con felice sintesi una realtà, quella del flusso dei dati personali in circolazione, ed insieme coglie la *ratio* complessiva di una disciplina finalizzata non già al divieto *della* circolazione, bensì al controllo *sulla* circolazione dei dati perché così è conformato l'interesse della persona rispetto a tutte le informazioni che la riguardano.

Il tempo trascorso consente di rilevare che privacy intesa come 'controllo' sui dati, ovvero come 'protezione dei dati', può dunque essere meglio intesa nell'attuale e diverso contesto fattuale e normativo. Piuttosto che richiamare il profilo della signoria sui dati, entrambe le formule esprimono la necessità che l'individuo abbia piena consapevolezza in ordine alle modalità con le quali sono trattate tutte quelle informazioni generate in una società che affida al trattamento dei dati personali lo svolgimento di gran parte delle attività economiche e su tale presupposto possa essere messo in grado

[30] Cfr. S. Rodotà, *Elaboratori elettronici e controllo sociale*, Bologna, il Mulino, 1973, 130.

di interloquire con chi svolge il trattamento ogni qual volta lo stesso risulti lesivo del diritto della personalità.

Di un diritto che, proprio in quanto volto a preservare il valore della persona, ha ancora motivo di essere considerato unitario.

La scelta di continuare a ritenere che la situazione giuridica soggettiva della persona fisica quanto al valore della persona debba essere considerata unitaria appare, d'altronde, cautela necessaria per realizzare una tutela adeguata rispetto al fenomeno del trattamento dei dati, segnato da una continua ed imponderabile evoluzione.

L'Autorità Garante per la protezione dei dati personali e le nuove sfide del Regolamento europeo

Augusta Iannini

Sommario: 1. L'impatto del Regolamento sull'organizzazione dell'Autorità Garante – 2. Gli effetti del d.lgs. n. 101/2018 – 3. Il rinnovato ruolo regolatorio dell'Autorità

1. L'impatto del Regolamento sull'organizzazione dell'Autorità Garante

Il titolo della relazione che mi è stata assegnata impone che raccolga la "sfida", descrivendo sinteticamente l'impatto che la nuova regolamentazione produrrà sull'organizzazione del Garante nazionale. Il regolamento europeo determina infatti diversi effetti sull'Autorità. Il primo interessa il settore fondamentale delle nostre attività, ovvero la competenza territoriale la cui individuazione è strettamente legata al luogo di stabilimento del titolare del trattamento. Questa indicazione determinerà una rivoluzione rispetto agli assetti attuali dell'Autorità, comporterà un enorme e nuovo lavoro di cooperazione tra le diverse istituzioni nazionali degli Stati membri, produrrà inevitabilmente l'insorgere di conflitti e la loro auspicabile composizione tra le diverse Autorità interessate e l'Autorità Capofila magari con l'intervento del Comitato europeo per la protezione dei dati, ultimo decisore della competenza di una Autorità nazionale rispetto all'altra. Pane quotidiano per le autorità giudiziarie ma non per la nostra Autorità. Lo sforzo organizzativo si preannuncia quindi notevole per un'istituzione che è stata sempre

abituata a spazi di riflessione di alto spessore, ora incompatibili con le nuove regole che impongono rapidità nell'affermazione del proprio ruolo e accettazione della propria responsabilità, anche in quei settori che il regolamento lascia alla discrezionalità degli Stati membri.

Altri effetti diretti del regolamento si produrranno nell'istituzionalizzazione del dialogo con la nuova figura del "data protection officer". Ancora tutto da approfondire il tema delle certificazioni e la loro incidenza rispetto al principio della responsabilizzazione del titolare del trattamento. Ancora non chiarita appare l'entità della risposta sanzionatoria rispetto alle violazioni accertate, non essendo previsto nel regolamento il livello minimo della sanzione ma soltanto il massimo: aspetto di eccentricità rispetto ai nostri principi e di problematicità di fronte ad una normativa di adeguamento che non ha affrontato questo tema.

2. Gli effetti del d.lgs. n. 101/2018

Sussistono poi degli effetti che scaturiscono proprio dalla normativa nazionale che ha dettato una disciplina ulteriore con riferimento alle materie rimesse alla discrezionalità degli Stati membri. Da pochi mesi è entrato in vigore il decreto legislativo 10 agosto 2018 n. 101, sul quale l'Autorità aveva espresso un circostanziato parere.

Dal coordinamento dei due testi che offrono ora una disciplina organica della tutela dei dati personali a livello nazionale, si possono individuare le scelte del legislatore.

Sotto il profilo dei poteri e del ruolo delle Autorità nazionali, il regolamento offre una precisa indicazione che è quella di assegnare al titolare del trattamento la responsabilità ("responsabilizzazione") delle scelte adottate per la tutela dei dati personali, evitando, ove possibile, l'intervento preventivo del potere pubblico e rimettendo ai singoli titolari la valutazione in ordine alle garanzie che devono accompagnare i differenti trattamenti. Tutto questo in una cornice che è diretta a limitare al minimo gli adempimenti formali richiesti. Tanto è vero che sono soppresse le notificazioni al Garante, le verifiche preliminari obbligatorie e quant'altro. Però, allo stesso tempo, il regolamento ha lasciato agli Stati membri uno spazio di libertà in specifici ambiti ritenendo che potesse essere

lecito e consentito introdurre misure anche più rigide, condizioni ulteriori per i trattamenti che vengono ritenuti più a rischio, recuperando un ruolo per le autorizzazioni formali da parte delle autorità di controllo. Mi riferisco alle ipotesi dell'art. 9 paragrafo 4, dell'art. 36 paragrafo 5, di tutti i trattamenti che sono previsti nel capo 9 del regolamento.

Il legislatore nazionale aveva due opzioni: lasciare uno spazio di autonomia ai titolari del trattamento oppure sfruttare al massimo le opportunità offerte dalle clausole di flessibilità. Nonostante la lettura del decreto sia resa assai faticosa per il necessario coordinamento tra tre testi, il regolamento, il codice della privacy e il nuovo decreto legislativo che modifica il codice del 2003 con incisi e inserimenti, emerge in modo non equivoco che l'Autorità riprende, per quanto possibile ed in alcuni settori, il suo ruolo tradizionale di autorità che indica preventivamente le regole del trattamento e che quindi non si limita soltanto a valutare l'operato dei titolari per poi sanzionarli per le loro scelte.

Da che cosa si evince questa tendenza? Intanto dalla scelta di lasciare al Garante l'individuazione preventiva delle misure da utilizzare nel trattamento di quelle particolari categorie di dati che, utilizzando una definizione consolidata, sinteticamente definirò "sensibili" oppure, ancora, dalla conservazione delle vecchie autorizzazioni generali che diventano, in quei settori oggetto di clausole di flessibilità, regole di deontologia con valore di condizioni di liceità e di correttezza del trattamento o infine anche dalla necessità di una autorizzazione del Garante per l'utilizzo a fini scientifici e di ricerca da parte di terzi di dati raccolti da altro soggetto.

3. Il rinnovato ruolo regolatorio dell'Autorità

L'immagine dell'Autorità, come descritta nel decreto legislativo, con il recupero, nelle materie in cui ha discrezionalità, dei suoi poteri regolatori tradizionali, è coerente con il principio di responsabilizzazione del titolare? Uso il termine "coerente" riferendomi proprio a quel principio di coerenza che informa il regolamento. È coerente con i contenuti di quei principi che impongono la responsabilizzazione del titolare con la conseguente sua valutazione sui rischi del trattamento? Sono consapevole che un'Autorità che ac-

compagna questo processo di responsabilizzazione con indicazioni preventive consente un grande vantaggio agli operatori, garantendo loro di essere sostenuti in quelle scelte impegnative che in maniera brutale il regolamento, introducendo concetti come *privacy by design*, *privacy by default*, responsabilizzazione, prevenzione, ha loro imposto.

Da tempo la legislazione europea ha elevato la prevenzione a percorso privilegiato: la normativa sulla responsabilità delle persone giuridiche ne è stato il primo esempio significativo. Al momento della implementazione nel nostro sistema giuridico delle convenzioni internazionali che imponevano l'introduzione di un principio del tutto nuovo rappresentato dalla responsabilità delle persone giuridiche scaturente da reato, le imprese, allarmate da una valutazione dell'autorità giudiziaria sulle modalità organizzative delle proprie aziende in funzione di prevenzione dalla commissione di reati, ottennero che il Ministero della Giustizia approvasse dei codici di comportamento aventi valenza generale su cui poi furono elaborati i modelli di organizzazione. A distanza di tempo quell'operazione non è stata però efficace perché quei modelli non sono stati valutati come idonei ad escludere la responsabilità degli enti, almeno secondo la giurisprudenza prevalente.

Sulla finalità di prevenzione del rischio derivante dal trattamento dei dati personali la scelta del legislatore delegato è stata diversa ed approfittando dell'esistenza di un'Autorità indipendente, si è nuovamente disegnato per questa istituzione un ruolo di regolazione, di suggerimento, di indirizzo.

Nonostante una mia istintiva predilezione per le scelte più estreme del Regolamento europeo, credo che gli operatori apprezzeranno questo ruolo per la maggiore certezza che offre ai titolari del trattamento ed agli interessati. Ma l'Autorità dovrà contemperare questa sua rinnovata missione con lo scopo del regolamento che è la libera circolazione dei dati, assicurando lo sviluppo dell'economia digitale in sicurezza. Quindi necessità di un costante confronto con le normative di adeguamento degli altri Stati membri che dovranno essere monitorate, valutate, approfondite alla luce del rispetto del principio di coerenza. Gli spazi di tolleranza rispetto ai principi fondanti del regolamento non potranno essere evanescenti per non riprodurre quelle concorrenzialità tra gli Stati membri, anche nel settore della tutela dei dati personali, in tutti quei settori (lavoro, manifestazio-

ne del pensiero, pubblica amministrazione etc.) rimessi alla loro discrezionalità. È in gioco il raggiungimento di un equilibrio difficile rispetto ad un tema di libertà che colloca il dato personale all'interno di diritti indisponibili.

L'oggetto del Regolamento Generale sulla protezione dei dati: tra diritto alla privacy e libera circolazione dei dati personali*

José Luis Piñar Mañas

Sommario: 1. Introducción. El doble objeto de la Directiva 95/46/ce y del Reglamento – 2. El nuevo Reglamento y el derecho fundamental a la protección de datos – 3. Protección de datos y libre circulación de datos dentro de la Unión Europea – 4. Conclusiones – Bibliografia

1. Introducción. El doble objeto de la Directiva 95/46/CE y del reglamento

Ya la Directiva 95/46/CE tenía como referencia dos ejes esenciales: que el tratamiento de datos personales no afectase a los derechos

* Una primera versión de este trabajo ha sido publicado en J.L. Piñar (a cura di), *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad*, Madrid, Editorial Reus, 2016, 51-62. El presente trabajo se ha iniciado en el marco del Proyecto de Investigación sobre "*Protección de datos y aplicación extraterritorial de las normas. La reforma de la Directiva 95/46/CE*", Ref. DER2012-35948, y continúa en el marco del Proyecto DER2016-79819-R, del Programa estatal de investigación, Desarrollo e Innovación Orientada a los Retos de la Sociedad, del Ministerio Español de Economía y Competitividad, sobre "*Protección de datos, seguridad e innovación: retos en un mundo global tras el Reglamento Europeo de Protección de Datos*", de los que soy investigador principal.

fundamentales y que se garantizase la libre circulación de los datos entre los Estados miembros[1].

El Reglamento sigue la misma tónica, aunque con algún avance conceptual, como veremos. Ya su propio título (como el de la Directiva) hace referencia a los dos elementos[2], y su artículo 1.1 dispone que «Il presente regolamento stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati».

El objeto, por tanto, es doble: regular un derecho (la protección de datos) y garantizar una libertad (la libre circulación de los datos)[3]. No podemos pues ignorar esta realidad ni dejar de resaltarla. Tanto en la construcción del mercado interior como en el seno de la Unión Europea el derecho a la protección de datos era y es fundamental y la libre circulación de datos necesaria. Y el marco de referencia de uno y otra es ahora el Reglamento, que tampoco puede ni debe ignorar el alcance económico que tiene el uso de los datos en la actualidad. Su considerando 2 lo reconoce: «Il presente regolamento è inteso a contribuire alla realizzazione di uno spazio di libertà, sicurezza e giustizia e di un'unione economica, al progresso economico e sociale, al rafforzamento e alla convergenza delle economie nel mercato interno e al benessere delle persone fisiche». Ese marco económico, en el que en no pocas ocasiones y necesariamente se mueve el tratamiento de datos, no puede ser, como digo, ni ignorado ni descuidado. Pero teniendo muy presente que en todo caso el derecho fundamental a la protección de datos prevalece sobre el interés económico de los responsables y encargados, como ya ha puesto de manifiesto el Tri-

[1] El considerando tercero del GDPR lo recuerda: «La direttiva 95/46/CE del Parlamento europeo e del Consiglio ha come obiettivo di armonizzare la tutela dei diritti e delle libertà fondamentali delle persone fisiche rispetto alle attività di trattamento dei dati e assicurare la libera circolazione dei dati personali tra Stati membri».

[2] Reglamento "relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati…".

[3] Muy claro es también el considerando 166: "…gli obiettivi del regolamento [sono] tutelare i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali, e garantire la libera circolazione di tali dati nell'Unione…". También el considerando 170, con interesantes referencias a los principios de subsidiariedad y proporcionalidad.

bunal de Justicia en su Sentencia de 13 de mayo de 2014, *Google Spain y Agencia Española de Protección de Datos (AEPD)*, asunto C 131/12[4].

Por otra parte el Reglamento es consciente de que la innovación tecnológica tiene una incidencia capital en la protección de datos, pero que ha de alcanzarse necesariamente un equilibrio entre una y otra, para nada incompatibles[5]. El considerando 6 lo pone de manifiesto:

> La rapidità dell'evoluzione tecnologica e la globalizzazione comportano nuove sfide per la protezione dei dati personali. La portata della condivisione e della raccolta di dati personali è aumentata in modo significativo. La tecnologia attuale consente tanto alle imprese private quanto alle autorità pubbliche di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività. Sempre più spesso, le persone fisiche rendono disponibili al pubblico su scala mondiale informazioni personali che li riguardano. La tecnologia ha trasformato l'economia e le relazioni sociali e dovrebbe facilitare ancora di più la libera circolazione dei dati personali all'interno dell'Unione e il loro trasferimento verso paesi terzi e organizzazioni internazionali, garantendo al tempo stesso un elevato livello di protezione dei dati personali.

2. El nuevo Reglamento y el derecho fundamental a la protección de datos

El artículo 8 de la Carta Europea de Derechos Humanos reconoce, como es sabido, el derecho fundamental a la protección de datos. No son muchos los textos constitucionales[6] que lo reconocen de forma

[4] Considerandos 97 y 99. El Tribunal lleva esa consideración incluso al propio fallo de la Sentencia.

[5] Sobre ello vid. M. Recio Gayo, *Protección de datos e innovación: ¿(in) compatibles?*, Madrid, Editorial Reus, 2016.

[6] Considero la Carta como un texto de naturaleza constitucional. Vid. J. Roldan Barbero, *La Carta de Derechos Fundamentales de la UE: su estatuto con-*

tan clara y expresa[7]. El avance que ya en el año 2000 se produjo en Europa, con un reflejo incuestionable a nivel mundial, fue extraordinario. El derecho a la protección de datos se elevó a la categoría de derecho fundamental autónomo, emancipado del derecho a la intimidad, lo que queda demostrado por el hecho de que la propia Carta reconoce el derecho a la intimidad personal y familiar en un artículo distinto, el 7[08].

Por su parte el artículo 16 del Tratado de Funcionamiento de la Unión Europea (antiguo artículo 286 TCE) reconoce asimismo el derecho y añade que «Il Parlamento europeo e il Consiglio, deliberando secondo la procedura legislativa ordinaria, stabiliscono le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale da parte delle istituzioni, degli organi e degli organismi dell'Unione, nonché da parte degli Stati membri nell'esercizio di attività che rientrano nel campo di applicazione del diritto dell'Unione, e le norme relative alla libera circolazione di tali dati». En fin, el artículo 39 del

stitucional, en *Revista de Derecho Comunitario Europeo*, año 7, núm. 16. septiembre-diciembre 2003, 943 y ss. Sin referirse a la Carta, por obvios motivos cronológicos, véase L.M. Díez-Picazo, *¿Una Constitución sin declaración de derechos? (Reflexiones constitucionales sobre los derechos fundamentales en la Comunidad Europea)*, en *Revista Española de Derecho Constitucional*, año 11, núm. 32, mayo-agosto 1991, 135 y ss.

[7] El artículo 16 de la Constitución mejicana es uno de esos casos. Vid. J.L. Piñar Mañas-L. Ornelas, *La Protección de Datos Personales en México*, México, D.F., Tirant lo Blanch, 2013.

[8] La bibliografía sobre los artículos 7 y 8 de la Carta es muy abundante. También otros preceptos de la Carta han de ser tenidos en cuenta. Vid. por todos J. Martin-Pérez de Nanclares, *Comentario al artículo 7* y *Comentario al artículo 8*, en A. Mangas Martín (a cura di), *Carta de los Derechos Fundamentales de la Unión Europea. Comentario artículo por artículo*, Madrid, Fundación BBVA, 2008, 209 y ss.; C. Ruiz Miguel, *El derecho a la protección de los datos personales en la Carta de Derechos Fundamentales de la Unión Europea: análisis crítico*, en *Revista de Derecho Comunitario Europeo*, año 7, núm. 14, enero-abril 2003, 7 y ss. S. Rodotà, *Democracia y protección de datos*, en *Cuadernos de Derecho Público*, nº 19-20, Monográfico sobre Protección de Datos, 15 y ss. Rodotà fue decisivo en el reconocimiento del derecho a la protección de datos en la Carta. De dicho autor también es esencial su obra *La vida y las reglas. Entre el derecho y el no derecho*, Trotta, Madrid, 2010, 69 y ss. (traducción del original *La vita e le regole. Tra diritto e non diritto*).

Tratado de la Unión Europea se refiere asimismo al derecho a la protección de datos[9].

La Directiva 95/46/CE es previa tanto a la Carta como al Tratado de Funcionamiento. No pudo por tanto tener en cuenta ni una ni otro. Por ello es lógico que no les dedique referencia alguna. Por el contrario sí busca su fundamento en el Convenio Europeo de Derechos Humanos[10]. En este sentido el considerando primero de la Directiva recuerda que uno de los objetivos de la Comunidad es «promuovere la democrazia basandosi sui diritti fondamentali sanciti dalle costituzioni e dalle leggi degli Stati membri nonché dalla convenzione europea di salvaguardia dei diritti dell'uomo e delle libertà fondamentali». Éste reconoce en su artículo 8 el derecho al respeto a la vida privada y familiar. A él se refiere el importante considerando 10 de la propia Directiva[11]. Por tanto ésta regula la protección de datos adelantándose a cualquier reconocimiento del mismo en las normas de derecho originario europeo y teniendo

[9] Artículo 39: «Conformemente all'articolo 16 del trattato sul funzionamento dell'Unione europea e in deroga al paragrafo 2 di detto articolo, il Consiglio adotta una decisione che stabilisce le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale da parte degli Stati membri nell'esercizio di attività che rientrano nel campo di applicazione del presente capo, e le norme relative alla libera circolazione di tali dati. Il rispetto di tali norme è soggetto al controllo di autorità indipendenti».

[10] También tiene en cuenta el Convenio 108, pero con la idea de superarlo. Así se desprende del considerando 11: «Considerando che i principi della tutela dei diritti e delle libertà delle persone, in particolare del rispetto della vita privata, contenuti dalla presente direttiva precisano ed ampliano quelli enunciati dalla convenzione del 28 gennaio 1981 del Consiglio d'Europa sulla protezione delle persone con riferimento al trattamento automatizzato dei dati di carattere personale».

[11] «Considerando che le legislazioni nazionali relative al trattamento dei dati personali hanno lo scopo di garantire il rispetto dei diritti e delle libertà fondamentali, in particolare del diritto alla vita privata, riconosciuto anche dall'articolo 8 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali e dai principi generali del diritto comunitario; che pertanto il ravvicinamento di dette legislazioni non deve avere per effetto un indebolimento della tutela da esse assicurata ma deve anzi mirare a garantire un elevato grado di tutela nella Comunità». La Directiva también tiene en cuenta el artículo 10 del Convenio sobre libertad de expresión e información (ver Considerando 37).

muy presente el derecho a la intimidad. En consonancia con ello el artículo 1º.1 de la Directiva dispone que «Gli Stati membri garantiscono, conformemente alle disposizioni della presente direttiva, la tutela dei diritti e delle libertà fondamentali delle persone fisiche e particolarmente del diritto alla vita privata, con riguardo al trattamento dei dati personali». Es decir, la Directiva pretende que los tratamientos de datos no violen los derechos fundamentales y en particular el derecho a la intimidad[12]. Este es también el planteamiento del Tribunal de Justicia en las primeras sentencias en que interpreta la Directiva[13]. En particular, ya afirmó en la Sentencia de 20 de mayo de 2003, *Rundfunk*, asuntos acumulados C-465/00, C-138/01 y C-139/0, que «le disposizioni della direttiva 95/46, poiché disciplinano il trattamento di dati personali che possono arrecare pregiudizio alle libertà fondamentali e, in particolare, al diritto alla vita privata, devono essere necessariamente interpretate alla luce dei diritti fondamentali, che secondo una costante giurisprudenza fanno parte integrante dei principi generali del diritto dei quali la Corte garantisce l'osservanza (v., segnatamente, sentenza 6 marzo 2001, causa C-274/99 P, Connolly/Commissione, Racc. pag. I-1611, punto 37)»[14]. Y en sus apartados 71 y siguientes pone de manifiesto que su análisis se basa en el artículo 8 del Convenio Europeo de Derechos Humanos.

[12] El considerando 2 lo deja claro: «Considerando che i sistemi di trattamento dei dati sono al servizio dell'uomo; che essi, indipendentemente dalla nazionalità o dalla residenza delle persone fisiche, debbono rispettare le libertà e i diritti fondamentali delle stesse, in particolare la vita privata, e debbono contribuire al progresso economico e sociale, allo sviluppo degli scambi nonché al benessere degli individui».

[13] Vid. J.L. Piñar Mañas-M. Recio Gayo, *El derecho a la protección de datos en la jurisprudencia del Tribunal de Justicia de la Unión Europea*, Madrid, La Ley Wolters Kluwer, 2018; J.L. Piñar Mañas, *El derecho a la protección de datos de carácter personal en la jurisprudencia del Tribunal de Justicia de las Comunidades Europeas*, en *Cuadernos de Derecho Público*, nº 19-20, Monográfico sobre Protección de Datos, 45 y ss. Ha sido traducido al inglés: *ECJ Case Law on the Right to Protection of Personal Data. Part. 1*, en *BNA International. World Data Protection Report*, volumen 6, nº 1, enero 2006, 3-11; La segunda parte, en la misma Revista, volumen 6, nº 2, febrero, 2006, 23-32.

[14] Apartado 68. Lo mismo ha reiterado la Sentencia de 13 de mayo de 2014 en el caso Google (también apartado 68).

La Jurisprudencia del Tribunal de Justicia fue evolucionando (hay que decir que lentamente hasta 2014) al objeto de tener en cuenta el artículo 8 de la Carta Europea de Derechos Humanos. En particular son capitales las Sentencias de 8 de abril de 2014, *Digital Rights Ireland Ltd*, asuntos acumulados C293/12 y C594/12, por la que se declara inválida la Directiva de retención de datos, de 13 de mayo de 2014, *Google Spain y Agencia Española de Protección de Datos (AEPD)*, asunto C 131/12, sobre derecho al olvido frente a los buscadores y en particular frente a Google, o la de 6 de octubre de 2015, *Maximillian Schrems*, asunto C-362/14, por la que declara inválida la Decisión 2000/520/CE, de 26 de julio de 2000, sobre la adecuación a la Directiva 95/46/CE de los principios de puerto seguro[15].

La aprobación de la Carta ha sido decisiva en la redacción del Reglamento General de Protección de Datos. La consideración de la protección de datos como derecho fundamental y el artículo 8 de la Carta están en la base misma del Reglamento, uno de cuyos objetivos es precisamente la regulación del derecho a la protección de datos. Su Considerando 1 es claro: «La protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale. L'articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea ("Carta") e l'articolo 16, paragrafo 1, del trattato sul funzionamento dell'Unione europea ("TFUE") stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano»[16].

Es decir, el Reglamento ya no sólo pretende que los tratamientos de datos no violen los derechos fundamentales y en particular el derecho a la intimidad, sino que parte de la base de que el simple hecho de tratar datos personales puede violar el derecho a la protección de datos de carácter personal. El objeto del Reglamento se aclara respecto al de la Directiva: regular el derecho a la protección de datos de carácter personal, ahora reconocido en el artículo 8 de la Carta. Lo que no debe hacer olvidar que el tratamiento de datos personales

[15] Hay que decir, además, que al plantear las correspondientes cuestiones prejudiciales en cada una de esas sentencias siempre se invocaba el artículo 8 de la Carta, que por tanto y necesariamente ha debido ser interpretado por el Tribunal de Justicia.

[16] Ver asimismo el considerando 12.

tiene una incidencia especial e innegable en otros muchos derechos fundamentales. Así lo manifiesta el considerando 4:

> Il trattamento dei dati personali dovrebbe essere al servizio dell'uomo. Il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità. Il presente regolamento rispetta tutti i diritti fondamentali e osserva le libertà e i principi riconosciuti dalla Carta, sanciti dai trattati, in particolare il rispetto della vita privata e familiare, del domicilio e delle comunicazioni, la protezione dei dati personali, la libertà di pensiero, di coscienza e di religione, la libertà di espressione e d'informazione, la libertà d'impresa, il diritto a un ricorso effettivo e a un giudice imparziale, nonché la diversità culturale, religiosa e linguistica.

En definitiva, pues, el Reglamento tiene como uno de sus objetos principales la regulación del derecho fundamental a la protección de datos de carácter personal reconocido en el artículo 8 de la Carta Europea de Derechos Fundamentales. Así se afirma expresamente en sus considerandos, pese a que ninguna referencia a la Carta haya en el articulado. Ni siquiera en el artículo 1.2 según el cual el Reglamento «protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali».

El Reglamento no contiene una definición del derecho a la protección de datos. Tampoco el Tribunal de Justicia lo ha definido, pese a que como hemos visto se ha ocupado de él ya en varias ocasiones. En mi opinión, como sí ha señalado el Tribunal Constitucional español más de una vez y muy destacadamente en la Sentencia 292/2000, de 30 de noviembre, debe entenderse que tal derecho atribuye a las personas físicas el poder de disposición sobre sus propios datos, sean o no íntimos, siempre que estén o vayan a estar sometidos a un tratamiento, informatizado o no. El Reglamento en el considerando 7 afirma, casi de pasada, que «le persone fisiche abbiano il controllo dei dati personali che li riguardano». Ese control es precisamente el

elemento central del derecho[17], el que justifica sus principios[18] y el reconocimiento de los derechos de los afectados[19].

3. Protección de datos y libre circulación de datos dentro de la Unión Europea

La regulación del derecho fundamental a la protección de datos debe ser compatible con su libre circulación dentro de la Unión Europea. Ya lo exigía la Directiva 95/46/CE y así lo exige también el Reglamento: su artículo 1.3 dispone que «la libera circolazione dei dati personali nell'Unione non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali».

En este sentido es muy importante hacer referencia al título que habilitó la aprobación de la Directiva y el que ha sido base para la aprobación del Reglamento.

Como ya he recordado en otro lugar[20], en la ya citada Sentencia del Tribunal de Justicia de 20 de mayo de 2003, *Rundfunk*, se planteó específicamente el tema de determinar si la Directiva se vincula exclusivamente al ejercicio de las libertades comunitarias y en particular a la libre circulación entre Estados miembros. La duda, desde el punto de vista técnico-jurídico comunitario se plantea desde el momento en que la adopción de la Directiva se

[17] Véase por todos C. Lesmes Serrano, *Comentario al artículo 1*, en C. Lesmes Serrano (a cura di), *La Ley de Protección de Datos. Análisis y comentario de su jurisprudencia*, Valladolid, Lex Nova, 2008, 48 y ss. P. Lucas Murillo de la Cueva-J.L. Piñar Mañas, *El derecho a la autodeterminación informativa*, Madrid, Fundación Coloquio Jurídico Europeo, 2009; R. Martínez, *Una aproximación crítica a la autodeterminación informativa*, Madrid, Civitas, 2004. J.L. Piñar Mañas, *Derecho fundamental a la protección de datos personales. Algunos retos de presente y futuro*, en *Asamblea: Revista Parlamentaria de la Asamblea de Madrid*, n.º 13, 2005, 21-46. S. Rodotà, *La vida y las reglas. Entre el derecho y el no derecho*, *op. cit*. A. Troncoso Reigada, *La Protección de datos personales. En busca del equilibrio*, Valencia, Tirant lo Blanch, 2011.

[18] Artículos 5 a 11 del Reglamento.

[19] Artículos 12 a 23.

[20] "El derecho a la protección de datos de carácter personal en la jurisprudencia del Tribunal de Justicia…", *op. cit*., 73-74.

fundamentó en el artículo 100-A del Tratado Constitutivo de la Comunidad Europea.

El Tribunal recuerda que

> la direttiva 95/46, adottata sulla base dell'art. 100 A del Trattato, mira a garantire la libera circolazione tra gli Stati membri dei dati personali attraverso l'armonizzazione delle disposizioni nazionali sulla tutela delle persone fisiche rispetto al trattamento di tali dati. Infatti, l'art. 1 della detta direttiva, che definisce l'oggetto di quest'ultima, dispone, al suo n. 2, che gli Stati membri non possono restringere o vietare la libera circolazione dei dati personali tra Stati membri, per motivi connessi alla tutela dei diritti e delle libertà fondamentali delle persone fisiche, in particolare della loro vita privata, rispetto al trattamento di tali dati[21].

Partiendo de esta base el Tribunal concluye que «poiché tutti i dati personali possono circolare tra gli Stati membri, la direttiva 95/46 impone in linea di principio il rispetto delle norme di tutela di tali dati rispetto a qualsiasi trattamento di questi ultimi, come disposto dal suo art. 3»[22].

Dicho esto, el Tribunal recuerda que, como ya ha tenido ocasión de señalar en numerosas ocasiones[23], «il ricorso alla base giuridica dell'art. 100 A del Trattato non presuppone l'esistenza di un nesso effettivo con la libera circolazione tra Stati membri in ciascuna delle situazioni previste dall'atto fondato su tale base. [...], ciò che rileva [...] è che l'atto adottato su tale fondamento abbia effettivamente ad oggetto il miglioramento delle condizioni di instaurazione e di funzionamento del mercato interno». De modo que la aplicabilidad de la Directiva no puede depender de la cuestión de si las situaciones concretas de que se trate «presentino un nesso sufficiente con l'esercizio

[21] Punto 39.

[22] Punto 40.

[23] Cita las sentencias de 5 de octubre de 2000, *Alemania/Parlamento y Consejo*, C-376/98, Rec. p. I-8419, apartado 85, y de 10 de diciembre de 2002, *British American Tobacco (Investments) e Imperial Tobacco*, C-491/01, Rec. p. I-0000, apartado 60.

delle libertà fondamentali garantite dal Trattato [...] Infatti, un'interpretazione in senso contrario rischierebbe di rendere particolarmente incerti ed aleatori i limiti del campo di applicazione della detta direttiva, il che sarebbe contrario al suo obiettivo essenziale, che è quello di ravvicinare le disposizioni legislative, regolamentari, ed amministrative degli Stati membri per eliminare gli ostacoli al funzionamento del mercato interno derivanti proprio dalle disparità esistenti tra le normative nazionali»[24]. Esta doctrina se ha reiterado en la Sentencia *Linqvist*[25].

El Reglamento, por su parte, busca su fundamento en el artículo 16 del Tratado de Funcionamiento de la Unión Europea, que como sabemos reconoce el derecho que toda persona tiene a la protección de los datos de carácter personal que le conciernan, si bien incluye también una referencia a la libre circulación de esos datos. Esta circunstancia no es baladí, y debe interpretarse en el sentido de que la libre circulación de los datos personales en la Unión debe en todo caso respetar el contenido del derecho a la protección de datos. Cierto que aquélla no podrá ser restringida ni prohibida por motivos relacionados con dicha protección (lo que podría poner en riesgo el buen funcionamiento del mercado interior, como advierte el considerando 13), pero lo prioritario es respetar en todo caso el derecho reconocido en el artículo 8 de la Carta Europea de Derechos Humanos. Y hacerlo, además, de forma homogénea en toda la Unión. El Reglamento busca mayor homogeneidad, mayor uniformidad en el tratamiento de datos en la Unión Europea. Según el considerando 5 del Reglamento «l'integrazione eco-

[24] Puntos 41 y 42.

[25] La Sra. Lindqvist sostuvo que «un particular que, en el ejercicio de su libertad de expresión, crea diversas páginas web en el marco de una actividad sin ánimo de lucro o en su tiempo de ocio, no realiza una actividad económica y, por tanto, su conducta no está sujeta al Derecho comunitario. Si el Tribunal de Justicia declarara lo contrario, se plantearía la cuestión de la validez de la Directiva 95/46, puesto que al adoptarla el legislador comunitario se habría excedido en las competencias que le confiere el artículo 100 A del Tratado CE (actualmente artículo 95 CE, tras su modificación). En efecto, la aproximación de las legislaciones, que tiene por objeto el establecimiento y el funcionamiento del mercado interior no puede servir de base legal para adoptar medidas comunitarias que regulen el Derecho de los particulares a la libertad de expresión en Internet» (ver punto 30 de la Sentencia).

nomica e sociale conseguente al funzionamento del mercato interno ha condotto a un considerevole aumento dei flussi transfrontalieri di dati personali[26]». Esta situación requiere «un quadro più solido e coerente in materia di protezione dei dati nell'Unione, affiancato da efficaci misure di attuazione, data l'importanza di creare il clima di fiducia che consentirà lo sviluppo dell'economia digitale in tutto il mercato interno» (considerando 7). Pues lo que sí puede poner en peligro el mercado único no es tanto un modelo riguroso de protección de datos sino la disparidad de regímenes jurídicos entre los distintos Estados miembros. Este es uno de los puntos que más se ha criticado de la Directiva 95/46/CE: no haber impedido

> la frammentazione dell'applicazione della protezione dei dati personali nel territorio dell'Unione, né ha eliminato l'incertezza giuridica o la percezione, largamente diffusa nel pubblico, che in particolare le operazioni online comportino rischi per la protezione delle persone fisiche. La compresenza di diversi livelli di protezione dei diritti e delle libertà delle persone fisiche, in particolare del diritto alla protezione dei dati personali, con riguardo al trattamento di tali dati negli Stati membri può ostacolare la libera circolazione dei dati personali all'interno dell'Unione. Tali differenze possono pertanto costituire un freno all'esercizio delle attività economiche su scala dell'Unione, falsare la concorrenza e impedire alle autorità nazionali di adempiere agli obblighi loro derivanti dal diritto dell'Unione (considerando 9).

Para superar esta situación, repito, el camino a seguir no es el de debilitar la protección de datos, sino reforzar y especificar los derechos de los interesados y las obligaciones de quienes tratan y determinan el tratamiento de los datos de carácter personal, así como establecer mecanismos de control y supervisión y un régimen sancionador equivalente entre los distintos Estados miembros (consi-

[26] Los flujos transfronterizos de datos son los que se producen entre Estados miembros. No implican, pues, transferencia internacional de datos. Ver el artículo 4.23 del Reglamento.

derando 11). En definitiva, «assicurare un livello coerente ed elevato di protezione delle persone fisiche e rimuovere gli ostacoli alla circolazione dei dati personali all'interno dell'Unione», para lo que «il livello di protezione dei diritti e delle libertà delle persone fisiche con riguardo al trattamento di tali dati dovrebbe essere equivalente in tutti gli Stati membri» (considerando 10). Y para ello, para garantizar un nivel coherente de protección en toda la Unión y evitar divergencias que dificulten la libre circulación de datos personales dentro del mercado interior,

> è necessario un regolamento che garantisca certezza del diritto e trasparenza agli operatori economici, comprese le micro, piccole e medie imprese, offra alle persone fisiche in tutti gli Stati membri il medesimo livello di diritti azionabili e di obblighi e responsabilità dei titolari del trattamento e dei responsabili del trattamento e assicuri un monitoraggio coerente del trattamento dei dati personali, sanzioni equivalenti in tutti gli Stati membri e una cooperazione efficace tra le autorità di controllo dei diversi Stati membri. Per il buon funzionamento del mercato interno è necessario che la libera circolazione dei dati personali all'interno dell'Unione non sia limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali.

4. Conclusiones

En definitiva, el mercado interior, seña de identidad de la Unión Europea, necesita de la protección de datos y de la libre circulación de estos datos en base a un régimen uniforme en todos los Estados miembros, lo que se pretende conseguir a través del nuevo Reglamento, intentando superar las divergencias que trajo consigo la Directiva 95/46/CE.

El objeto del Reglamento es en este sentido doble: regular el derecho fundamental a la protección de datos que reconoce el artículo 8 de la Carta Europea de Derechos Humanos y garantizar la libre circulación de dichos datos dentro de la Unión Europea. Pero siem-

pre partiendo de la base de que esa libre circulación en ningún caso puede justificar una reducción en el nivel de protección.

Bibliografia

L.M. Díez-Picazo, ¿Una Constitución sin declaración de derechos? (Reflexiones constitucionales sobre los derechos fundamentales en la Comunidad Europea), en *Revista Española de Derecho Constitucional*, año 11, núm. 32, mayo-agosto 1991, 135 y ss.

C. Lesmes Serrano, *Comentario al artículo 1*, en C. Lesmes Serrano (a cura di), *La Ley de Protección de Datos. Análisis y comentario de su jurisprudencia*, Valladolid, Lex Nova, 2008, 48 y ss.

P. Lucas Murillo de la Cueva-J.L. Piñar Mañas, *El derecho a la autodeterminación informativa*, Madrid, Fundación Coloquio Jurídico Europeo, 2009.

J. Martín-Pérez de Nanclares, *Comentario al artículo 7* y *Comentario al artículo 8*, en A. Mangas Martín (a cura di), *Carta de los Derechos Fundamentales de la Unión Europea. Comentario artículo por artículo*, Madrid, Fundación BBVA, 2008, 209 y ss.

R. Martínez, *Una aproximación crítica a la autoderminación informativa*, Madrid, Civitas, 2004.

J.L. Piñar Mañas, *El derecho a la protección de datos de carácter personal en la jurisprudencia del Tribunal de Justicia de las Comunidades Europeas*, en *Cuadernos de Derecho Público*, nº 19-20, Monográfico sobre Protección de Datos, 45 y ss. Ha sido traducido al inglés: *ECJ Case Law on the Right to Protection of Personal Data. Part. 1*, en *BNA International. World Data Protection Report*, volumen 6, nº 1, enero 2006, 3-11; la segunda parte, en la misma Revista, volumen 6, nº 2, febrero, 2006, 23-32.

Derecho fundamental a la protección de datos personales. Algunos retos de presente y futuro, en *Asamblea: Revista Parlamentaria de la Asamblea de Madrid*, n.º 13, 2005, 21-46.

J.L. Piñar Mañas (a cura di), *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad*, Madrid, Editorial Reus, 2016.

J.L. Piñar Mañas-M. Recio Gayo, *El derecho a la protección de datos en la jurisprudencia del Tribunal de Justicia de la unión Europea*, Madrid, La Ley Wolters Kluwer, 2018.

M. Recio Gayo, *Protección de datos e innovación: ¿(in) compatibles?*, Madrid, Editorial Reus, 2016.

S. Rodotà, *Democracia y protección de datos*, en *Cuadernos de Derecho Público*, nº 19-20, Monográfico sobre Protección de Datos, 15 y ss.

La vida y las reglas. Entre el derecho y el no derecho, Madrid, Trotta, 2010 (traducción del original italiano *La vita e le regole. Tra diritto e non diritto*).

J. Roldan Barbero, *La Carta de Derechos Fundamentales de la UE: su estatuto constitucional*, en *Revista de Derecho Comunitario Europeo*, año 7, núm. 16, septiembre-diciembre 2003, 943 y ss.

C. Ruiz Miguel, *El derecho a la protección de los datos personales en la Carta de Derechos Fundamentales de la Unión Europea: análisis crítico*, en *Revista de Derecho Comunitario Europeo*, año 7, núm. 14, enero-abril 2003, 7 y ss.

A. Troncoso Reigada, *La Protección de datos personales. En busca del equilibrio*, Valencia, Tiran lo Blanch, 2011.

GDPR e Intelligenza Artificiale

Codici di condotta, certificazioni, sigilli, marchi e altri poteri di *soft law* previsti dalle leggi nazionali di adeguamento: strumenti essenziali per favorire una applicazione proattiva del Regolamento europeo nell'epoca della IA[*]

Franco Pizzetti

Sommario: 1. Il GDPR e le leggi nazionali di adeguamento: un quadro di riferimento – 2. GDPR e Intelligenza Artificiale: un problema aperto – 3. I Codici di condotta e l'Intelligenza Artificiale nel quadro del GDPR (e della legislazione nazionale di adeguamento)

1. Il GDPR e le leggi nazionali di adeguamento: un quadro di riferimento

1.1. Il Regolamento europeo 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali,

[*] Il presente testo costituisce una sintesi dell'intervento svolto al Convegno "L'entrata in vigore del Regolamento UE 20167679. La riforma alla prova della prassi in Italia e in Spagna", Pisa, 8-9 giugno 2018, ripreso successivamente nel corso della Tavola rotonda "Macchine intelligenti e automazione responsabile", Pisa, 12 ottobre 2018, coordinata dalla prof.ssa Dianora Poletti nel quadro degli eventi dell'Internet Festival svoltosi in data 12 e 13 ottobre 2018 sul tema *Intelligenza artificiale e nuovi diritti*.
Franco Pizzetti ha trattato più ampiamente il tema nel saggio *La protezione dei dati personali e la sfida dell'Intelligenza Artificiale*, in F. Pizzetti, *Intelligenza artificiale, protezione dei dati personali e regolazione*, Torino Giappichelli, 2018. Al volume citato hanno contribuito con saggi autonomi, R. Angelini, M. Bassani, D.Benedetti, R. Bifulco, A. Caselli, G. D'Acquisto, G.F. Italiano, L. Liguori, A. Massolo, M. Naldi, O. Pollicino, A. Spina.

nonché alla libera circolazione di tali dati, ormai noto come il GDPR, segue due direttrici di fondo, che è assolutamente necessario tenere sempre ben presenti: la prima, ovviamente, è assicurare una elevata tutela delle persone fisiche e dei loro diritti rispetto ai trattamenti dei dati personali; la seconda, è quella di creare un clima di fiducia nell'effettiva tutela dei trattamenti legati alla libera circolazione dei dati nella società digitale anche al fine di favorire "lo sviluppo dell'economia digitale in tutto il mercato interno".

Queste due linee strategiche sono espresse con la massima chiarezza nei primi sette Considerando, il cui contenuto deve orientare tutta la lettura, interpretazione e applicazione delle norme contenute nel GDPR e nelle leggi nazionali di attuazione[1].

Quello che emerge chiaramente, in particolare dal Considerando 7, è che il Regolamento non si limita ad assicurare solo la protezione dei dati personali e la loro libera circolazione, come avveniva nella impostazione della Direttiva 95/46 CE, che il GDPR stesso ha abrogato dal 25 maggio 2018. Il nuovo Regolamento, infatti, fa almeno due passi in avanti in più.

Il primo concerne appunto la tutela dei dati personali rispetto ai trattamenti che li riguardano, che ora si fonda non più su un ampio, ma generico, dovere di rispettare i diritti e le libertà fondamentali delle persone fisiche ma dà attuazione a quanto previsto dall'art. 8 della Carta dei diritti fondamentali dell'Unione Europea, che ricono-

[1] È bene ricordare sempre che le leggi nazionali che gli Stati membri possono approvare con riferimento alla tutela dei trattamenti di dati personali si basano strettamente e soltanto sulla competenza riconosciuta da norme specifiche del GDPR agli Stati membri. Di conseguenza, le leggi nazionali in materia formano parte integrante della tutela dei dati personali sul territorio di ciascun Paese dell'Unione, avendo un duplice vincolo: a) di avere la loro base giuridica non sulla sovranità dei legislatori nazionali ma sulla competenza ad essi assegnata dal GDPR; b) di dovere, di conseguenza, essere sempre interpretate e applicate in conformità alle norme e ai principi del Regolamento europeo.
In questo senso è esemplare quanto previsto dall'art. 22 del decreto legislativo 10 agosto 2018 n. 101 di adeguamento della normativa nazionale alle disposizioni del Regolamento 2016/679 UE, che al primo comma afferma: «Il presente decreto e le disposizioni dell'ordinamento nazionale si interpretano e si applicano alla luce della disciplina dell'Unione europea in materia di protezione dei dati personali e assicurano la libera circolazione dei dati personali tra Stati membri ai sensi dell'art. 1, paragrafo 3 del Regolamento (UE) 2016/679».

sce la tutela delle persone rispetto ai trattamenti dei dati che sono ad esse riconducibili come un diritto fondamentale dell'Unione.

Non a caso, del resto, si è passati dalla Direttiva 95/46 al Regolamento 2016/679. La ragione essenziale dell'adozione di un Regolamento, come tale immediatamente applicabile in tutta l'Unione, è infatti proprio la conseguenza di due innovazioni fondamentali intervenute successivamente: a) l'adozione, nell'ambito dei Trattati di Lisbona del 2009, della Carta dei diritti fondamentali dell'Unione; b) il fatto che l'art.8 della Carta individua tra i diritti fondamentali anche quello delle persone fisiche alla tutela dai trattamenti relativi ai dati che li riguardano.

Di questa profonda evoluzione giuridica e di prospettiva dà conto, del resto, il Considerando 1, posto non a caso all'inizio del Regolamento.

Il secondo passo in avanti che il GDPR fa rispetto alla Direttiva riguarda invece la libera circolazione dei dati all'interno del territorio dell'Unione.

La Direttiva, nel Considerando 3, fondava la libera circolazione dei dati sulle esigenze legate all'instaurazione e al funzionamento del mercato interno. Si ricordi, del resto, che l'adozione della Direttiva 95/46 avvenne sostanzialmente nell'ambito di attuazione del Trattato di Maastricht e per facilitare la piena attuazione del mercato interno. Per questo anche i riferimenti contenuti nei Considerando 4) 5) e 6) della Direttiva riguardavano lo sviluppo e integrazione dell'economia europea nell'ambito del mercato interno.

Il Regolamento invece non si limita a sottolineare l'esigenza della integrazione economica e sociale dell'Unione come fondamento della libertà di circolazione dei dati. Sottolinea anche che l'esigenza di una robusta tutela dei trattamenti è condizione essenziale anche per rafforzare la fiducia delle persone fisiche nello sviluppo dell'economia digitale all'interno dell'Unione.

Questi due "cambi di passo" sono molto importanti.

Il primo è legato alla adozione della Carta dei diritti fondamentali dell'Unione ed al conseguente riconoscimento del diritto alla protezione dei dati personali come diritto fondamentale.

Il secondo sottolinea che gli ulteriori obiettivi del Regolamento non sono più solo il funzionamento del mercato interno e lo sviluppo economico dell'Unione ma anche, e forse soprattutto, l'incremento della fiducia delle persone fisiche nell'economia digitale.

Entrambi questi mutamenti di prospettiva concorrono in maniera determinante a ridefinire il quadro di fondo nel quale occorre collocare il passaggio dalla Direttiva 95/46 al Regolamento 1026/679 e segnano il fortissimo salto di qualità e di prospettiva che vi è tra i due sistemi normativi.

Il GDPR si pone come una "nuova regolazione" che, muovendo dalla Direttiva 95/46, vuole garantire un quadro normativo adeguato allo sviluppo dell'economia digitale. Lo scopo ultimo è far fronte agli enormi cambiamenti avvenuti, proprio nell'ambito dei trattamenti dei dati, nel passaggio dall'organizzazione economica e produttiva della metà degli anni novanta, fondata ancora essenzialmente sul libero scambio di beni, merci e servizi, e il contesto economico e produttivo attuale, basato in misura sempre crescente sull'economia digitale. Un "cambio di fase" che alla metà degli anni novanta non era neanche pensabile in queste dimensioni, e che richiede una utilizzazione sempre più ampia della circolazione e degli scambi di dati, compresi quelli personali.

1.2. Proprio questa diversità di contesto e di prospettiva spiega anche un'altra caratteristica che differenzia in modo del tutto evidente il quadro della tutela dei trattamenti dei dati personali come regolato dalla Direttiva 95/46 e le leggi nazionali di armonizzazione, e quello che segna invece il nuovo Regolamento e, quindi, anche le leggi nazionali di adeguamento nelle materie in cui il GDPR prevede la competenza degli Stati.

Mentre la Direttiva 95/46 comprendeva solo 33 articoli e sostanzialmente poneva al centro della sua regolazione da un lato i dati, e dall'altro gli interessati, il GDPR si compone di ben 99 articoli e pone al centro di tutto il sistema regolatorio il titolare e le sue responsabilità.

Responsabilità che, e anche questo è un punto molto importante, per il titolare cominciano già dalla fase della progettazione dei trattamenti. Infatti già prima che i trattamenti abbiano inizio il titolare è tenuto a valutare i rischi che i trattamenti che vuole porre in essere possono far correre agli interessati, e a calibrare su tale valutazione le misure organizzative e tecniche da adottare. Del resto, se al centro del GDPR non vi fosse il titolare e il trattamento fin dalla fase della sua progettazione non avrebbe senso neppure prevedere, come fa l'art. 25, che il titolare debba applicare fin dalla progettazione misure adeguate a garantire la *privacy by design* e *by default*.

Inoltre, anche se il GDPR utilizza la parola *accountability* solo nel paragrafo 2 dell'art. 5, è noto a tutti che l'aspetto più innovativo del GDPR consiste proprio nel mettere al centro di tutto il sistema questo principio, legato non solo alla responsabilità del titolare per i trattamenti che pone in essere ma anche al fatto che egli deve essere in grado di dimostrare in qualunque momento la conformità dei suoi comportamenti a quanto previsto dal GDPR.

Principio, questo, ripreso in molte altre disposizioni ma enfatizzato soprattutto nell'art. 24 che, definendo appunto gli obblighi del titolare fin dalla progettazione dei trattamenti, sottolinea che egli deve anche essere in grado di dimostrare in qualunque momento di aver rispettato e di rispettare pienamente la normativa relativa alla tutela dei trattamenti di dati personali che pone in essere.

Ovviamente le differenze tra Direttiva 95/46 e GDPR vanno molto oltre gli aspetti qui richiamati. Tuttavia proprio la centralità della responsabilità del titolare fin dalla fase della progettazione dei trattamenti e il principio di *accountability*, inteso come obbligo di essere in grado in qualunque momento di rispettare quanto previsto dalla normativa di protezione dei trattamenti, costituiscono gli aspetti più innovativi e importanti del GDPR e quelli che di più segnano la differenza di prospettiva tra i due sistemi normativi che si sono succeduti tra il 1995 e il 2018.

1.3. Il ruolo che nell'ambito del GDPR assume il principio di *accountability* è pienamente comprensibile se lo si collega strettamente al fatto che obiettivo fondamentale del Regolamento non è solo garantire la protezione dei trattamenti e la libera circolazione dei dati ma anche, e in modo particolarmente rilevante, incrementare la fiducia delle persone fisiche nell'economia digitale.

Proprio l'obiettivo di rafforzare la fiducia delle persone fisiche non solo nella tutela dei loro diritti fondamentali a cominciare da quello riconosciuto nell'art. 8 della Carta dei diritti dell'Unione, ma anche nel funzionamento stesso dell'economia digitale spiega la centralità che nel GDPR assumono: il titolare del trattamento, che è tale fin dalla fase della progettazione; la *privacy by design* e *by default*; e, soprattutto del principio di *accountability*, che costituisce l'aspetto più rilevante e riassuntivo degli obblighi posti in capo al titolare.

Si comprende bene dunque perché il GDPR sia un sistema normativo fondato essenzialmente sul principio di effettività e adeguatezza.

Le norme in esso contenute, comprese quelle relative alle basi di legittimità dei trattamenti, ai diritti degli interessati a cominciare dal diritto all'informativa, per finire ai principi di liceità, correttezza e trasparenza, che sono posti dall'art. 5 del GDPR come i principi-cardine dei trattamenti, rispondono alla medesima logica.

Molto più di quanto accadesse nella Direttiva, le norme contenute nel GDPR non sono, dunque, solo disposizioni da rispettare ma una metodologia da adottare per quanto riguarda i trattamenti di dati personali.

In sostanza tutte le norme del GDPR, da quelle maggiormente prescrittive anche dal punto di vista del loro contenuto, a quelle che indicano criteri, limiti e condizioni dei trattamenti che il titolare (e il responsabile) sono tenuti a rispettare nel quadro della concretezza della loro attività, sono sempre ispirate all'obiettivo di incrementare la fiducia delle persone fisiche sulla tutela dei loro dati stimolando la loro fiducia in coloro che li trattano. E quindi, per loro natura, perseguono un obiettivo "sostanzialista" che non si risolve unicamente nel loro rispetto formale.

Certamente sono disposizioni giuridiche che vanno lette, interpretate e applicate. Esse però molto spesso sono anche, in modo assolutamente evidente, norme che indicano i criteri da adottare, le metodologie da seguire, le modalità con le quali valutare le misure da adottare per garantire non solo la tutela dei trattamenti ma anche la conquista della fiducia delle persone fisiche, viste sia come cittadini e in quanto tali titolari di diritti fondamentali sia come consumatori o utilizzatori di servizi e, in quanto tali bisognosi di poter avere fiducia in chi assicura loro questi servizi e nelle tecnologie e metodologie che esso utilizza.

Nel suo complesso, dunque, il GDPR è caratterizzato da una sua intrinseca flessibilità, che deriva dal fatto che spetta sempre al titolare individuare e definire sotto la sua esclusiva responsabilità quali siano, rispetto al trattamento che pone in essere, le concrete misure organizzative e tecniche da adottare in conformità alle regole del GDPR.

1.4. Un altro profilo che è molto importante sottolineare è che il titolare (e per la sua parte il responsabile *ex* art. 26) deve anche essere in grado di garantire costantemente che i trattamenti posti in essere assicurino la piena tutela dei diritti degli interessati.

Si tratta di un profilo molto rilevante che non deve mai essere trascurato.

Non vi è dubbio, infatti, che il GDPR ponga al centro di tutto il sistema regolatorio di tutela dei trattamenti di dati personali il titolare, il quale è tenuto, fin dalla loro fase di progettazione (e dunque quando ancora non vi sono "interessati" perché il trattamento non ha ancora avuto inizio) il rispetto delle regole legate alla valutazione dei rischi e alla definizione delle modalità organizzative e tecnologiche da adottare per garantire che essi siano ridotti al minimo possibile. Si collocano qui infatti tutti gli istituti legati alla *privacy by design*, *by default*, la definizione delle misure di sicurezza adeguate e, soprattutto, la eventuale necessità di ricorrere anche alla DPIA, nei casi in cui essa è richiesta in base ai criteri indicati all'art. 35 del GDPR, nonché in base agli elenchi definiti dalle Autorità di controllo in base all'art. 35 paragrafo 4 e da queste comunicati all'EDPB a norma dell'art. 68.

Tuttavia sarebbe profondamente sbagliato non tener conto che anche nel nuovo sistema regolatorio fondato sul GDPR e sulle leggi nazionali di adeguamento, la tutela dei diritti dell'interessato e la loro concreta azionabilità rimangono assolutamente fondamentali.

In primo luogo, infatti, non bisogna mai dimenticare il fatto che il GDPR e le leggi nazionali di adeguamento sono prima di tutto un sistema normativo che ha come obiettivo la tutela del diritto fondamentale previsto dall'art. 8 della Carta di Nizza e degli altri diritti e libertà della persona umana. Come ricorda il Considerando 4, «il trattamento dei dati personali deve essere al servizio dell'uomo e il regolamento rispetta tutti i diritti fondamentali e osserva le libertà e i principi riconosciuti dalla Carta». Dunque, anche se uno degli scopi più innovativi del GDPR è quello di «creare un clima di fiducia che consenta lo sviluppo dell'economia digitale in tutto il mercato interno», è indiscutibile che la tutela in concreto dei diritti delle persone fisiche i cui dati personali sono oggetto dei trattamenti rimane un aspetto fondamentale di tutto il sistema regolatorio. Così come resta essenziale che la tutela dei trattamenti posti in essere dal titolare tenga anche conto, fin dalla progettazione, di tutti i diritti e le libertà delle persone fisiche, come recita l'art. 24 del GDPR.

In secondo luogo, è ovvio che incrementare la fiducia delle persone fisiche nello sviluppo della società digitale richiede anche una

robusta e efficace tutela "in concreto" dei diritti eventualmente lesi dai trattamenti posti in essere.

Di qui la necessità di collocare nella giusta prospettiva sia il ruolo del titolare che quello dell'interessato.

I due "protagonisti" del GDPR si distinguono per il fatto che il titolare deve assolvere a obblighi specifici già nella fase di progettazione dei trattamenti, e dunque quando, per definizione, non può ancora esservi l'"interessato". Tuttavia è certamente vero che tra gli obblighi del titolare vi è anche, e fin dalla fase di progettazione, quello di rendere sempre azionabili ed effettivi i diritti che il GDPR e, sulla sua scia, le legislazioni nazionali di adeguamento, assicurano all'interessato.

Si tratta di un aspetto da tenere costantemente presente perché nel quadro regolatorio del GDPR sono riconosciuti agli interessati nuovi diritti, strettamente legati anche all'evoluzione della società e dell'economia digitale quali: il diritto alla cancellazione, come formulato dall'art. 17, in particolare nei paragrafi 1 e 2; il diritto alla limitazione dei trattamenti come definito dall'art. 18, in particolare in connessione al diritto di opposizione di cui all'art. 21 (cfr. art. 18, paragrafo 1, lettera d); l'obbligo di notificazione definito dall'art. 19, che pone a carico del titolare l'obbligo di comunicare «a ciascuno degli interessati cui sono stati trasmessi i dati personali le eventuali rettifiche o cancellazioni o limitazioni del trattamento effettuate a norma degli artt. 16, 17, paragrafo1 e dell'art.18, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato»; il diritto alla portabilità dei dati di cui all'art. 20; il diritto di opposizione di chi all'art. 21, con particolare riguardo al paragrafo 5 che consente all'interessato di esercitare, nell'ambito dei servizi della società dell'informazione, il suo diritto «con mezzi automatizzati che utilizzano specifiche tecniche»; i diritti che l'interessato può attivare rispetto ai processi decisionali automatizzati relativi alle persone fisiche, compresa la profilazione, di cui all'art. 22.

Si tratta in gran parte di diritti già presenti anche nella Direttiva 95/46 ma che ora vengono "rivisitati" e "ridefiniti" in modo sostanziale avendo a mente i problemi della società digitale e del suo sviluppo. Sono inoltre diritti del tutto nuovi, almeno nel quadro della tutela generale dei trattamenti di dati personali, quali quello relativo alla portabilità dei dati e quelli contenuti nella disciplina relativa ai trattamenti automatizzati con effetti decisionali.

È evidente che vi è una strettissima interrelazione fra gli obblighi del titolare in sede di progettazione dei trattamenti *ex* art. 24 e la previsione di modalità tecniche e organizzative che consentano, in concreto, la attivazione da parte degli interessati di "tutti" i diritti che il GDPR prevede.

Si tratta di una "dimensione" della responsabilità del titolare *ex* art. 24 GDPR non sempre adeguatamente sottolineata dai commentatori ma che assume invece un rilievo molto forte proprio nel contesto dell'evoluzione continua della società digitale e delle tecnologie che ne caratterizzano lo sviluppo, anche sul piano economico.

1.5. Va da sé che la stretta connessione tra doveri e responsabilità del titolare e diritti, nuovi e vecchi, degli interessati collocata nel contesto del GDPR accentua la duplice necessità, insita in questo sistema regolatorio, di flessibilità nelle misure adottate, che devono sempre essere "tarate" sul tipo di trattamenti, progettati prima, posti in essere dopo, e di costante rivisitazione, da parte del titolare, ma anche da parte delle Autorità di controllo, delle misure adottate.

In sostanza, quello che conta sottolineare è che la *accountability* del titolare e la sua responsabilità relativa a poter dimostrare in ogni momento la conformità dei trattamenti posti in essere alle norme del GDPR non si esaurisce affatto nella valutazione dei rischi che i trattamenti possono comportare per i diritti e le libertà delle persone fisiche, ma si estende, necessariamente, anche a poter dimostrare in ogni momento di aver adottato tutte le misure organizzative e tecniche idonee a consentire agli interessati il pieno e totale esercizio dei diritti ad essi riconosciuti dalla normativa europea e dalle normative nazionali di adeguamento nelle materie di competenza dei legislatori nazionali.

In questa luce assume una rilevanza ancora più forte e incisiva l'obbligo, costantemente ripetuto in tutte le norme che definiscono i doveri e le responsabilità dei titolari, di procedere al riesame e all'aggiornamento delle misure adottate.

Insomma, proprio perché il GDPR ha una impronta fortemente "sostanzialistica" e basata su una visione della regolazione non solo come un insieme di norme ma anche come una metodologia da seguire per garantire la tutela del diritto fondamentale alla protezione dei dati personali e incrementare la fiducia dei cittadini nella società digitale, è evidente che i doveri dei titolari si estendono neces-

sariamente a garantire anche misure adeguate a consentire l'esercizio dei diritti degli interessati.

Questo aspetto, di per sé è del tutto ovvio anche se finora poco sottolineato, ha però una precisa conseguenza riguardo alla flessibilità delle misure da adottare e all'adattamento dell'applicazione delle norme all'evoluzione della tecnologia.

La necessità di un continuo aggiornamento e riesame delle misure adottate è fondamentale non solo per potere dimostrare un generico rispetto delle regole del GDPR ma anche per poter garantire agli interessati l'esercizio dei loro diritti e poter dimostrare, in qualunque momento, alle Autorità, sia di controllo che giurisdizionali, che il titolare non solo rispetta i diritti degli interessati ma ne agevola l'azionabilità.

Insomma il titolare non è solo vincolato al rispetto dei diritti degli interessati ma deve fare quanto è in suo potere per assicurarne la tutela anche sotto il profilo della loro azionabilità e del loro effettivo esercizio.

1.6. Se ci si colloca in questa prospettiva si riesce più facilmente a comprendere anche quanto importante ampio sia il ruolo delle Autorità di controllo e vigilanza.

Esse, nel sistema del GDPR e, soprattutto, nel contesto della società digitale, non possono limitarsi a vigilare sul rispetto delle norme. Devono necessariamente e costantemente svolgere anche un ruolo proattivo, garantendo che i titolari concorrano concretamente non solo a rispettare i diritti degli interessati ma anche a tutelare in concreto il loro esercizio e la loro azionabilità

In questo senso le Autorità e il ruolo ad esse affidato sono essenziali proprio come anello di congiunzione tra il rispetto formale delle norme, la tutela in concreto dei diritti, l'incremento della fiducia dei cittadini in una economia digitale in continuo sviluppo.

È evidente, infatti, che non solo le misure che il titolare deve adottare per minimizzare i rischi ma anche quelle che deve porre in essere per assicurare in concreto la portabilità dei dati, la possibilità di notificazione a terzi dell'esercizio del diritto di rettifica e cancellazione, la possibilità di esercitare, anche nel quadro delle nuove tecnologie, il diritto alla limitazione dei trattamenti e di opposizione e, infine, la definizione delle modalità adottate per garantire l'effettiva tutela assicurata dall'art. 22 agli interessati rispetto ai trattamenti

automatizzati con efficacia decisionale, diventano parte integrante anche del ruolo di vigilanza e controllo delle Autorità.

Detto in altri termini, spetta alle Autorità vigilare non solo sul rispetto dei doveri del titolare come definiti nel Capo IV del GDPR, ma anche sulle garanzie effettive che i trattamenti posti in essere assicurano agli interessati rispetto ai diritti ad essi riconosciuti dal Capo III. Spetta dunque alle Autorità controllare anche che le misure organizzative e tecnologiche adottate dal titolare assicurino e facilitino l'adempimento delle richieste degli interessati basate sull'esercizio dei loro diritti. Questo vale, ovviamente per tutti i diritti dell'interessato ma assume un rilievo particolare rispetto a quelli "nuovi", previsti dal GDPR proprio avendo a mente la necessità di estendere la protezione dei trattamenti e la tutela degli interessati anche rispetto ai nuovi sviluppi dell'economia digitale.

1.7. In questo quadro si possono comprendere anche gli amplissimi poteri di *soft law* riconosciuti alle Autorità di controllo nazionali, al Gruppo europeo dei Garanti (EDPB) e alla stessa Commissione.

Si tratta di poteri che possono assumere le vesti giuridiche più diverse, andando dalla possibilità di stabilire gli elenchi nazionali relativi all'obbligo di DPIA di cui all'art. 35 paragrafo 4, salvo comunicazione all'EDPB *ex* art. 68, fino alla adozione di Linee guida e di provvedimenti a carattere generale. Un potere, quest'ultimo, riconosciuto esplicitamente all'EDPB, che può adottare Linee guida di efficacia europea, ma che implicitamente può essere esercitato anche dalle Autorità di controllo, salvo l'obbligo di rispettare le norme relative al meccanismo di cooperazione e coerenza di cui al Capo VII del GDPR.

Vale la pena, inoltre, sottolineare che tutte le leggi nazionali di adeguamento hanno moltiplicato i poteri di *soft law* delle loro Autorità di controllo.

Emblematico in questo senso quanto previsto dal d.lvo n. 101 del 2018 che, anche rimodulando istituti di *soft law* già presenti nel d.lvo n.196 del 2003, ha rafforzato moltissimo i poteri del Garante italiano nelle materie di competenza nazionale. Lo dimostra, tra l'altro, la previsione di: regole deontologiche, di cui all'art. 2 *septies*; misure di garanzia, di cui all'art. 2 *septies*; provvedimenti di carattere generale relativi a trattamenti che comportano rischi elevati per l'esecuzione di compiti di interesse pubblico, di cui all'art. 2 *quinquedecies*.

Quello che interessa mettere in rilievo è che i poteri assegnati alle Autorità di controllo e alla Commissione sono particolarmente importanti in un contesto nel quale la flessibilità e la capacità del GDPR e della normativa nazionale di adeguamento all'evoluzione delle tecnologie è essenziale, sia per garantire che i titolari adottino le misure organizzative e tecniche adeguate rispetto ai rischi che i trattamenti comportano, sia per definire quali misure debbano essere adottate anche al fine di assicurare l'effettività dell'esercizio dei diritti degli interessati.

1.8. In questo contesto si collocano anche i Codici di condotta di cui agli artt. 40 e 41 del GDPR; le certificazioni, di cui agli artt.42 e 43; i sigilli e i marchi di cui agli artt. 42 paragrafo 8 e art. 43, paragrafo 9.

Sono tutti istituti attivabili su richiesta delle categorie o associazioni interessate o anche di singoli titolari.

Le concrete finalità che possono indurre le associazioni di categoria o gli organismi rappresentativi dei titolari e responsabili ad attivare le procedure per proporre l'adozione di Codici di condotta, o spingere anche singoli titolari o responsabili a richiedere certificazioni, sigilli e marchi, possono essere molteplici.

La premessa comune a tutti questi istituti è che la loro attivazione può essere promossa dagli Stati membri, dalle Autorità di controllo, dal Comitato europeo per la protezione dei dati e dalla Commissione ma è necessario che le proposte o le richieste di Codici di condotta siano elaborate da associazioni o organismi che rappresentino i titolari o i responsabili dei trattamenti (cfr. art. 40, paragrafo 1).

Anche per quanto riguarda le certificazioni, i sigilli e i marchi gli Stati membri, Commissione, Autorità di controllo e Comitato europeo per la protezione dei dati possono incoraggiarne la richiesta ma spetta sempre ai titolari o ai responsabili assumere, anche singolarmente, le iniziative necessarie per ottenerli (cfr. art. 42). L'art. 42, paragrafo secondo consente anche a titolari o responsabili del trattamento non soggetti al GDPR ai sensi dell'art. 3, di chiedere che tali istituti possano essere appropriati anche rispetto ai trattamenti da loro posti in essere, al fine di dimostrare che anche essi adottano garanzie e misure appropriate "nel quadro dei trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali" (cfr. art. 42, paragrafo 2).

Le finalità principali che possono guidare titolari e responsabili a sottoporsi ai procedimenti di certificazione relativi ai loro tratta-

menti o chiedere sigilli e marchi che ne garantiscano la conformità alle regole e alla metodologia del GDPR sono ovviamente quelle di poter aumentare e consolidare la fiducia degli interessati, ma più in generale, delle persone fisiche nella loro attività.

Questi strumenti sono dunque strettamente e direttamente funzionali non solo a ottenere una garanzia formale rispetto alla correttezza della loro attività ma anche ad aumentare la fiducia nelle attività da essi poste in opera e rispetto alle quali i trattamenti di dati personali costituiscono uno strumento ma non la finalità ultima che riguarda invece lo scopo di tali trattamenti e dunque la produzione di beni e servizi, specialmente nell'ambito della società digitale.

Una "operazione fiducia" che può assumere gli aspetti più diversi a seconda dei casi, soprattutto quando oggetto delle certificazioni e dei sigilli e marchi siano specificamente le misure di sicurezza adottate o le modalità con le quali gli utenti sono informati dei trattamenti nel corso stesso del loro svolgimento.

1.9. Ancora più complesse possono essere le finalità che possono spingere associazioni o organismi rappresentativi di titolari o responsabili a elaborare proposte di Codici di condotta.

Secondo quanto specifica l'art. 40 paragrafo secondo lo scopo dei Codici di condotta è quello di "precisare l'applicazione del Regolamento".

Questa stessa norma contiene inoltre un lungo elenco, che va dalla lettera a) alla lettera k) e che indica, a titolo esemplificativo, quali possono essere gli oggetti di questi Codici. Oggetti e settori tra i quali assumono un particolare rilievo quelli relativi alle informazioni da dare agli interessati, all'esercizio dei loro diritti e le notificazioni di *data breaches* sia rispetto alle Autorità di controllo che agli interessati stessi ai sensi degli artt. 33 e 34 GDPR.

Non meno importanti sono anche gli altri settori specificamente indicati, tra i quali quello relativo alle misure di sicurezza da adottare, alle modalità di raccolta dei dati, ai casi in cui prevedere la pseudonimizzazione e le modalità con le quali, rispetto ai singoli ambiti di attività oggetto dei Codici di condotta, deve essere rispettato quanto previsto dall'artt. 24 e 25 in materia di *privacy by design* e *privacy by default*.

Non è questa la sede per analizzare più da vicino l'ampiezza dei settori nei quali i Codici di condotta, tenendo conto delle caratteristi-

che dell'attività svolta dalle associazioni di titolari o responsabili che li promuovono, possono definire modalità specifiche di applicazione delle norme del GDPR.

È evidente però che lo strumento dei Codici di condotta, a differenza delle Certificazioni, dei Sigilli e Marchi, non ha tanto la finalità di garantire gli interessati dell'affidabilità dei trattamenti e della loro coerenza con le finalità perseguite al fine di aumentare la loro fiducia nei titolari o responsabili, quanto, piuttosto, lo scopo di definire nei diversi ambiti di trattamenti e di finalità oggetto delle elaborazioni dei singoli Codici modalità di attuazione delle norme del GDPR più idonee a garantire gli obiettivi essenziali che sono alla base della regolazione europea: la tutela del diritto fondamentale alla tutela dei trattamenti di dati personali, la libera circolazione dei dati e le modalità più idonee, settore per settore, per rendere efficace e pienamente attivabile l'azionabilità dei diritti degli interessati e la soddisfazione delle loro richieste legittime.

In questo senso è possibile dire, in modo solo un poco "immaginifico" che i Codici di condotta, una volta approvati, costituiranno una sorta di Allegato al GDPR, valido per lo specifico ambito di attività che ne è oggetto e idoneo a garantire modalità specifiche idonee a garantire non solo la sicurezza dei trattamenti ma anche la concreta azionabilità e difesa dei diritti degli interessati.

Come si è già detto, anche le leggi nazionali di adeguamento al GDPR si sono mosse nello stesso senso, spesso anche ampliando, nelle materie di loro competenza, i poteri delle Autorità oltre gli strumenti già previsti dal GDPR.

Per quanto riguarda la legislazione italiana i casi più significativi riguardano la previsione delle regole deontologiche *ex* art. 2 *quater* e delle misure di garanzia per i trattamenti dei dati relativi alla salute, biometrici e genetici di cui all'art. 2 *septies*.

Anche in questi casi si tratta infatti di istituti di *soft law* il cui scopo è non solo aumentare la tutela dei diritti degli interessati ma anche garantire la loro concreta azionabilità anche ampliandone, almeno per quanto riguarda le regole deontologiche, la portata.

Merita ricordare, infatti, che l'art. 2 *quater*, riprendendo e adeguando al GDPR una norma già presente nel d.lvo n. 196 del 2003, specifica che il rispetto di queste regole è condizione di liceità e correttezza dei trattamenti.

2. GDPR e Intelligenza Artificiale: un problema aperto

2.1. Come già era capitato alla Direttiva 95/46, pensata ed elaborata a partire dal 1990 nell'ambito del completamento del mercato unico come regolato dal Trattato di Maastricht e entrata in vigore nel 1995, mentre già stava "esplodendo" l'uso commerciale della rete e quindi l'economia digitale, anche il GDPR è nato in qualche modo "vecchio".

I lavori preparatori del nuovo Regolamento sono iniziati fin dal 2009, subito dopo l'entrata in vigore del Trattato di Lisbona e quindi anche della Carta dei diritti fondamentali dell'Unione.

Già il 1 dicembre 2009, infatti, il Working Party approvò la Opinion n. 169 intitolata "The Future of Privacy: Joint contribution to the Consultaton of the European Commission on the legal framework for the fundemntal right to protection of personal data I" che può essere considerata come l'avvio di fatto del procedimento di formazione del GDPR.

Successivamente il 25 gennaio 2012, anche al fine di dare attuazione a quanto previsto dall'art. 16 del Trattato sul funzionamento dell'Unione, la Commissione presentò la proposta di Regolamento destinata ad essere approvata, dopo un iter lungo e tormentato soltanto il 27 aprile del 2016 ed entrata in vigore, come tutti sappiamo, solo il 25 maggio 2018. Insieme alla proposta di questo Regolamento nella stessa data del 25 gennaio 2012 la Commissione presentò anche la proposta di Direttiva relativa al trattamento dei dati a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, poi adottata ed entrata in vigore, come Direttiva 2018/680 contemporaneamente al GDPR. Di questo "Pacchetto per la protezione dei dati personali non fece invece parte la proposta di un nuovo Regolamento in materia di e-privacy, che infatti è tuttora in discussione nell'ambito della procedura di concertazione tra Parlamento e Consiglio.

Per questo il GDPR esplicitamente chiarisce che le norme in esso contenute non abrogano né sostituiscono la Direttiva 2002/58 e successive modificazioni.

Le tappe qui richiamate chiariscono bene che i lavori preparatori del nuovo Regolamento sono avvenuti in un tempo che, dati i ritmi dell'innovazione tecnologica, non può che apparirci ormai lontano, quando ancora non era diffusa la tecnologia cloud; non era possibile

avvalersi a basso costo di processori molto potenti; la costituzione di enormi banche date che rendessero possibile tecnologia Big Data era frenata dai costi ancora troppo elevati e da processori non adeguati; la stessa velocità di trasmissione ed elaborazione dei dati era molto inferiore all'attuale.

Soprattutto a quell'epoca lo sviluppo delle molte e diverse tecnologie che oggi sono ricomprese nella generica, e non nuova, definizione di "Intelligenza Artificiale" non aveva ancora assunto la posizione centrale che oggi ha nel dibattito politico, giuridico, scientifico e tecno logico che caratterizza la fase attuale dell'economia digitale.

Infatti, malgrado che l'espressione "Intelligenza Artificiale" si debba a Jhon McCarthty che, sotto questo nome, organizzò un gruppo di lavoro che si incontrò per la prima volta nel New Hampshire, al Dartmouth College, nell'estate del 1956, i temi legati all'Intelligenza Artificiale, che già gli studi di Alan Turing avevano anticipato fin dal 1936 e riproposto nel 1950, è diventato familiare al grande pubblico solo da pochissimo tempo, man mano che la tecnologia della raccolta, elaborazione e utilizzazione dei dati ha sviluppato la possibilità di implementare la programmazione e la costruzione di macchine in grado non solo di eseguire in modo automatizzato programmi predefiniti (i robot e l'automazione delle macchine sono noti da decenni) ma di "pensare" e cioè di reagire, sempre nell'ambito del programma come definito dagli algoritmi utilizzati, alle sollecitazioni e ai condizionamenti ambientali nei quali deve operare.

2.2. Ovviamente non è questa la sede per approfondire i temi legati alle tecnologie che oggi comunemente indichiamo, con un grado infinito di approssimazione, come Intelligenza Artificiale, né è il caso che ci diffondiamo ad esplorare il tema di cosa si debba intendere per Internet delle cose.

Quello che certamente è possibile e doveroso registrare è che il GDPR, pur approvato nel 2016 ed entrato in vigore quest' anno si basa ancora su una impostazione ormai datata.

Tutto il suo impianto normativo, infatti, appare imperniato su una visione ancora "monodimensionale" dei trattamenti dei dati personali, incentrata intorno a un titolare che progetta i trattamenti, ne valuta i rischi e adotta tutte le misure necessarie a tutelare i diritti e le libertà fondamentali delle persone, ivi comprese, ovviamente, tutte le misure necessarie ed adeguate per consentire ad esse

di esercitare i loro diritti qualora, a seguito di trattamenti di dati che le riguardino, esse assumano la veste di "interessato".

Nell'ambito del GDPR sembra non avere spazio la prospettiva della "catena dei trattamenti" che è invece alla base dell'evoluzione dell'economia digitale, sia attraverso la prospettiva dei Big Data, utilizzati da chi li raccoglie non solo per le finalità più diverse ma anche messi a disposizione di altri titolari di altri e specifici trattamenti, strettamente connessi con la predisposizione di algoritmi in grado di sviluppare la tecnologia del *machine learning* o delle macchine "intelligenti. Programmi che, a loro volta, sono poi messi a disposizione di costruttori delle macchine intelligenti per programmarle e consentire loro di sviluppare le proprie attività nell'ambito di programmi che consentano ad esse una più o meno ampia "capacità decisionale". Infine vi è il rapporto tra macchina "intelligente" e utente finale, che si giova delle prestazioni offerte da queste tecnologie, ivi compresa la c.d. "Internet delle cose", ma che a tal fine deve consentire, consapevolmente o meno, alle macchine di utilizzare anche i dati personali che li riguardano per le finalità connesse alle attività per le quali esse sono programmate.

Nel tessuto normativo del GDPR, infatti, la c.d. "catena dei trattamenti" non assume una rilevanza autonoma. Protagonista centrale è il titolare come tale, insieme al responsabile quando una parte dei trattamenti è affidata a soggetti terzi legati al titolare da un contratto o altro atto giuridico vincolante. La stessa figura dei contitolari di cui all'art. 26 del GDPR è di scarsa utilità perché si riferisce a titolari che "determinano congiuntamente le finalità e i mezzi del trattamento" e dunque presuppone in qualche modo che vi sia un unico trattamento la definizione del quale è oggetto del concorrere delle decisioni di due o più diversi soggetti la cui contitolarità è data proprio dalla unitarietà del trattamento e delle sue finalità.

Lo stesso Considerando 79, anche con riferimento alla figura dei contitolari si limita a dire che la protezione dei diritti e delle libertà degli interessati «esigono una chiara ripartizione delle responsabilità ai sensi del presente regolamento, compresi i casi in cui un titolare del trattamento stabilisca le finalità e i mezzi del trattamento congiuntamente con altri titolari del trattamento o quando l'operazione di trattamento viene eseguita per conto del titolare del trattamento».

Come si vede, tanto la norma dell'art. 26 quanto il Considerando 79 non affrontano in alcun modo la tematica della "catena dei trattamenti" connessa invece allo svilupparsi delle tecnologie di IA e comunque a quelle collegate all'uso di trattamenti di dati nell'ambito dei Big Data e della loro successiva utilizzazione per finalità molteplici, ivi compresa quella della comunicazione ad altri soggetti che li utilizzano come titolari autonomi nell'ambito di ulteriori e diversi trattamenti, dotati di proprie, e autonome, finalità specifiche, connesse a loro volta ad attività poste in essere, grazie ai risultati di tali trattamenti, da altri titolari per finalità ulteriori e diverse.

In sostanza, quello che pare di poter dire è che il GDPR, che pure mette al centro di tutto il suo sistema regolatorio il titolare dei trattamenti e la sua responsabilità sembra essere prigioniero di una visione molto restrittiva, e persino "statica", della realtà dell'economia digitale che peraltro intende promuovere e sviluppare tanto da considerare suo obiettivo primario accrescere la fiducia dei cittadini nei confronti delle tecnologie che la caratterizzano e ne garantiscono la crescita.

2.3. Vi è, tuttavia, un aspetto che è opportuno mettere in luce molto più di quanto sinora sia stato fatto.

A guardare per così dire "dall'alto" il tessuto normativo del GDPR si vede con una certa facilità che vi è una evidente disparità tra la ampiezza dei diritti e, in particolare, dei "nuovi diritti" riconosciuti agli interessati e le responsabilità definite a carico dei titolari e dei responsabili.

Tanto il GDPR è in qualche modo "arretrato" sul piano delle responsabilità del titolare e del responsabile, tanto è invece "avanzato" sul piano dei diritti degli "interessati".

Si tenga conto che i due piani sono solo apparentemente coincidenti.

Quando il titolare progetta i suoi trattamenti *ex* art. 24 GDPR non ci sono ancora gli "interessati". La posizione di "interessato", infatti, si assume e si perde a seconda che i dati utilizzati da trattamenti effettivamente in atto riguardino o meno una specifica persona fisica.

In altri termini: in fase di "progettazione" dei trattamenti di cui all'art. 24 GDPR la "platea degli interessati" è potenzialmente indeterminata, mentre in fase di "attuazione" l'ambito degli interessati è

definito, anche se può variare a seconda dei dati in ciascun momento effettivamente trattati.

L'aspetto di maggiore interesse del GDPR è che mentre pare un poco "unidimensionale" nel definire le responsabilità del titolare, soprattutto dal punto di vista della concezione del titolare e del trattamento che questi progetta come parti di una "monade" chiusa su se stessa, nel Capo III, relativo ai diritti degli interessati esso individua una ampia sfera di nuovi diritti che comportano necessariamente rapporti e interconnessioni tra i diversi titolari.

Si pensi, ad esempio, alla portabilità dei dati, al diritto alla cancellazione, a quello relativo all'obbligo del titolare di notificare a terzi a cui abbia comunicato i dati dell'interessato le richieste di questo, fino ai diritti di opposizione, di limitazione e, soprattutto, di conoscenza della logica utilizzata nel caso di trattamenti interamente automatizzati di dati con effetti decisionali.

Sono tutti diritti che comportano di necessità la adozione di standard comuni tra una pluralità di titolari e, in particolare, tra quelli che operano in un medesimo settore. Il riferimento è al diritto alla portabilità dei dati o ai diritti collegati a una attività legittima di trasferimento di dati da un titolare all'altro, come nel caso del diritto alla cancellazione dell'art. 17, del diritto alla rettifica e alla relativa notificazione dell'art. 16, del diritto di opposizione e di limitazione degli artt. 16, 17 e 18, non caso richiamati dall'art. 19.

Dunque non possiamo dire che il regolatore europeo non avesse ben chiara la possibilità (ed anzi la attualità) della "catena dei trattamenti" che caratterizza in maniera crescente la economia digitale.

Quello che possiamo dire, però, è che vi è una forte ed evidente discrepanza fra le regole relative ai doveri e alle responsabilità del titolare (e del responsabile) e quelle che presiedono invece alla definizione dei diritti dell'interessato.

2.4. La discrepanza, o lo "iato", fra la definizione formale della responsabilità e degli obblighi del titolare (e del responsabile) e i diritti degli interessati è certamente colmabile in misura ampia dalla non mai abbastanza sottolineata flessibilità che caratterizza il GDPR e, in parte rilevante, anche la legislazione nazionale di attuazione.

Per questo si insiste tanto sul considerare il GDPR non solo come un insieme di norme ma anche come una metodologia relativa al trattamento dei dati nella società e nell'economia digitale.

Per questo, anche si insiste tanto sui poteri di *soft law* dei Garanti e sui compiti ad essi assegnati come Autorità non solo di vigilanza ma anche di guida e supporto all'evoluzione nel tempo di questa normativa.

Occorre riconoscere, tuttavia, che la discrepanza tra il modo col quale sono definiti e specificati i nuovi diritti degli interessati e quello con cui sono individuati doveri e responsabilità dei titolari è molto forte. Una discrepanza che certamente nel quadro dello sviluppo della Intelligenza Artificiale è destinata a manifestarsi in modo sempre più evidente.

2.5. La catena dei trattamenti, ignorata nel Capo IV relativo ai doveri dei titolari e responsabili, campeggia invece al centro dei "nuovi diritti" degli interessati.

Tutti i nuovi diritti, infatti, presuppongono anche doveri ai quali i titolari devono adempiere rispetto ad altri titolari, siano essi interessati alla portabilità dei dati, alla notifica relativa alle richieste di rettifica, cancellazione, limitazione dei trattamenti o, infine, coinvolti nell'uso dei dati raccolti da un titolare e ceduti ad altro per finalità legate ai trattamenti posti in essere in modo automatizzato e con effetto decisionale.

La domanda che si pone necessariamente è dunque come, e attraverso quali istituti di flessibilità del GDPR, si possa trovare una soluzione a questi problemi e assicurare allo stesso tempo che l'evoluzione delle tecnologie digitali sia accompagnata dalla evoluzione, anche metodologica, delle modalità da adottare per garantire in ogni contesto la effettività e la stessa azionabilità dei diritti degli interessati.

3. I Codici di condotta e l'Intelligenza Artificiale nel quadro del GDPR (e della legislazione nazionale di adeguamento)

3.1. Nel quadro sommariamente ricostruito sembra che i Codici di condotta di cui agli artt. 40 e 41 del GDPR, così come, su un altro piano, le regole deontologiche e le misure di garanzia previste dal d.lvo n. 101 del 2018, che ha novellato il Codice italiano in materia di protezione dei dati personali contenuto nel d.lvo n. 196 del 2003, possano costituire una strada assai utile per rimettere in asse sia

il rapporto tra titolari all'interno della "catena dei trattamenti", sia quello che intercorre tra titolare del trattamento finale della catena e utente, nell'ambito delle diverse tecnologie relative all'Intelligenza Artificiale.

Questo vale soprattutto, ma non solo, rispetto alla realizzazione delle c.d. "macchine intelligenti", le cui prestazioni ultime richiedono quasi sempre anche un rilevante uso di dati personali per offrire agli utenti le loro prestazioni. Dati personali che le macchine devono raccogliere, catalogare, mettere a confronto con quelli contenuti nei loro programmi, e che spesso riguardano non solo gli utenti destinatari diretti delle prestazioni, ma anche terzi che rientrano nel raggio di azione della macchina e i cui dati sono necessari, non meno di quelli propri degli utenti specifici, per assicurare un corretto utilizzo del sistema.

In questa sede, tuttavia, non si approfondisce nel dettaglio anche il tema delle regole deontologiche e delle misure di garanzia previste dagli art. 2 *quater* e 2 *septies* del d.lvo 101 del 2018.

Per non ampliare troppo l'analisi ci si limita a una prima riflessione relativa ai Codici di condotta *ex* art. 40, da un lato, e al loro rapporto con le regole deontologiche e le misure di garanzia previste dal Codice italiano novellato dal d.lvo n. 101 del 2018, dall'altro.

In particolare, merita sottolineare alcune differenze procedimentali e di contenuto che distinguono, su questo terreno, gli strumenti europei da quelli previsti dal Codice novellato nei settori di competenza del legislatore nazionale.

I Codici di condotta di cui all'artt. 40 e 41 del GDPR possono e devono essere distinti in due categorie, in ragione e della procedura necessaria per adottarli e del loro ambito di efficacia territoriale.

Da un lato vi sono i Codici di condotta la cui efficacia riguarda il territorio di un unico Stato e la cui approvazione spetta, ai sensi dell'art. 40, paragrafo 5, alla Autorità di controllo competente in base all'art. 55 del GDPR. Da un altro lato sono previsti Codici di condotta ai quali, seguendo la procedura prevista dall'art. 40, paragrafi 7, 8 e 9, e assunto il parere del Comitato europeo reso ai sensi dell'art. 63, la Commissione può decidere di riconoscere validità su tutto il territorio dell'Unione.

3.2. Le due tipologie di Codici si distinguono tra loro per ambito territoriale di validità e procedura di adozione, modifica, monitoraggio

e eventuale proroga, ma non per oggetto e tipologia di contenuto né per diversa efficacia delle loro disposizioni, salvo l'ambito territoriale, si intende.

Essi si differenziano invece notevolmente dalle regole deontologiche e dalle misure di garanzia della legislazione nazionale italiana, sia per la procedura da seguire che nell'oggetto ed efficacia delle relative disposizioni.

Per quanto riguarda la procedura, in entrambi i casi il sistema di adozione delle misure di *soft law* è diverso rispetto a quello previsto per i Codici di condotta del GDPR.

Infatti, mentre i Codici di condotta di cui all'art. 40 del GDPR sono sempre promossi dalle associazioni di titolari o responsabili interessati o da organismi che li rappresentino, potendo gli Stati membri, la Commissione, le Autorità di controllo e il Comitato europeo svolgere solo un'attività di incoraggiamento e stimolo, le regole deontologiche e le misure di garanzie di cui agli artt. 2 *quater* e 2 *septies* del d.lvo n. 101 del 2018 sono promosse dal Garante.

Le due norme non impongono, né prevedono, che la elaborazione delle stesse sia compiuta da associazioni o categorie di titolari e interessati.

Per le regole deontologiche si tratta di una formula che ripete il dettato dell'abrogato art. 12 del d.lvo n. 196 del 2003 e che ha sempre reso incerto il rapporto tra Autorità garante e categorie e associazioni dei titolari.

Nel quadro del GDPR, e in presenza del dettato, su questo punto, assai più chiaro dell'art. 40, la formulazione dell'art. 2 *quater* può aprire la strada a incertezze se il potere di adottare regole deontologiche sia un potere proprio del Garante, che ovviamente deve tener conto del principio di rappresentatività delle categorie con le quali può interloquire, o invece richieda la sottoscrizione dei rappresentanti delle categorie.

Interrogativo, questo, affatto marginale, tanto più che invece, l'abrogato art. 12 del d.lvo n. 196 del 2003 prevedeva esplicitamente la sottoscrizione dei rappresentanti delle categorie interessate di quelli che allora erano chiamati Codici deontologici e di buona condotta e che ora assumono la qualifica di regole deontologiche.

In compenso l'art. 2 *quater* prevede che il Garante debba sottoporre lo schema delle regole che intende adottare a consultazione pubblica per almeno sessanta giorni.

Una innovazione rilevante rispetto al vecchio art. 12 del Codice italiano, ma anche una differenza significativa rispetto all'art. 40 del GDPR, che non prevede alcuna forma di consultazione pubblica né da parte delle associazioni proponenti né da parte della Autorità di controllo. È pur vero che il Considerando 99 prevede che, nell'elaborare la proposta di Codice, le associazioni o gli organismi rappresentativi sentano le parti interessate pertinenti, compresi gli interessati, e tengano conto delle osservazioni ricevute, ma resta il fatto che nella norma non vi sono prescrizioni specifiche.

Altra differenza evidente riguarda gli effetti dei due strumenti, giacché l'art. 2 *quater* stabilisce esplicitamente che il rispetto delle regole deontologiche è condizione di liceità e correttezza dei trattamenti, mentre l'art. 40 non contiene alcuna specificazione circa un effetto esplicito del mancato rispetto dei Codici, rinviando di fatto all'art. 41 e al meccanismo di monitoraggio in esso previsto. Infatti, in base all'art. 41, paragrafo 1, del GDPR spetta all'organismo di monitoraggio definire anche modalità specifiche per l'accertamento delle eventuali violazioni, gestire i reclami relativi e definire e adottare le opportune misure. La medesima norma stabilisce anche che i poteri conferiti all'organismo di monitoraggio possono persino arrivare a decidere la sospensione dei titolari o dei responsabili dall'applicazione del Codice.

Dunque, mentre le conseguenze dell'eventuale violazione delle regole deontologiche della normativa italiana sono definite e specificate, assai più generiche, e di fatto flessibili nel tempo grazie al ruolo del meccanismo di certificazione di cui all'art. 41 del GDPR, sono le eventuali violazioni dei Codici di condotta di cui all'art. 40.

Profondamente diverso è anche l'ambito di competenza assegnato ai Codici di condotta dall'art. 40 del GDPR e quello riconosciuto alle regole deontologiche dall'art. 2 *quater* del d.lvo n. 101 del 2018.

L'ambito di competenza dei Codici si estende in pratica a tutte le diverse parti del GDPR. Di conseguenza, sia rispetto ai diritti degli interessati che ai doveri e responsabilità dei titolari (e responsabili) consente la definizione di modalità specifiche di attuazione, tenendo conto anche delle specificità dei settori e delle esigenze delle micro, piccole e medie imprese.

L'art. 2 *quater* invece delimita l'ambito delle regole deontologiche alle sole materie di competenza del legislatore nazionale e ai tratta-

menti previsti da disposizioni enumerate e puntualmente elencate del Regolamento europeo.

Infine, merita osservare che mentre l'art. 40 paragrafo 1 specifica chiaramente che la finalità dei Codici di condotta è quella di «contribuire alla corretta applicazione del presente Regolamento», l'art. 2 *quater*, come già a suo tempo l'abrogato art. 12 del d.lvo n. 196 del 2003, nulla dice sulle finalità delle Regole deontologiche.

3.3. La medesima analisi comparativa tra gli strumenti di *soft law* relativi ai Codici di condotta e a quelli previsti dal d.lvo n. 101 del 2018 a favore del Garante italiano dovrebbe essere fatta rispetto alle misure di garanzia di cui all'art. 2 *septies*.

In realtà il contenuto, le finalità e anche gli effetti delle misure di garanzia sono definiti con più precisione di quanto non accada per le regole di condotta e quindi è anche più facile sia definire le differenze tra i due strumenti che evidenziare i problemi che ne derivano.

In modo ancora più evidente di quanto accada per le Regole deontologiche, è evidente che le misure di garanzia sono disposte dal Garante, e solo dal Garante (art. 2 *septies* paragrafo 1). Come previsto per le regole deontologiche, anche le misure di garanzia devono essere sottoposte a consultazione pubblica per un periodo non inferiore ai sessanta giorni (cfr. art. 2 *septies*, comma 3) e devono essere sottoposte a revisione almeno biennale. Inoltre devono tener conto anche delle Linee guida del Comitato europeo e delle migliori prassi in materia (art. 2 *septies*, comma 2).

L'art. 2 *septies*, comma 1, definisce in modo puntuale il contenuto delle misure di garanzia, facendo riferimento ai trattamenti di cui al paragrafo 4 dell'art. 9 del GDPR, mentre il comma 5 dell'art. 2 *septies* specifica che esse devono essere adottate in relazione a ciascuna categoria dei dati personali (rectius dei trattamenti di dati) previsti dall'art. 9, paragrafo 4 del GDPR.

Sempre il comma 5 dell'art. 2 *septies* definisce anche la loro efficacia, configurandole come «ulteriori condizioni sulla base delle quali il trattamento di dati è consentito».

Sono caratteristiche specifiche, puntuali e molto chiare, che differenziano questi strumenti di *soft law* sia dai Codici di condotta dell'art. 40 che dalle regole deontologiche dell'art. 2 *quater* del d.lvo n. 101 del 2018, ora nel Codice novellato.

Esse, però, sono previste esplicitamente in settori molto delicati, quali i trattamenti di dati relativi alla salute, biometrici e genetici, nell'ambito dei quali è del tutto evidente che lo sviluppo di tecnologie riconducibili a ciò che convenzionalmente definiamo Intelligenza Artificiale è in pieno sviluppo.

Ancor più di quanto accade rispetto al rapporto tra regole deontologiche e Codici di condotta, il problema di quale sia oggi, e molto più in futuro, il rapporto che può instaurarsi tra Codici di condotta *ex* art. 40 GDPR e misure di garanzia *ex* art. 2 *septies* del d.lvo n. 101 del 2018 (Codice italiano novellato) è destinato a diventare molto più rilevante di quanto forse oggi si possa pensare.

3.4. In sostanza, l'esistenza di uno strumento di *soft law* così incisivo e penetrante come sono i Codici di condotta *ex* art. 40 e gli strumenti di *soft law* previsti dal legislatore nazionale, in particolare quelli relativi alle regole deontologiche e alle misure di garanzia, è destinato a porre problemi molto rilevanti, tanto più nella logica dello sviluppo della Intelligenza Artificiale e in un quadro che prevede anche la possibilità di Codici di condotta validi su tutto il territorio dell'Unione.

La questione centrale, in sostanza, è se nelle materie che il GDPR rimette *anche* alla competenza del legislatore nazionale, l'eventuale adozione di strumenti nazionali di *soft law*, specificamente riferiti a settori determinati e con procedure ed effetti propri, comporti il venir meno, in quelle materie e in quegli ambiti, della possibilità di adozione di Codici di condotta adottati *ex* art. 40, paragrafo 5 o *ex* art. 40, paragrafi 7, 8 e 9.

La questione, in sostanza, diventa se nei settori regolati dal legislatore nazionale gli strumenti di *soft law* previsti dal GDPR non possano avere efficacia per "sopravvenuta carenza di competenza" del regolatore europeo, sostituito in toto dal legislatore nazionale, o se invece, come finora si ritiene, la legislazione nazionale si affianchi e si adegui a quelle europea ma non possa farne venir meno la competenza.

Questo problema non è stato né affrontato né risolto dal legislatore delegato italiano che, all'art. 20 del d.lvo n. 101 del 2018 si limita ad disciplinare le conseguenze della abrogazione di due Codici deontologici e di buona condotta contenuti nell'Allegato A del vecchio Codice e relativi ai «sistemi informativi gestiti da privati in tema di crediti al consumo, affidabilità e puntualità dei pagamenti» (A.5) e

al «trattamento dati effettuato per svolgere investigazioni difensive o per far valere o difendere un diritto in sede giudiziaria» (A.7). Entrambi questi Codici sono considerati abrogati dall'art. 20 perché chiaramente estranei alla competenza del legislatore nazionale. La medesima norma, tuttavia, prevede che essi restino applicabili ancora per sei mesi dopo l'entrata in vigore del decreto legislativo n. 101 del 2018 affinché le categorie interessate decidano se riproporne i contenuti, anche modificati, ai sensi della procedura di cui all'art. 40 del GDPR, ma dà per scontato che in tutte le altre materie di competenza nazionale i vecchi Codici deontologici e di buona condotta si "trasformino" nelle regole deontologiche del 2 quater, fermo restando la necessità che il Garante verifichi che tutte le norme in esse contenute siano compatibili col GDPR.

L'art. 20, dunque, nulla dice circa la possibilità che in futuro si possa avviare, da parte delle associazioni o organismi rappresentativi di titolari (e responsabili) operanti nei settori oggetto di regole deontologiche, la procedura per elaborare Codici condotta *ex* art. 40 del GDPR. Né affronta la questione se questi Codici, ove se ne ritenesse possibile l'adozione anche nelle materie di competenza del legislatore nazionale, incontrino o meno un limite e un vincolo nelle regole deontologiche.

Lo stesso interrogativo ci si deve porre rispetto alle misure di garanzia dell'art. 2 *septies*.

Già si è detto che esse non hanno nulla a che vedere con le regole per facilitare la applicazione delle norme del GDPR ma pongono invece condizioni ulteriori di legittimità dei trattamenti di cui all'art. 9, paragrafo 4.

Tuttavia anche rispetto a queste misure ci si può, e ci si deve, porre l'interrogativo se la loro previsione nel decreto delegato, e la loro adozione da parte del Garante, presupponga l'esclusione della possibilità di proporre Codici di condotta *ex* art. 40 da parte di titolari o responsabili operanti nei settori dell'art. 9, paragrafo 4.

A questo interrogativo se ne deve poi aggiungere un altro: nel caso in cui si ritenga sussistente la possibilità di applicare anche in questi settori i Codici di cui all'art. 40 del GDPR, le misure italiane di garanzia costituiscono un vincolo rispetto alle norme eventualmente contenute in questi Codici, in quanto devono comunque essere considerate come ulteriori condizioni di legittimità dei trattamenti, validi solo sul territorio italiano?

Si tratta di problemi di evidente rilevanza, soprattutto se si tiene conto che l'art. 40 del GDPR prevede anche Codici di condotta la cui validità è estesa all'intero territorio dell'Unione.

3.5. Questi temi sono destinati ad assumere una rilevanza enorme se, come chi scrive ritiene, i Codici di condotta *ex* artt. 40 e 41 del GDPR sono la strada maestra per conciliare la già sottolineata relativa "unidimensionalità" del GDPR per quanto riguarda l'individuazione dei doveri dei titolari e dei responsabili, con la grande innovazione che esso contiene in materia di diritti degli interessati. Una questione centrale nell'ambito dello lo sviluppo di una economia digitale che va ampliando sempre di più la rilevanza delle "catene dei trattamenti". Una evoluzione segnata dal passaggio di dati personali da un titolare all'altro, ciascuno dei quali pone in essere autonomamente i trattamenti dei dati relativi a una parte della catena, ma senza concorrere necessariamente con i titolari delle fasi successive né alla definizione delle metodologie da adottare nelle diverse fasi di trattamenti né alla individuazione della finalità ultima della "catena" alla quale per la sua parte concorre.

Così chi gestisce una banca dati sempre più ampia per quantità e qualità di dati contenuti, operando con tecniche Big Data può fornire, sempre che vi sia una adeguata base di legittimità che giustifichi il trasferimento, un numero anche molto elevato di dati, "grezzi" o "selezionati" in base a criteri definiti, a un soggetto terzo che li può usare per mettere a punto algoritmi specifici rispetto alle istruzioni e ai dati che si vogliono fornire alle macchine intelligenti. A sua volta chi elabori algoritmi può cederli ad altri titolari che li possono utilizzare per progettare e istruire macchine capaci di analizzare la realtà in cui operano e adottare, ovviamente sempre nell'ambito del programma e delle istruzioni ricevute, decisioni autonome che ne migliorano l'efficienza e permettono di offrire applicazioni e servizi sempre più innovativi.

A sua volta chi costruisce queste macchine le può mettere in circolazione e destinarle agli utenti finali tramite una catena di distributori che inevitabilmente trattano a loro volta dati personali e soprattutto sono nella maggior parte dei casi responsabili, anche contrattualmente, del funzionamento delle macchine che forniscono. Un funzionamento che, ovviamente, va ben oltre il compimento di azioni meccaniche e che, a sua volta, utilizza, raccoglie, tratta e

conserva ulteriori dati personali relativi all'utente e, nella maggior parte dei casi, anche a soggetti terzi.

Infine il rapporto tra macchina e utente può avere gradi di complessità e richiedere trattamenti di dati personali, sia dell'utente che di terzi, in misura rilevante e variabile, anche in ragione dell'uso che gli utenti fanno della macchina o del device di cui si servono.

Nell'ambito di "catene" di questo tipo, qui sommariamente descritte solo a titolo di esemplificazione, è chiaro che a ogni fase di trattamenti corrispondono titolari autonomi e diritti specifici degli interessati, che possono anche mutare di fase in fase. Più difficile può essere accertare, per ciascuna fase, chi e in che misura può essere definito come "interessato"; chi, per ciascuna fase, assume il ruolo di titolare o responsabile con i doveri che ne conseguono; come e nei confronti di chi possono essere esercitati, in ciascuna fase e nel passaggio da una fase all'altra, i diritti alla portabilità dei dati, alla loro rettifica o cancellazione, alla limitazione e alla opposizione ai trattamenti, alla richiesta di conoscere la "logica" dei trattamenti interamente automatizzati; chi, nel passaggio da una fase all'altra, debba dare agli interessati le informazioni necessarie e quale ne debba essere il contenuto, tenendo conto del principio di trasparenza e delle modalità previste dagli artt. 5, 12, 13 e 14 del GDPR.

3.6. È chiaro che ci troviamo, e sempre più ci troveremo, di fronte a problemi di enorme complessità regolatoria. Già oggi la realtà ci impone di fare i conti con questioni sempre più complesse da risolvere per garantire agli interessati l'effettività e l'azionabilità dei loro diritti.

Poter disporre di strumenti come i Codici di condotta *ex* art. 40, dotati anche di un proprio, e non a caso previsto, meccanismo di monitoraggio e di controllo sull'attuazione o la violazione dei Codici stessi, apre la strada a possibilità suggestive. Inoltre l'art. 40 medesimo fa riferimento non solo a specifici settori di attività ma anche ai problemi delle micro, piccole e medie imprese. Problemi, questi, che nel contesto della Intelligenza Artificiale sono destinati a diventare sempre più complessi e a risolvere i quali difficilmente possono essere sufficienti le Linee guida adottate dal Comitato europeo *ex* art. 70 paragrafo 1. Ancor meno possono essere adeguate ad affrontare una realtà così complessa le Linee guida che, *ex* art. 154-*bis* del

Codice novellato, il Garante può adottare nei settori in cui il legislatore nazionale è competente.

È chiaro tuttavia che dalla capacità di dare una risposta adeguata alle sfide legate all'evoluzione tecnologica dipende, e sempre più dipenderà, la capacità degli apparati regolatori europeo e nazionali di incrementare la fiducia dei cittadini nell'economia digitale.

Su questo piano, chi affronta questi temi da un punto di vista prevalentemente giuridico deve risolvere un nodo fondamentale, strettamente legato ai rapporti tra GDPR e legislazioni nazionali di adeguamento: quello di definire con chiarezza quale è il rapporto tra la competenza del regolatore europeo e delle norme del GDPR e la competenza dei legislatori nazionali, soprattutto con riferimento agli strumenti di *soft law* che i due livelli di regolazione prevedono.

Si tratta di un problema immediato, che non può non essere quanto prima affrontato anche a livello di Comitato europeo per la protezione dei dati.

È evidente che occorre una risposta europea condivisa, sia perché i Codici di condotta possono avere anche efficacia su tutto il territorio dell'Unione, sia perché tra i settori in cui il GDPR riconosce competenza ai legislatori nazionali vi sono i trattamenti di dati relativi alla salute, ai dati biometrici e ai dati genetici oltre che i trattamenti relativi alla ricerca scientifica.

Settori tutti nei quali la rapidità dello sviluppo delle tecnologie di Intelligenza Artificiale rischia di essere molto, molto più veloce della capacità regolatoria delle Autorità di controllo e dei decisori europei e nazionali.

El Delegado de Protección de Datos en el Reglamento General de Protección de Datos

Joana Marí

Sommario: 1. Cuestiones generales – 2. ¿Cuándo debe nombrarse un DPD? – 3. Cualidades personales y profesionales de la figura del DPD – 4. Posición del DPD en las organizaciones – 5. Funciones del DPD – Conclusión

1. Cuestiones generales

El Delegado de Protección de Datos (DPD), que viene regulado en los artículos 37 a 39 del Reglamento General de Protección de Datos, de obligado cumplimiento desde el 25 de mayo de 2018, no es una figura nueva en el marco europeo. La propia Directiva 95/46/CE, en su artículo 18, ya se refería al encargado de protección de los datos personales, nombrado por el responsable del tratamiento, al que encomendaría la función de hacer cumplir en el ámbito interno, de manera independiente, las disposiciones nacionales adoptadas en virtud de la Directiva y de llevar un registro de los tratamientos efectuados por el responsable del tratamiento.

A su vez, este encargado de la protección de los datos personales debería realizar controles previos en determinados tratamientos de datos personales que pudieran suponer riesgos específicos para los derechos y libertades de los interesados (art. 20). Pese a esta regulación, no fueron muchos los Estados miembros que la acogieron; es el caso de España, donde es una figura totalmente nueva para las organizaciones tanto públicas como privadas.

El RGPD configura al DPD como una pieza clave para el cumplimiento normativo, en particular si tenemos en cuenta los principales ejes entorno a los cuales gira la regulación. Me refiero al principio de responsabilidad proactiva y demostrable (la *accountability*) y al enfoque en el riesgo, sin olvidar el principio de transparencia que debe regir todas las fases del tratamiento de los datos personales.

Ante este nuevo planteamiento, que varía completamente la perspectiva de cumplimiento y exige a los responsables y encargados del tratamiento un compromiso real con los derechos y libertades de las personas, el DPD se convierte en el garante de estos derechos y libertades dentro de cada organización. Por este motivo las organizaciones, al decidir quién debe asumir esta responsabilidad, deben alejarse de formalismos y confiarla a aquellas personas que cumplen los requisitos regulados en la norma y que tienen por objetivo, en último término, convertir el derecho a la protección de datos personales en parte integrante de la idiosincrasia de las entidades. El DPD solo podrá desplegar sus funciones de forma plenamente efectiva si cuenta con la total confianza de la alta dirección y con la complicidad del conjunto de la organización.

2. ¿Cuándo debe nombrarse un DPD?

En plena coherencia con el enfoque en el riesgo que adopta el RGPD, debemos indicar que no todas las organizaciones están obligadas a designar un DPD. El RGPD regula esta figura como una medida organizativa encaminada a maximizar las garantías para los derechos y libertades en los que pueda existir un riesgo o alto riesgo. Así, el artículo 37.1 establece que el responsable y el encargado del tratamiento deberán nombrarlo siempre que:

> a) el tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial;
>
> b) las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala, o

> c) las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos personales con arreglo al artículo 9 y de datos relativos a condenas e infracciones penales a que se refiere el artículo 10.

En consonancia con el principio de accountability, es recomendable documentar el análisis realizado en el momento de determinar si es o no necesario nombrar un DPD, en especial si la conclusión a la que llegamos es que esta obligación no nos es aplicable.

Respecto de las autoridades y organismos públicos, para determinar cuándo nos encontramos ante esta categoria deberemos acudir al ordenamiento jurídico de cada Estado miembro. En determinados casos no planteará ninguna duda, por ejemplo en el caso de administraciones públicas en sentido estricto. Sin embargo, el Grupo de Trabajo del artículo 29 (ahora Comité Europeo de Protección de Datos) ha señalado en sus directrices sobre los delegados de protección de datos, de 13 de diciembre de 2016 (revisadas y adoptadas el 5 de abril de 2017), que una labor pública pueden llevarla a cabo no solo las autoridades y organismos públicos sino, también, otras entidades[1]. En estos casos, las personas pueden estar en una situación muy similar a la que se produce cuando una autoridad u organismo público trata sus datos (los datos pueden tratarse para fines similares y las personas suelen tener un poder de decisión igualmente escaso o nulo sobre si sus datos se tratan, y cómo), siendo recomendable el nombramiento de un DPD.

En relación con la designación del DPD, en España la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, amplia los supuestos en que deberá, obligatoriamente, nombrarse un DPD, en concreto:

> a) Los colegios profesionales y sus consejos generales.
>
> b) Los centros docentes, así como las universidades públicas y privadas

[1] Por ejemplo, empresas privadas que prestan servicios públicos o ejercen funciones públicas.

c) Las entidades que exploten redes y presten servicios de comunicaciones electrónicas cuando tratan habitual y sistemáticamente datos personales a gran escala.

d) Los prestadores de servicios de la sociedad de la información cuando elaboren a gran escala perfiles de los usuarios del servicio.

e) Los bancos, las cajas de ahorros, las cooperativas de Crédito, el Instituto de Crédito Oficial,

f) los establecimientos financieros de crédito

g) Las entidades aseguradoras y Reaseguradoras

h) las empresas de servicios de inversión, reguladas por la legislación del mercado de valores,

i) los distribuidores y comercializadores de energía eléctrica y los distribuidores y comercializadores de gas natural.

j) Las entidades responsables de ficheros comunes para la evaluación de la solvencia patrimonial y crédito o de los ficheros comunes para la gestión y prevención del fraude,

k) Las entidades que desarrollen actividades de publicidad y prospección comercial, cuando lleven a cabo tratamientos basados en las preferencias de los afectados o realicen actividades que impliquen la elaboración de perfiles de los mismos.

l) Los centros sanitarios legalmente obligados al mantenimiento de las historias clínicas de los pacientes.
Se exceptúan los profesionales de la salud que, a pesar de estar legalmente obligados al mantenimiento de las historias clínicas de los pacientes, ejerzan su actividad a título individual.

> m) Las entidades que tengan como uno de sus objetos la emisión de Informes comerciales que puedan referirse a personas físicas.
>
> n) Los operadores que desarrollen la actividad de juego a través de canales electrónicos, informáticos, telemáticos e interactivos, de acuerdo con la normativa de regulación del juego.
>
> o) Las empresas de seguridad privada.
>
> p) Las federaciones deportivas cuando traten datos de menores de edad.

Finalmente, en cuanto a la designación, indicar que el DPD puede ser interno o externo, pero es importante que la forma de contacto se establezca claramente y que sea de fácil acceso, ya que es el punto de contacto en materia de protección de datos para los interesados y para las autoridades de control. En este último caso, recordemos que el nombramiento del DPD se debe comunicar a las autoridades de control y, por otra parte, que los responsables y encargados deben publicar los datos de contacto del DPD.

3. Cualidades personales y profesionales de la figura del DPD

En segundo lugar, quiero hacer referencia a las características personales y profesionales que deben confluir en la persona nombrada como DPD. En este sentido, el artículo 37.5 del RGPD nos indica que:

> El delegado de protección de datos será designado atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho y la práctica en materia de protección de datos y a su capacidad para desempeñar las funciones indicadas en el artículo 39.

Así, su nombramiento no solo puede responder a sus conocimientos en materia de protección de datos, sino que debe estar

en condiciones de cumplir las funciones que le son asignadas. A esto debe añadirse que el DPD, asimismo, ocupa una posición especial dentro de las organizaciones y que, en consecuencia, esta circunstancia es también importante en el análisis de su capacidad. Por otra parte, el Considerando 97 del RGPD señala que su nivel de conocimientos debe determinarse atendiendo al tipo de tratamientos de datos que se realicen y a la protección exigida para los datos personales tratados (según el grado de sensibilidad, complejidad y cantidad).

En cuanto a sus cualidades profesionales, que no vienen concretadas en el RGPD, el Grupo de Trabajo del artículo 29, en las directrices antes señaladas, indica que deben tenerse en cuenta:

- Los conocimientos sobre la legislación y prácticas nacionales y europeas en materia de protección de datos y una profunda comprensión del RGPD.
- El conocimiento del sector empresarial y de la organización del responsable del tratamiento. Asimismo, el DPD debe tener un buen conocimiento de las operaciones de tratamiento que se llevan a cabo, así como de los sistemas de información y de las necesidades de seguridad y protección de datos del responsable del tratamiento.
- En el caso de una autoridad u organismo público, el DPD debe también poseer un conocimiento sólido de las normas y procedimientos administrativos de la organización.

Pero, como decía no solo son importantes las cualidades profesionales, sino también las personales. A este efecto, son útiles las indicadas en los *Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001*, de 14 de octubre de 2010 (en adelante, Estándares).

En estos Estándares se señalan como importantes las siguientes habilidades personales: integridad, iniciativa, organización, perseverancia, discreción, capacidad para afirmarse en circunstancias difíciles, interés en la protección de datos y motivación para ser DPD; e interpersonales: comunicación, negociación, resolución de conflictos y capacidad para construir relaciones de trabajo.

Por otra parte, y antes de entrar a analizar las funciones a realizar, considero imprescindible hacer referencia, en este punto, a su posición dentro de la organización, directamente vinculada con la exigencia de independencia en el ejercicio de sus funciones.

4. Posición del DPD en las organizaciones

La posición, o estatuto, del DPD viene regulada en el artículo 38 del RGPD, en el que se señala:

> 1. El responsable y el encargado del tratamiento garantizarán que el delegado de protección de datos **participe de forma adecuada y en tiempo oportuno** en todas las cuestiones relativas a la protección de datos personales.
>
> 2. El responsable y el encargado del tratamiento **respaldarán al delegado de protección de datos en el desempeño de las funciones** mencionadas en el artículo 39, **facilitando los recursos** necesarios para el desempeño de dichas funciones y el **acceso a los datos personales y a las operaciones de tratamiento**, y para el **mantenimiento de sus conocimientos especializados**.
>
> 3. El responsable y el encargado del tratamiento garantizarán que el delegado de protección de datos **no reciba ninguna instrucción en lo que respecta al desempeño de dichas funciones**. **No será destituido ni sancionado por el responsable o el encargado por desempeñar sus funciones.** El delegado de protección de datos **rendirá cuentas directamente al más alto nivel jerárquico** del responsable o encargado.
>
> 4. Los interesados podrán ponerse en contacto con el delegado de protección de datos por lo que respecta a todas las cuestiones relativas al tratamiento de sus datos personales y al ejercicio de sus derechos al amparo del presente Reglamento.
>
> 5. El delegado de protección de datos estará obligado a mantener el secreto o la confidencialidad en lo que respecta al desempeño de sus funciones, de conformidad con el Derecho de la Unión o de los Estados miembros.

> 6. El delegado de protección de datos podrá desempeñar otras funciones y cometidos. El responsable o encargado del tratamiento garantizará que dichas funciones y cometidos **no den lugar a conflicto de intereses**.[2]

De esta lista se deduce, con claridad, que el DPD debe poder actuar en base a un conocimiento real y directo de la estrategia de su organización, para poder incorporar todos los aspectos necesarios para la garantía de los derechos y libertades de los interesados y con un alto nivel de independencia. Por tanto, que no tema las posibles consecuencias negativas derivadas del correcto desempeño de sus atribuciones.

De los puntos anteriores, quiero destacar lo indicado por el Grupo de Trabajo del artículo 29 en sus directrices, en relación con lo siguiente:

a. Participación de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales

El DPD debe estar presente desde los primeros momentos en que se tratan cuestiones relativas a la protección de los datos. Este es un punto muy importante, si tenemos en cuenta obligaciones como la protección de datos desde el diseño y por defecto o la realización de evaluaciones de impacto sobre la protección de datos, reguladas en el RGPD.

El DPD debe ser considerado como el interlocutor dentro de la organización para todo aquello que afecta al tratamiento de datos personales y, por ejemplo, debe garantizarse que:

- Es invitado a participar en reuniones con los cuadros directivos altos y medios.
- Está presente cuando deben adoptarse decisiones que afectan a la protección de datos.
- En caso de que se produzca una violación de seguridad debe consultarse, rápidamente, con el DPD.

[2] *https://www.boe.es/diario_boe/txt.php?id=BOE-A-2018-16673*

b. Recursos necesarios

En este punto, el Grupo de Trabajo del artículo 29 llama a tener en cuenta las siguientes cuestiones:

- Apoyo activo a la labor del DPD por parte de la alta dirección.
- El DPD debe disponer de tiempo suficiente para el desempeño de sus funciones, en particular, cuando se es DPD a tiempo parcial.
- Dotarlo de los recursos financieros, infraestructura y personal necesarios.
- Comunicación oficial de la designación del DPD a todo el personal de la organización.
- Facilitarle el acceso necesario a otros servicios, como recursos humanos, departamento jurídico, TI, seguridad, etc., necesarios para el correcto desempeño de su trabajo.
- Formación continua.

c. Independencia

El artículo 38, apartado 3, establece algunas garantías básicas que contribuyen a asegurar que los DPD puedan realizar sus tareas con el suficiente grado de autonomía dentro de su organización. En particular, los responsables o encargados del tratamiento están obligados a garantizar que el DPD «no reciba ninguna instrucción en lo que respecta al desempeño de dichas funciones». El considerando 97 añade que los DPD «sean o no empleados del responsable del tratamiento, deben estar en condiciones de desempeñar sus funciones y cometidos de manera independiente».

Esto significa que, en el desempeño de sus tareas con arreglo al artículo 39, no debe instruirse a los DPD sobre cómo abordar un asunto, por ejemplo qué resultado debería lograrse, cómo investigar una queja o si se debe consultar a la autoridad de control. Asimismo, no se les debe instruir para que adopten una determinada postura con respecto a un asunto relacionado con la ley de protección de datos, por ejemplo una interpretación concreta de la ley.

No obstante, la autonomía de los DPD no significa que tengan poder para adoptar decisiones más allá de sus funciones, definidas con arreglo al artículo 39.

El responsable o el encargado del tratamiento siguen siendo responsables del cumplimiento de la normativa de protección de datos y deben ser capaces de demostrar dicho cumplimiento. Si el respon-

sable o el encargado del tratamiento toma decisiones que son incompatibles con el RGPD y con el consejo del DPD, este debe tener la posibilidad de expresar con claridad sus discrepancias al más alto nivel de dirección y a los encargados de la toma de decisiones. A este respecto, el artículo 38, apartado 3, establece que el DPD «rendirá cuentas directamente al más alto nivel jerárquico del responsable o encargado». Dicha notificación directa garantiza que la alta dirección (por ejemplo, el consejo de administración) está informada del consejo y las recomendaciones del DPD, como parte de la misión del DPD de informar y asesorar al responsable o al encargado del tratamiento. Otro ejemplo de notificación directa es la elaboración de un informe anual de las actividades del DPD, que se presentará al más alto nivel directivo.

d. Destitución o sanción por el desempeño de las funciones del DPD

Sólo indicar que el RGPD no especifica cómo o cuándo puede un DPD ser destituido o sustituido por otra persona. Pero, por descontado, cuanto más estable sea el contrato del DPD y más garantías existan contra el despido improcedente, más probabilidad habrá de que pueda actuar con independencia.

e. Conflicto de intereses

Este punto es esencial desde la perspectiva de la garantía de la independencia, y así lo indica el Grupo de Trabajo del artículo 29 al señalar que, si bien un DPD puede desarrollar funciones no vinculadas a su cargo de DPD, solamente le serán atribuibles aquellas que no supongan un conflicto de intereses.

Generalmente hay cargos que, por sus propias características, ya suponen un conflicto. Sería el caso de los puestos de alta dirección (director general, director de operaciones, director financiero, director médico, jefe del departamento de mercadotecnia, jefe de recursos humanos o director del departamento de TI). Por otra parte, también pueden suponer un conflicto de intereses los cargos inferiores, cuando les corresponda determinar los fines y medios del tratamiento, o las situaciones en las que el DPD represente al responsable o al encargado del tratamiento ante los tribunales, en casos relacionados con la protección de datos.

En los Estándares de la UE se señalan determinadas circunstancias que nos pueden orientar respecto a la probabilidad de que exista un conflicto de intereses, en concreto cuando:

- Ejerce sus funciones a tiempo parcial.
- Tiene un contrato por tiempo limitado o de corta duración.
- Debe informar y es evaluado por un superior directo en la jerarquía (director o jefe de unidad).
- Debe solicitar personal y recursos (recursos de TI, presupuesto para viajes de negocios y capacitación) a su superior directo.

Llegados a este punto, es importante señalar que, justamente, en los Estándares, se señalan los aspectos vinculados al conflicto de intereses como uno de los aspectos a tener presente en el momento de valorar las cuestiones éticas vinculadas al desempeño de las funciones de DPD. En este punto, los Estándares indican que existirá conflicto de intereses cuando las demás funciones u obligaciones encomendadas a un DPD pueden generar intereses directamente adversos a los de la protección de los datos personales dentro de su institución.

Otras condiciones vinculadas a la ética profesional, referenciadas en los Estándares, son:

- Deber de lealtad respecto a la protección de los datos personales.
- *Need to know*, el amplio margen de acceso a la información, locales, etc. que tiene atribuido como DPD debe ser utilizado de forma estricta y acorde con las necesidades derivadas del ejercicio de sus funciones.
- Deber de confidencialidad respecto de la información conocida en el ejercicio de sus funciones.

5. Funciones del DPD

En cuanto a las funciones atribuidas al DPD, vienen reguladas de forma muy breve en el artículo 39.1 del RGPD:

> a) informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del presente Reglamento y de otras disposiciones de protección de datos de la Unión o de los Estados miembros;

> b) supervisar el cumplimiento de lo dispuesto en el presente Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes;
>
> c) ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35;
>
> d) cooperar con la autoridad de control;
>
> e) actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36, y realizar consultas, en su caso, sobre cualquier otro asunto.

Además, se hace una mención específica del DPD en el artículo 35.2 del RGPD, en relación con su intervención en las evaluaciones de impacto en la protección de datos personales, estableciendo que el responsable del tratamiento debe recabar el asesoramiento del DPD al realizar la evaluación de impacto. Por su parte, el Grupo de Trabajo del artículo 29 recomienda su intervención no solo en el momento de realizar la evaluación sino, también, antes (en la determinación de la metodología a utilizar) y después de hacerla (respecto de las medidas que deben aplicarse para mitigar los riesgos y respecto de si la evaluación se ha realizado correctamente). En todo caso, si no se siguen las indicaciones del DPD este hecho debe documentarse.

Respecto a su intervención en caso de violación de seguridad, aparte de la obligación de facilitar a la autoridad de control sus datos de contacto en el momento de realizar la notificación, el Grupo de Trabajo del artículo 29 en sus directrices sobre la notificación de las violaciones de seguridad de los datos personales en el Reglamento 2016/679, aprobadas el 3 de octubre del 2017 (revisadas y aprobadas

el 6 de febrero de 2018), indica que se debería obtener su opinión en cuanto a la estructura, configuración y gestión de la documentación de las violaciones de seguridad y que, incluso, podría ocuparse del mantenimiento de los archivos. Siendo que el DPD tiene un rol principal en el asesoramiento, prevención y seguimiento en caso de violaciones, es imprescindible que se le informe rápidamente cuando se produce una violación de seguridad y que se involucre en su gestión y en el proceso de notificación.

El RGPD nos recuerda que el DPD tiene que actuar siempre atendiendo al riesgo concreto de los tratamientos realizados y priorizar sus acciones en función de ese riesgo.

Pese a la brevedad de la lista, nada obsta para que el responsable o el encargado del tratamiento le asignen otras funciones, siempre que no exista un conflicto de intereses. De hecho, el punto 6 del Esquema de certificación de la Agencia Española de Protección de Datos[3], al referirse al perfil del DPD, indica que éste tiene, como mínimo, las siguientes funciones:

a) Informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del Reglamento y de otras disposiciones de protección de datos de la Unión o de los Estados miembros;
b) Supervisar el cumplimiento de lo dispuesto en el Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales,
c) Supervisar la asignación de responsabilidades,
d) Supervisar la concienciación y formación del personal que participa en las operaciones de tratamiento
e) Supervisar las auditorías correspondientes;
f) Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación.
g) Cooperar con la autoridad de control;

[3] *https://www.aepd.es/reglamento/cumplimiento/delegado-de-proteccion-de-datos.html*

h) Actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa.
i) Realizar consultas a la autoridad de control, en su caso, sobre cualquier otro asunto.

En el mismo apartado del Esquema se concretan las áreas de las tareas de asesoramiento y supervisión:

a) Cumplimiento de principios relativos al tratamiento, como los de limitación de finalidad, minimización o exactitud de los datos.
b) Identificación de las bases jurídicas de los tratamientos.
c) Valoración de compatibilidad de finalidades distintas de las que originaron la recogida inicial de los datos.
d) Determinación de la existencia de normativa sectorial que pueda determinar condiciones de tratamiento específico distintas de las establecidas por la normativa general de protección de datos.
e) Diseño e implantación de medidas de información a los afectados por los tratamientos de datos.
f) Establecimiento de mecanismos de recepción y gestión de las solicitudes de ejercicio de derechos por parte de los interesados.
g) Valoración de las solicitudes de ejercicio de derechos por parte de los interesados.
h) Contratación de encargados de tratamiento, incluido el contenido de los contratos o actos jurídicos que regulen la relación responsable-encargado.
i) Identificación de los instrumentos de transferencia internacional de datos adecuados a las necesidades y características de la organización y de las razones que justifiquen la transferencia.
j) Diseño e implantación de políticas de protección de datos.
k) Auditoría de protección de datos.
l) Establecimiento y gestión de los registros de actividades de tratamiento.
m) Análisis de riesgo de los tratamientos realizados.
n) Implantación de las medidas de protección de datos desde el diseño y protección de datos por defecto adecuadas a los riesgos y naturaleza de los tratamientos.
o) Implantación de las medidas de seguridad adecuadas a los riesgos y naturaleza de los tratamientos.

p) Establecimiento de procedimientos de gestión de violaciones de seguridad de los datos, incluida la evaluación del riesgo para los derechos y libertades de los afectados y los procedimientos de notificación a las autoridades de supervisión y a los afectados.
q) Determinación de la necesidad de realización de evaluaciones de impacto sobre la protección de datos.
r) Realización de evaluaciones de impacto sobre la protección de datos.
s) Relaciones con las autoridades de supervisión.
t) Implantación de programas de formación y sensibilización del personal en materia de protección de datos.

Es decir, el DPD debe asesorar y estar involucrado en cualquier cuestión que afecte al tratamiento de datos personales. En este punto, es importante señalar que las modernas tecnologías de tratamiento y análisis de la información distorsionan, en determinados ámbitos, lo que se puede o no considerar dato personal. En este contexto, es importante que el DPD participe desde, también el primer momento en el análisis y supervisión de las decisiones que determinen que no se están tratando datos personales en el sentido de la definición del artículo 4 del RGPD.

En relación con la atribución de funciones, y teniendo en cuenta la brevedad de la regulación, sería recomendable que el responsable y el encargado del tratamiento las concretasen por escrito, en aras de la independencia y de evitar la existencia de conflicto de intereses.

Conclusión

De todo lo expuesto, podemos concluir que la figura del DPD se convierte en una pieza central para la garantía del conjunto de derechos y libertades de las personas, en aquellas situaciones en las que el tratamiento de sus datos pueda generar un riesgo o un alto riesgo para ellos. Es necesario que las organizaciones se comprometan con sus usuarios y sus derechos, pasando a considerar el cumplimiento de la normativa de protección de datos como un elemento indispensable para la innovación y el crecimiento sostenible de la economía, la política y la sociedad en su conjunto.

El RGPD: entre la tutela del interesado y la saturación informativa

Mònica Vilasau Solana

Sommario: Introducción – 1. Análisis de la posible aplicación del TRLCU al tratamiento de datos personales – 2. Análisis de los artículos del TRLCU que podrían resultar aplicables – 3. Los deberes de información en el RGPD – 4. ¿Comporta la aplicación del TRLCU una mayor protección que la ofrecida exclusivamente por el RLOPD? – Bibliografía

Introducción

Los supuestos en que se tratan datos de carácter personal pueden conceptuarse como una relación jurídica, integrada por dos partes, el responsable del tratamiento (RT) y el afectado por el mismo. En tanto que relación jurídica, en este trabajo se analizará si cabe aplicar la normativa de defensa de consumidores y usuarios a la misma. En caso de considerar que resulta aplicable, deberá determinarse qué preceptos concretos. A continuación se examinará si la aplicación conjunta de la normativa de defensa de consumidores y usuarios y la relativa a la protección de datas otorga mayor protección al afectado por un tratamiento de datos o no es así.

Se considera oportuno explorar esta vía porque el derecho de los consumidores constituye uno de los principales fenómenos que ha irrumpido y transformado el derecho privado a partir del último cuarto del siglo XX y por lo tanto resulta conveniente examinar en qué medida interactúa con la normativa sobre el tratamiento de datos personales.

1. Análisis de la posible aplicación del TRLCU al tratamiento de datos personales

1.1. Dos premisas:

Para determinar si la normativa de defensa de consumidores y usuarios puede resultar aplicable al tratamiento de datos de carácter personal y en qué medida, se examinará someramente el ámbito subjetivo y objetivo de aplicación del RDL 1/2007 (TRLCU)[1].

Sin embargo, antes de llevar a cabo este estudio es preciso hacer referencia a dos premisas.

1ª Premisa: este análisis solo contempla la fase de preparación de dicha relación jurídica. No tiene en cuenta la fase de ejecución ni de cumplimiento.

La importancia de esta fase preparatoria se debe al hecho que las normas de defensa de consumidores y usuarios han producido dos cambios sustanciales. Por un lado han dado relevancia negocial a las manifestaciones de empresarios y profesionales en el mercado a través de la publicidad y por el otro han impuesto a empresarios y profesionales deberes especiales de información a favor de los consumidores antes de la celebración de los contratos[2].

De estos cambios se analizará con más detalle el segundo de ellos en la medida que el derecho a la información, además de todas las posibles exigencias e implicaciones del TRLCU, se concibe como un

[1] Se trata del Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias. Boletín Oficial del Estado (BOE) n. 287, de 30 de noviembre de 2007. La última actualización publicada es del 12-7-2018.

[2] En este sentido puede consultarse L.M. Miranda Serrano, *La protección del consumidor como ariete de la reforma del viejo Derecho privado; en especial, en la fase previa a la contratación de bienes y servicios*, en L.M. Miranda Serrano-J. Pagador López-M. Pino Abad (coord), *La protección de los consumidores en tiempos de cambio*, Madrid, Iustel, 1ª ed., 2015, 37-64. Véase concretamente, 38 y 39. Marín López también pone el acento en esta fase precontractual, en que el consumidor se dispone a contratar movido por la publicidad. M.J. Marín López, *La formación del contrato con consumidores*, en M.A. Parra Lucán (dir.), *Negociación y perfección de los contratos*, Cizur Menor, Thomson-Aranzadi, 2014, 1ª ed., 789- 848, 790.

Principio de protección de datos [art. 5.1.a) RGPD[3]]. Así mismo, la definición de consentimiento que proporciona el art. 4.11 RGPD, exige que se trate de una manifestación de voluntad *informada*.

La segunda premisa es que entre los supuestos en que se obtienen datos personales, aquél que merece un especial interés es el supuesto en que se tratan datos *extracontractuales*. Esto es, datos que *no* son necesarios para el negocio principal que se hubiera perfeccionado de forma anterior o simultánea. Es precisamente en función de esta *necesidad* del dato, que LLÁCER distingue entre datos contractuales y datos extracontractuales. Los primeros son aquellos indispensables para el contrato mientras que los segundos no guardan relación directa con aquél ni son precisos para ejecutarlo[4].

Al adquirir un billete de avión, es obvio que existen unos datos como son el nombre y apellidos, documento nacional de identidad (DNI), dirección postal, de correo electrónico o el número de tarjeta de crédito que son necesarios para el perfeccionamiento y ejecución del contrato. Sin embargo estos datos, contractuales, no son los que centrarán el análisis de este trabajo. Los que focalizarán este estudio son aquellos que son totalmente colaterales al negocio principal realizado o bien que se obtienen aprovechando que se lleva a cabo un contrato pero al margen del mismo. Sería el caso, entre otros, de datos relativos al historial de navegación, aquellos que se proporcionan para obtener un producto gratuito, para participar en un sorteo u obtener un descuento.

[3] Se trata del Reglamento (UE) 2016/679 del Parlamento europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). Diario Oficial de la Unión Europea (L 119/1), de 4.5.2016.

[4] La terminología de datos extracontractuales es utilizada por Llácer, de quien la tomo. Señala esta autora que «Los datos contractuales sirven el interés concurrente del afectado-consumidor y del responsable-proveedor: ambos tienen interés en la celebración y el cumplimiento del contrato. En cambio, los datos extracontractuales son ajenos al mismo y, como se ha indicado, sirven el interés legítimo del responsable del tratamiento "siempre que no se vulneren los derechos y libertades fundamentales del interesado" (art. 6.2 in fine LOPD)». En cuanto a los datos *extracontractuales*, «su tratamiento requiere el consentimiento inequívoco del afectado, es decir, *un negocio previo de autorización*». (Mª.R. Llácer Matacás, *La autorización al tratamiento de información personal en la contratación de bienes y servicios*, Madrid, Dykinson, 2012, 73 y 76).

Dentro de estos datos extracontractuales, se analizarán principalmente dos escenarios para estudiar la hipótesis de trabajo: las redes sociales y las campañas de márqueting en que se obtienen datos de los afectados.

A continuación, como ya se ha avanzado, se examinará si el TRLCU resulta aplicable a estos supuestos, teniendo en cuenta el ámbito subjetivo y objetivo de dicho texto legal.

1.2. La determinación del ámbito subjetivo de aplicación del TRLCU

En cuanto al ámbito subjetivo, el art. 2 TRLCU determina que dicha norma será de aplicación a las *relaciones* entre consumidores o usuarios y empresarios.

Así mismo, en cuanto al concepto general de consumidor y de usuario se establece (art. 3 TRLCU) que: «A efectos de esta norma y sin perjuicio de lo dispuesto expresamente en sus libros tercero y cuarto, *son consumidores o usuarios las personas físicas que actúen con un propósito ajeno a su actividad comercial, empresarial, oficio o profesión*[5].

Son también consumidores a efectos de esta norma las personas jurídicas y las entidades sin personalidad jurídica que actúen *sin ánimo de lucro* en un ámbito *ajeno a una actividad comercial o empresarial*»[6].

En principio, pues, todo afectado o interesado sujeto individual (persona física), cuyos datos sean tratados y que entable una relación con un responsable de tratamiento y que actúe con un propósito ajeno a su actividad comercial, empresarial, oficio o profesión, entraría dentro del concepto de consumidor *ex* art. 3.1 del TRLCU.

En base a los posibles escenarios descritos, el usuario de facebook podría ser calificado como consumidor *ex* art. 3 TRLCU, siempre que actuara con un propósito ajeno a su actividad comercial, empresarial, oficio o profesión. Por el contrario, si se tratara de un usuario que utilizara la red social para sus negocios, para hacer publicidad de una tienda o de un servicio, no sería consumidor *ex* art. 3 TRLCU.

[5] La cursiva es mía.

[6] La cursiva es mía.

En resumen, respecto de las *personas físicas*, resultará aplicable el TRLCU siempre que actúen con un *propósito ajeno* a su actividad comercial, empresarial, oficio o profesión. Así mismo en este supuesto resultará aplicable el RGPD (en tanto que dicho RGPD tutela las personas físicas (art. 1.1 RGPD), y siempre que se trate de tratamientos realizados en el ejercicio de actividades exclusivamente personales o domésticas [art. 2.2.c) RGPD]. Esto es, siempre que el responsable del tratamiento lleve a cabo este tipo de actividades.

En cuanto a las personas jurídicas, estas pueden en determinados casos ser calificadas como consumidores. Por ejemplo, si una fundación utilizara una red social o página web en un *ámbito ajeno a una actividad comercial o empresarial y sin ánimo de lucro* (art. 3.2 TRLCU), para adquirir productos completamente ajenos a su objeto, y al llevar a cabo la adquisición proporcionara determinados datos, tendría la consideración de consumidor, *ex* art. 3 TRLCU.

A este supuesto podría resultar aplicable el TRLCU y en cambio *no* resultaría aplicable el RGPD. No tendría la protección que brinda el RGPD puesto que el art. 1.1 RGPD establece que la normativa tiene por objeto la protección de las *personas físicas*. En definitiva para que la persona jurídica resulte comprendida dentro del término consumidor, el art. 3.II TRLCU exige dos presupuestos que deben concurrir cumulativamente: (i) que actúe en un ámbito *ajeno* a una actividad comercial o empresarial (ii) *sin ánimo de lucro*[7].

Este breve análisis nos muestra que el ámbito subjetivo de aplicación del TRLCU y del RGPD no siempre coinciden. En efecto, el primero, además de aplicarse a las personas físicas, puede resultar aplicable a las personas jurídicas, mientras que el segundo solo es aplicable a las personas físicas.

1.3. La determinación del ámbito objetivo de aplicación del TRLCU

El art. 2 TRLCU determina que «Está norma será de aplicación a las relaciones entre consumidores o usuarios y empresarios».

[7] La ausencia de ánimo de lucro es un presupuesto necesario para la consideración de *consumidor* de una persona jurídica o un ente sin personalidad, pero no para una persona física. (M.J. Marín López, *El "nuevo" concepto de consumidor y empresario tras la Ley 3/2014, de reforma del TRLGDCU*, en *Revista CESCO de Derecho de Consumo*, nº 9, 2014, 9-16, 13).

La condición de consumidor ya ha sido analizada en el epígrafe anterior. En cuanto a las características del empresario, el art. 4 TRLCU dispone que: «A efectos de lo dispuesto en esta norma, se considera empresario a toda persona física o jurídica, ya sea privada o pública, que actúe directamente o a través de otra persona en su nombre o siguiendo sus instrucciones, con un propósito relacionado con su actividad comercial, empresarial, oficio o profesión».

Como ya se ha señalado, los posibles escenarios que se toman en consideración para estudiar los preceptos aplicables son las redes sociales y aquellos en que se obtienen datos en campañas publicitarias o de márqueting (y concretamente, cuando se trata de datos extracontractuales).

En cuanto a las redes sociales, cuando el usuario de una red social accede a la misma goza de un espacio con una serie de aplicaciones y al utilizarlas (así como de forma previa al darse de alta en las mismas), proporciona todo un conjunto de datos personales a dicha red social. El usuario utiliza el espacio que le proporciona la red social e intercambia mensajes con otras personas, accede a información, cuelga fotografías, muestra sus preferencias y publica sus opiniones. El usuario proporciona un conjunto de información especialmente en dos momentos distintos, al darse de alta y en la medida en que utiliza dicha red social e interactúa con otros sujetos. Entre esta información cabe destacar el historial de navegación, las preferencias o bien sus contactos.

Por otro lado existen negocios cuyo único objeto es precisamente la obtención de datos. Esto es, no se trata de que se obtengan datos *extracontractuales* de forma indirecta, sino que todo el negocio se organiza y va dirigido a la obtención de datos. Entre muchos supuestos, un ejemplo lo constituye aquél en que se proporcionan tarjetas de fidelización al afectado de modo que cada vez que realiza una adquisición, el sujeto proporciona dicha tarjeta y ello le permite acumular puntos que luego pueden canjearse por productos o servicios. Esta práctica la llevan a cabo muchísimas empresas, tanto en los negocios *on-line* como *off-line*. La mayoría de grandes superficies o de cadenas comerciales proporcionan tarjetas cliente.

Se trata de tarjetas de fidelización que como su nombre indica persiguen que el consumidor siga ligado a dicha cadena mediante la obtención de descuentos que constituyen un aliciente para seguir consumiendo. Pero la finalidad principal de estas tarjetas es la de

proporcionar datos respecto de sus titulares. Los datos de las actividades comerciales de sus usuarios permiten llevar a cabo análisis de mercado y realizar perfiles de los clientes y enviarles publicidad *ad hoc*.

Por lo tanto es obvio que en los supuestos que se plantean, redes sociales o distintas formas de márqueting, el profesional que ofrece el servicio o producto actúa con un «propósito relacionado con su actividad comercial, empresarial, oficio o profesión». En consecuencia, considero que en las relaciones entre consumidores/usuarios y este tipo de profesionales, resultará aplicable el TRLCU (en base a la aplicación conjunta de los arts. 2, 3 y 4 TRLCU).

2. Análisis de los artículos del TRLCU que podrían resultar aplicables

2.1. Panorama general de los preceptos que pueden resultar aplicables:

En la medida que resulta aplicable el TRLCU, corresponde a continuación analizar qué preceptos concretos del mismo son importantes.

De entrada considero que resultará aplicable todo el Libro I del TRLCU, dedicado a Disposiciones Generales, y concretamente, aquél que resultará más relevante será el Título I, dedicado a: «ámbito de aplicación y derechos básicos de los consumidores y usuarios».

En este título, y dentro del capítulo 2 (derechos básicos de los consumidores y usuarios), existe un precepto esencial. Se trata del art. 8 TRLCU que dispone que

> Son derechos básicos de los consumidores y usuarios:
>
> a) La protección contra los riesgos que puedan afectar su salud o seguridad.
>
> b) La protección de sus legítimos intereses económicos y sociales; en particular frente a las prácticas comerciales desleales y la inclusión de cláusulas abusivas en los contratos.

> c) La indemnización de los daños y la reparación de los perjuicios sufridos.
>
> d) La información correcta sobre los diferentes bienes o servicios y la educación y divulgación para facilitar el conocimiento sobre su adecuado uso, consumo o disfrute.
>
> e) La audiencia en consulta, la participación en el procedimiento de elaboración de las disposiciones generales que les afectan directamente y la representación de sus intereses, a través de las asociaciones, agrupaciones, federaciones o confederaciones de consumidores y usuarios legalmente constituidas.
>
> f) La protección de sus derechos mediante procedimientos eficaces, en especial ante situaciones de inferioridad, subordinación e indefensión.

También constituye un precepto de referencia el art. 19.2. TRLCU que prevé que:

> Sin perjuicio de lo dispuesto en los apartados siguientes, para la protección de los legítimos intereses económicos y sociales de los consumidores y usuarios, las prácticas comerciales de los empresarios dirigidas a ellos están sujetas a lo dispuesto en esta Ley, en la Ley de Competencia Desleal y en la Ley de Ordenación del Comercio Minorista. A estos efectos, se consideran prácticas comerciales de los empresarios con los consumidores y usuarios todo acto, omisión, conducta, manifestación o comunicación comercial, incluida la publicidad y la comercialización, directamente relacionada con la promoción, la venta o el suministro de bienes o servicios, incluidos los bienes inmuebles, así como los derechos y obligaciones, con independencia de que sea realizada antes, durante o después de una operación comercial.

Por otro lado debe tenerse especialmente en cuenta el art. 20 TRLCU que dispone lo siguiente:

Art. 20. Información necesaria en la oferta comercial de bienes y servicios.

1. Las prácticas comerciales que, de un modo adecuado al medio de comunicación utilizado, incluyan información sobre las características del bien o servicio y su precio, posibilitando que el consumidor o usuario tome una decisión sobre la contratación, *deberán contener*, *si no se desprende ya claramente del contexto*, *al menos la siguiente información:*

a) Nombre, razón social y domicilio completo del empresario responsable de la oferta comercial y, en su caso, nombre, razón social y dirección completa del empresario por cuya cuenta actúa.

b) Las características esenciales del bien o servicio de una forma adecuada a su naturaleza y al medio de comunicación utilizado.

c) El precio final completo, incluidos los impuestos, desglosando, en su caso, el importe de los incrementos o descuentos que sean de aplicación a la oferta y los gastos adicionales que se repercutan al consumidor o usuario.

En el resto de los casos en que, debido a la naturaleza del bien o servicio, no pueda fijarse con exactitud el precio en la oferta comercial, deberá informarse sobre la base de cálculo que permita al consumidor o usuario comprobar el precio. Igualmente, cuando los gastos adicionales que se repercutan al consumidor o usuario no puedan ser calculados de antemano por razones objetivas, debe informarse del hecho de que existen dichos gastos adicionales y, si se conoce, su importe estimado.

d) Los procedimientos de pago, plazos de entrega y ejecución del contrato y el sistema de tratamiento de las reclamaciones, cuando se aparten de las exigencias de la diligencia profesional, entendiendo por tal la definida en el artículo 4.1 de la Ley de Competencia Desleal.

e) En su caso, existencia del derecho de desistimiento.

2. El incumplimiento de lo dispuesto en el apartado anterior será considerado práctica desleal por engañosa en iguales términos a los que establece el artículo 7 de la Ley 3/1991, de 10 de enero, de Competencia Desleal.

De entre los distintos aspectos que se recogen en estos preceptos, aquellos que se consideran más relevantes, en el presente trabajo, son los relativos a la información que debe proporcionarse. La razón de ello ya ha sido subrayada previamente: por tratarse de uno de los principales deberes que forman parte de la fase preparatoria de una relación jurídica y por constituir también un Principio de protección de datos.

2.2. Los preceptos relativos al deber de información

Como ya se ha podido constatar, en la normativa de defensa de consumidores y usuarios, en la fase previa a la celebración de los contratos, destacan los deberes de información precontractual. Ello es debido a que en la contratación de consumo se da una situación de asimetría o desigualdad informativa.

Esta desigualdad informativa trata de paliarse con las normas protectoras de los consumidores a través de la imposición a los empresarios o profesionales de determinados deberes precontractuales de información.

Se pretende asegurar que el consumidor conozca las características esenciales del contrato y del bien o servicio que pretende adquirir, y que a la vista de la información proporcionada pueda decidir fundadamente sobre si contratar o no. La doctrina distingue entre (i) deberes genéricos de información y (ii) deberes específicos de información.

2.2.1. Deberes de información genéricos

Tal y como determina el art. 8.d) TRLCU, constituye un *derecho básico de los consumidores y usuarios* la información correcta sobre los diferentes bienes o servicios. En consonancia con este precepto, el art. 17.1 TRLCU determina que los poderes públicos deben asegurar que los consumidores y usuarios dispongan de la información precisa para el eficaz ejercicio de sus derechos y velen para que se les preste información comprensible.

Así mismo existen otros preceptos que es preciso tener en cuenta. El art. 20 TRLCU, como ya se ha dicho, tiene como finalidad evitar prácticas comerciales engañosas en los casos en que los empresarios dirigen a los consumidores auténticas ofertas comerciales en sentido técnico jurídico. La finalidad es que el consumidor adopte decisiones informadas.

El art. 20 TRLCU dispone que las prácticas comerciales que incluyan información sobre las características del bien o servicio y su precio, posibilitando que el consumidor o usuario tome una decisión sobre la contratación, deberán contener un conjunto de información, si no se desprende claramente del contexto.

La información deberá hacer referencia a los datos que permiten identificar al empresario responsable de la oferta, datos relativos a las características esenciales del bien o servicio, el precio final completo, procedimientos de pago, plazos de entrega, ejecución del contrato y sistema de tratamiento de las reclamaciones y en su caso, la existencia del derecho de desistimiento [vid. art. 20.1. § (a) a (e)].

El art. 20 TRLCU establece dos reglas de presentación de la información. Se trata de la aplicación de los principios de veracidad y proporcionalidad en el suministro de la información. Estos requisitos están relacionados con las reglas contenidas en la Ley de competencia desleal relativas a omisiones engañosas. Según esta ley, se considera desleal (omisión engañosa), el supuesto en que «la información que se ofrece es poco clara, ininteligible, ambigua, no se ofrece en el momento adecuado, o no se da a conocer el propósito comercial de esa práctica, cuando no resulte evidente por el contexto» (art. 7.1 LCD)[8].

Existe por lo tanto una auténtica obligación legal del empresario de suministrar al consumidor información previa al contrato. Según CÁMARA, «[p]uede decirse con razón que en el ámbito de la contratación de consumo se ha invertido el paradigma, pasando de un consentimiento libre, basado en la autonomía de las partes, a un consentimiento informado, garantizado por deberes legales de información precontractual en aras de una mayor solidaridad en el ámbito contractual».

Con estos deberes se pretende en definitiva: (i) Proteger la libertad de decidir sobre si contratar o no con pleno conocimiento de causa. (ii) Permitir conocer las cualidades de la prestación en términos que permitan comparar los bienes o servicios, *junto con sus condiciones jurídicas y económicas*. Se trata no solo de garantizar un consentimiento libre y bien formado, sino también de favorecer la

[8] Ley 3/1991, de 10 de enero, de Competencia Desleal. BOE n. 10, de 11 de enero de 1991. Última modificación: 28 de marzo de 2014.

competencia y el correcto funcionamiento del mercado. (iii) Facilitar la comprensión del alcance del compromiso que se adquirirá, tanto en el plano económico como jurídico.

La doctrina infiere cuatro principios de estos deberes de información.

i. Principio de transparencia. La información que debe suministrarse al consumidor debe ser clara y comprensible, tal y como se establece en los requisitos de transparencia/incorporación de las cláusulas no negociadas individualmente (art. 80 TRLCU). Reglas relativas a la posibilidad de comprensión directa, accesibilidad y legibilidad, de forma que permita al consumidor el conocimiento previo a la celebración del contrato. Para determinar si la información precontractual es comprensible, el parámetro lo constituye el consumidor medio.
ii. Principio de proporcionalidad. La información debe ponerse a disposición del consumidor de forma adaptada a las circunstancias y ser relevante y suficiente. No se requiere una información exhaustiva, que podría resultar contraria al principio de proporcionalidad y que por el contrario podría crear confusión y no comprensión en el consumidor.
iii. Principio de veracidad, pues se requiere que la información sea veraz. En cuanto a este requisito, se busca evitar que la falsedad pueda confundir al consumidor, bien por vía de afirmaciones falaces, bien de inexactitudes o de omisiones engañosas.
iv. Principio de gratuidad. La información debe suministrarse de forma gratuita.

Llevado a cabo este análisis puede afirmarse que el contenido de la información que debe proporcionarse puede resultar excesiva. Como se ha indicado, el hecho que la norma establezca una exhaustiva relación de deberes informativos obedece al intento de corregir la situación de asimetría/desequilibrio entre las partes contratantes. Estas exigencias informativas tienen su fundamento en la buena fe y pretenden lograr que las decisiones negociales de los afectados sean auténticamente libres.

Junto con los preceptos que regulan cómo debe materializarse el deber de información, existen aquellos preceptos que sancionan su incumplimiento: arts. 20.2 y art. 49 TRLCU.

2.2.2. Deberes de información específicos

Tienen especial interés los deberes impuestos en la Ley 34/2002, de 11 julio, Ley de Servicios de la Sociedad de la Información (LSSI)[9] y a los que el propio TRLCU hace referencia.

En la relación TRLCU - LSSI, se declara supletoria la primera respecto de la segunda. Sin embargo, si una disposición general o sectorial sobre prestación de servicios, incluidos los servicios de la sociedad de la información y de comercio electrónico, en lo referente al *contenido o el modo* en que se debe proporcionar la información entrara en conflicto con alguna disposición del TRLCU, prevalecerá este último (art. 97.7.2 TRLCU).

Por lo tanto, es claro que se da una importancia primordial al contenido y modo de proporcionar información, puesto que a pesar de que el art. 94.2 TRLCU declara al TRLCU como supletorio respecto de la LSSI, se excepciona, en caso de contradicción entre ambas normas, aquellos aspectos relativos al contenido y modo de proporcionar la información, en que prevalecerá el TRLCU (art. 94.2[10] y 97.7.2 TRLCU).

La LSSI establece en varios artículos deberes de información:

Art. 10.1 LSSI: el prestador de servicios de la SI debe proporcionar los datos que permitan identificar al prestador de servicios de la sociedad de la información. También es preciso publicar una serie de datos relativos al precio del producto o servicio y la circunstancia de si el prestador está adherido a determinados códigos de conducta [art. 10.1 § (a) a (g) LSSI].

[9] Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico. BOE n. 166, de 12 de julio de 2002

[10] Téngase en cuenta que el art. 94 TRLCU se halla ubicado en el Libro II (contratos y garantías), Título III (contratos celebrados a distancia y contratos celebrados fuera del establecimiento mercantil), Capítulo I (Disposiciones generales). El art. 94 hace referencia a las comunicaciones comerciales y contratación electrónica. Se dispone en este precepto que en las comunicaciones comerciales por correo electrónico y en la contratación a distancia por medios electrónicos se aplicará además de lo dispuesto en este título, la normativa específica sobre servicios de la sociedad de la información (art. 94.1). En caso de contradicción entre las disposiciones de este Título del TRLCU y la LSSI, esta última será preferente, salvo lo previsto en el art. 97.7, párrafo segundo (art. 94. TRLCU).

La importancia de estos deberes de información se constata al analizar las sanciones que su incumplimiento lleva aparejado: art. 38.3.b) y 38.4.b) LSSI.

Por otro lado, según dispone el art. 12 *bis*.1. LSSI, «Los proveedores de servicios de intermediación establecidos en España de acuerdo con lo dispuesto en el artículo 2 de esta Ley que realicen actividades consistentes en la prestación de servicios de acceso a Internet, estarán obligados a informar a sus clientes de forma permanente, fácil, directa y gratuita, sobre los diferentes medios de carácter técnico que aumenten los niveles de la seguridad de la información y permitan, entre otros, la protección frente a virus informáticos y programas espía, y la restricción de los correos electrónicos no solicitados». De nuevo se establece la exigencia de que se trate de información permanente, fácil, directa y gratuita.

El hecho de no suministrar la información debida puede ser constitutivo de una infracción leve *ex* art. 38.4.c) LSSI[11].

Otro de los supuestos en que debe proporcionarse información es aquel relacionado con la instalación de cookies y otros datos en los equipos de los destinatarios de las comunicaciones. Según dispone el art. 22.2. LSSI «Los prestadores de servicios podrán utilizar dispositivos de almacenamiento y recuperación de datos en equipos terminales de los destinatarios, a condición de que los mismos *hayan dado su consentimiento* después de que se les haya facilitado información clara y completa sobre su utilización, en particular, sobre los fines del tratamiento de los datos, con arreglo a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal».

El incumplimiento de la previsión relativa a la obtención del consentimiento previa información adecuada puede ser constitutivo de una infracción leve *ex* art. 38.4.g) LSSI. Sin embargo, esta misma conducta, según las circunstancias, puede ser constitutiva de una sanción grave [38.3.i) LSSI].

Por otro lado, en los supuestos en que se pretenda perfeccionar un contrato, ello comportará una serie de obligaciones informativas.

[11] Puede constituir un supuesto de infracción leve «El incumplimiento de lo previsto en el artículo 20 para las comunicaciones comerciales, ofertas promocionales y concursos».

Dispone el art. 27.1 LSSI que «Además del cumplimiento de los requisitos en materia de información que se establecen en la normativa vigente, el prestador de servicios de la sociedad de la información que realice actividades de contratación electrónica tendrá la obligación de poner a disposición del destinatario, antes de iniciar el procedimiento de contratación y mediante técnicas adecuadas al medio de comunicación utilizado, de forma permanente, fácil y gratuita, información clara, comprensible e inequívoca sobre los siguientes extremos». Concretamente se refiere a los trámites necesarios para celebrar el contrato, la accesibilidad del documento electrónico en que se formalice el contrato, los medios técnicos que se ponen a disposición del interesado y las lenguas en que podrá formalizarse el contrato [art. 27.1 § (a) a (d) LSSI][12].

Del mismo modo, junto a la información contemplada en el art. 27.1 LSSI, deberá proporcionarse otra. Según dispone el art. 27.4 LSSI: «Con carácter *previo al inicio del procedimiento de contratación*, el prestador de servicios deberá *poner a disposición del destinatario* las *condiciones generales* a que, en su caso, deba sujetarse el contrato, de manera que éstas puedan ser *almacenadas y reproducidas* por el destinatario».

El art. 27.1 hace referencia a un deber de información relativo a los aspectos del perfeccionamiento del contrato (requisitos más bien relacionados con la utilización de la tecnología). En cambio el art. 27.4 hace referencia a supuestos más relacionados con el *contenido del contrato*, en concreto con las condiciones generales a que deba sujetarse el contrato.

El incumplimiento de estos deberes está sujeto a diferentes tipos de sanciones [(infracción *leve*, *ex* art. 38.4.e) LSSI; infracción *grave*, art. 38.3.e) LSSI][13].

[12] Por otro lado el art. 27.2 LSSI establece unos supuestos en que el prestador no tendrá la obligación de facilitar la información señalada en el apartado anterior: si ambos contratantes así lo acordaren, y ninguno de ellos tuviera la consideración de consumidor, y por otro lado si el contrato se celebrara exclusivamente mediante el intercambio de correo electrónico u otro tipo de comunicación electrónica equivalente.

[13] En este caso se estaría vulnerando la obligación establecida en el art. 27.4 LSSI. En cuanto a las consecuencias que puede tener el incumplimiento del deber de informar *ex* art. 10 y 27 LSSI y sus posibles consecuencias relativas a la validez del

3. Los deberes de información en el RGPD

Como ya se ha reiterado, la necesidad de proporcionar información forma parte de la definición de consentimiento para el tratamiento de datos (art 4. 11 RGPD)[14] y también constituye un Principio de protección de datos [art. 5.1.a) RGPD].

Ello se puede analizar desde dos perspectivas: (i) contenido de la información y (ii) la forma de proporcionar la información. Nos centraremos en el contenido de la información.

De forma más específica, los deberes de información se regulan en los arts. 12, 13 y 14 RGPD. Estos preceptos concretan la información que debe proporcionarse al afectado, distinguiendo en función de si los datos han sido recabados del afectado o no es así[15].

3.1. Supuesto en que los datos son recabados del afectado (art. 13 RGPD)

En cuanto al ámbito subjetivo, es necesario proporcionar información sobre la identidad del responsable del tratamiento o de su representante y en el caso de existir, los datos de contacto del delegado de protección de datos [art. 13.1.b) RG]. Así mismo también es preciso informar acerca de los destinatarios o categoría de destinatarios de los datos [art. 5.1.a) LOPD, art. 13.1.e) RGPD] y de la intención de llevar a cabo transferencias internacionales de datos [art. 13.1.f) RGPD].

contrato, véase P. Grimalt Servera, *La formación del contrato celebrado por medios electrónicos*, en M.A. Parra Lucán (dir.), *Negociación y perfección de los contratos*, Cizur Menor, Thomson-Aranzadi, 2014, 1ª ed., 355-392, 371-372.

[14] En cuanto a los requisitos del consentimiento, véase el documento del Grupo del art. 29, WP 259 rev.01, *Guidelines on consent under Regulation 2016/679*, adoptado el 28 de noviember 2017, y revisado y adoptado el 10 de abril de 2018, véase los §§ 2 y 3.

[15] En relación al deber de información, véase el documento del Grupo del art. 29, WP 260 rev.01, *Guidelines on transparency under Regulation 2016/679*, adoptado el 29 de noviembre de 2017, y revisado y adoptado el 11 de abril de 2018. Concretamente, en cuanto a la información que debe proporcionarse, véase los §§ 23 a 29. Resulta útil consultar el anexo en que consta una tabla con la información que debe proporcionarse y que comprara los arts. 13 y 14, *vid*. páginas 35 a 40. También puede consultarse el documento del Grupo del art. 29, WP 259, cit, §§ 3.3.

En cuanto al contenido del tratamiento, aquello más relevante sobre lo que tendrá que informarse es acerca de los fines del tratamiento a que se destinan los datos [art. 13.1.c) RGPD].

Asimismo un aspecto que considero de gran relevancia es la necesidad de informar, según dispone el RGPD, acerca de la base jurídica del tratamiento [art. 13.1.c) RGPD].

En aquellos casos en que el tratamiento se base en el art. 6, apartado 1, letra f), también deberá informarse acerca de los intereses legítimos del responsable o de un tercero [art. 13.1.d) RGPD]. Esto es, no solo que se está recurriendo a esta base legal que habilita el tratamiento de datos, sino especificar también cual es el interés legítimo en que se fundamenta el tratamiento concreto.

En cuanto al contenido, según el RGPD también es preciso hacer referencia a los derechos que puede ejercer el afectado [5.1.d) LOPD y art. 13.2.b) RGPD]. También del derecho a presentar una reclamación ante la autoridad de control [art. 13.2.d) RGPD].

Asimismo debe informarse acerca de si la comunicación de los datos es un requisito legal o contractual, o bien un requisito necesario para suscribir un contrato, y si el afectado está obligado o no a facilitar los datos y las consecuencias de no hacerlo [art. 13.2.e) RGPD].

Constituye una novedad el hecho de tener que proporcionar información del plazo durante el cual se conservarán los datos y si ello no fuera posible, de los criterios utilizados para determinar este plazo [art. 13.2.a) PRGPD]. Otro aspecto sobre el que debe informarse es acerca de la facultad de revocar el consentimiento [el RGPD hace referencia a retirar), *ex* art. 13.2.c) RGPD].

El RGPD establece, respecto de la información que debe proporcionarse, que no será preciso proporcionar la información referida cuando y en la medida que el interesado ya disponga de la misma [art. 13.4 RGPD].

3.2. Cuando los datos *no* se obtengan del afectado por el tratamiento (art. 14 RGPD)

En cuanto al ámbito subjetivo, es preciso proporcionar información sobre la identidad del responsable del tratamiento y sus datos de contacto y en su caso de su representante [art. 14.1.a) RGPD]. También, en caso de que exista, de los datos de contacto del delegado de protección de datos [art. 14.1.b) RGPD]. Asimismo también es preciso

informar acerca de los destinatarios o categoría de destinatarios de los datos (art. 4.1.e) RGPD] y de la intención de llevar a cabo transferencias internacionales de datos [art. 14.1.f) RGPD].

En relación al ámbito objetivo, el RT facilitará al interesado información relativa a los fines del tratamiento a que se destinan los datos y la base jurídica del mismo y las categorías de datos personales de que se trate [arts. 14.1.c) y d) RGPD]. El aspecto más relevante es que debe informarse de «la fuente de la que proceden los datos personales y, en su caso, si proceden de fuentes de acceso público» [art. 14.2.f) RGPD]. Esta exigencia es lógica, en la medida que precisamente en este caso los datos no se han obtenido del afectado. También debe informarse acerca de la categoría de datos que se recaban [art. 14.1.d) RGPD].

3.3. Información a proporcionar en los casos de elaboración de perfiles

Un aspecto importante contemplado en el RGPD es la regulación del cumplimiento del deber de información en los supuestos de elaboración de perfiles, aspecto regulado en los arts. 13.2 (f), 14.2 (g) y 22 RGPD[16].

Este deber de información ya se establecía en la Directiva [art. 12.a.iii) DPD], que al regular el derecho de acceso ya contemplaba un derecho de información en cierto modo similar. Concretamente reconocía el derecho del interesado de obtener del responsable del tratamiento, «el conocimiento de la lógica utilizada en los tratamientos automatizados de los datos referidos al interesado, al menos en los casos de las decisiones automatizadas a que se refiere el apartado 1 del art. 15».

Un aspecto positivo de los preceptos del RGPD (arts 13.2 y 14.2) es que no hacen depender el hecho de proporcionar información de que lo solicite el afectado, en la medida que establecen: «Además de la información mencionada en el apartado 1, el *responsable del tratamiento facilitará al interesado* la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente respecto del interesado: [...]». En consecuencia, los arts. 13.2 y 14.2 RGPD no condicionan la comunicación de la información a la iniciativa del afectado por el tratamiento (esto es, de que lo solicite) sino que se

[16] Al respecto *vid* el documento del Grupo del art. 29, WP 260 rev.01, *cit*, § 41.

establece un deber positivo a cargo del responsable del tratamiento de proporcionar dicha información.

Sin embargo, en cuanto al contenido del deber de informar, este queda en cierta forma diluido, en la medida en que dispone que se proporcionará *información significativa* sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado [arts. 13.2 (f) y 14.2 (g) RGPD]. Por esta razón algunos autores consideran que en realidad no existe en el RGPD un verdadero derecho a obtener una explicación acerca de las decisiones automatizadas[17].

Finalmente debe mencionarse que en otros supuestos, por ejemplo como disponen los arts. 15 a 22 y 34 RGPD (este último relativo a la comunicación de una violación de la seguridad al interesado), puede que deba facilitarse más información (u otra información) al afectado (*vid* art. 12.1 RGPD).

4. ¿Comporta la aplicación del TRLCU una mayor protección que la ofrecida exclusivamente por el RLOPD?

la cuestión que se analiza en este punto es si la aplicación de los preceptos del TRLCU que han sido identificados en los epígrafes anteriores comporta un incremento de protección para el afectado respecto aquel ofrecido exclusivamente por las normas relativas al tratamiento de datos personales.

En definitiva, si el TRLCU aporta o no un nivel de protección suplementario. Este análisis se focalizará en las disposiciones relativas al deber de información.

4.1. Los aspectos más relevantes del deber de información

Se constata como TRLCU y RGPD establecen el deber de proporcionar información relativa a diferentes preguntas que se pueden plantear. Entre ellas destacan las relativas a *quién* y a *qué*.

[17] Véase por todos: S. Wachter-B. Mittelstadt-L. Floridi, *Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation*, *International Data Privacy Law*, 2017. Disponible en SSRN: https://ssrn.com/abstract=2903469 or http://dx.doi.org/10.2139/ssrn.2903469

En cuanto a la primera de ellas, el *quién*, se trata en definitiva de contestar las cuestiones relativas a quién es el responsable del tratamiento así como identificar al empresario que proporciona el bien o servicio.

Los arts. 13.1.a) y 14.1.a) RGPD disponen el deber de identificar al sujeto responsable del tratamiento y el texto refundido también establece la necesidad de identificar correctamente al empresario que es el responsable de la oferta [art. 20.1.a) TRLCU].

En definitiva, proporcionar información respecto dos responsables, que puede que sean el mismo sujeto o bien que no sea así.

Piénsese en el caso de proporcionar datos para participar en un sorteo de un ipad. Quién diseña la campaña lo que persigue es obtener una base de datos saneada para posteriormente llevar a cabo una campaña publicitaria. Puede que el sujeto que es el RT, quién se presenta como tal, sea así mismo quién ha diseñado la estrategia económica del negocio (recabar datos para generar una base de datos), pero puede que se trate de dos sujetos distintos.

Puede tratarse de una misma persona que lleve a cabo dos roles distintos, o bien de dos sujetos distintos que desempeñan sus respectivas responsabilidades. Sin embargo, deberá proporcionarse información al afectado respecto de los dos responsables, y ello puede generar confusión y desconcierto en el afectado/consumidor. La fuente de confusión no es tanto el hecho de reiterar la información, sino que deberá proporcionarse información que afecta dos aspectos similares (*quién* es el responsable) y puede que tenga la misma respuesta o que no sea así.

El otro aspecto sobre el que recae un deber primordial de información es sobre el *qué*. Sobre el objeto del tratamiento y objeto del negocio llevado a cabo. En consecuencia, deberá informarse acerca del tratamiento de los datos y del negocio concreto que existe como sustrato del tratamiento de la información personal.

Según dispone el RGPD, deberá informarse principalmente acerca de:

- la finalidad del tratamiento y la base jurídica del mismo [arts. 13.1.c) y 14.1.c) RGPD];
- la intención de transferir los datos [arts. 13.1.f) y 14.1.f) RGPD];
- el plazo durante el que se conservarán los datos [arts. 13.2.a) y 14.2.a) RGPD];

- si el interesado está o no obligado a facilitar los datos y las consecuencias de no hacerlo [art. 13.2.e) RGPD];
- la fuente de la que proceden los datos [art. 14.2.f) RGPD]
- la existencia de decisiones automatizadas, incluida la elaboración de perfiles [arts. 13.2.f) y 14.2.g) RGPD].

En cuanto al TRLCU, aquello más relevante es la información referente a:

- las características esenciales o principales del bien o del servicio [arts. 20.1.b, 60.2.a) y 97.1.a)]
- el precio final completo [arts. 20.1.c, 60.2.c), 97.1.e)].

Siguiendo con el ejemplo del supuesto en que se invita a proporcionar datos a cambio de participar en el sorteo de un ipad, los deberes de información relativos al contenido diferirán. En cuanto al marco del RGPD, se deberá informar de que se tratarán datos para una finalidad de márqueting.

En el marco del TRLCU, considero que debería explicarse mínimamente el objeto del negocio llevado a cabo. Esto es, cuál es el *objetivo* de la obtención de los datos en *un sentido económico*. Se trataría de dotar de contenido a una de las finalidades que se atribuye a la información. Concretamente, se trata de facilitar la comprensión del alcance del compromiso que se adquirirá, tanto en el plano económico como jurídico, con el desglose previo de las circunstancias en que se desenvolverá la ejecución del contrato y los derechos y obligaciones que afectarán al consumidor[18].

Precisamente este último aspecto es aquél que considero más relevante. En consecuencia, ante un determinado hecho, proporcionar

[18] CÁMARA, al hacer referencia al fundamento de los deberes de información precontractual, indica que estos tienen distintas finalidades. En primer lugar, proteger la libertad de decidir sobre si contratar o no con pleno conocimiento de causa. En segundo lugar, permitir conocer las cualidades de la prestación en términos que permitan comparar los bienes o servicios, así como sus condiciones jurídicas y económicas. En tercer lugar, facilitar la comprensión del alcance del compromiso que se adquirirá, tanto en el plano económico como jurídico, con el desglose previo de las circunstancias en que se desenvolverá la ejecución del contrato y los derechos y obligaciones que afectarán al consumidor. Véase, S. Cámara Lapuente, *Comentario al artículo 60 TRLCU*, en S. Cámara Lapuente (dir), *Comentarios a las Normas de Protección de los Consumidores. Texto refundido (RDL 1/2007) y otras leyes y reglamentos vigentes en España y en la Unión Europea*, Madrid, Colex, 2011, 484-510, 489.

información para participar en un sorteo, existen distintas normativas para las que esta conducta será relevante.

En base al RGPD, ello comportará un deber de información en la medida que se obtienen datos personales.

En base al TRLCU deberá informarse acerca del porqué se lleva a cabo una conducta relevante en tanto que el sujeto es un consumidor. Si se lleva a cabo un contrato, en este caso existirán los deberes de información derivados del art. 60 TRLCU, cuya finalidad principal es que el afectado/consumidor entienda qué negocio subyace al tratamiento de datos[19]. Y esto en la mayoría de las ocasiones no se explica adecuadamente.

Normalmente la información que se facilita es que de proporcionarse los datos se participará en un sorteo de un determinado bien. Pero esta *no es la verdadera finalidad del negocio jurídico*. Si se facilitan los datos, el empresario los utilizará para llevar a cabo un análisis de mercado y perfiles de los afectados.

Sin embargo, para fomentar y motivar que las personas proporcionen información, se utiliza como anzuelo la participación en un sorteo. Pero la finalidad económica del negocio es que la empresa X pueda confeccionar una base de datos saneada y legitimada y esté habilitada para tratar los datos de los consumidores/afectados (realizar estudios de mercado, campañas publicitarias o incluso ceder los datos a terceros). En definitiva, aquello fundamental es explicar no solo cuál es la finalidad del tratamiento, sino del *negocio concreto que se lleva a cabo*, que es más amplio que el tratamiento.

Si solo se presta atención a la relación de tratamiento de datos solo debería proporcionarse información sobre el responsable del tratamiento de datos y de la finalidad de dicho tratamiento: participar en un sorteo de un ipad.

Sin embargo, considero que también debe informarse sobre el negocio que subyace al tratamiento, la realización de perfiles y la elaborar una base de datos con finalidades de márqueting. En definitiva, si solo se tiene en cuenta el hecho de proporcionar el dato de

[19] El afectado/consumidor proporciona datos para participar en un sorteo pero la finalidad de este negocio es la de engrosar una base de datos con finalidad de márqueting y llevar a cabo perfiles de los sujetos cuyos datos son procesados.

forma aislada solo debería explicarse la finalidad del tratamiento, que es la de participar en un sorteo. Sin embargo, junto con el tratamiento de datos existe un negocio jurídico más amplio que subyace y respecto del que también debe informarse.

En este sentido, un aspecto que puede parecer inocuo pero que tiene trascendencia es el relativo al precio. El art. 20.1.c) TRLCU hace referencia a la necesidad de hacer constar el *precio final completo*. En relación con esta exigencia, considero que sería contrario a este precepto declarar que un servicio que se presta o un bien que se proporciona es gratuito cuando en realidad se están recabando datos personales, actividad que constituye un beneficio importante para el responsable del tratamiento/empresario. Es más, incluso puede argumentarse que el hecho de afirmar que se trata de un bien o servicio gratuito podría calificarse como práctica comercial desleal en base al art. 5.1.e) LCD[20].

Al respecto resulta oportuno hacer referencia a una Recomendación de la Comisión francesa de cláusulas abusivas que analizó las condiciones de los contratos de prestación de servicios de redes sociales y las comparó con el ordenamiento francés[21].

[20] El art. 5.1.e) LCD dispone que «1. Se considera desleal por engañosa cualquier conducta que contenga información falsa o información que, aun siendo veraz, *por su contenido o presentación induzca o pueda inducir a error a los destinatarios*, siendo susceptible de alterar su comportamiento económico, siempre que incida sobre alguno de los siguientes aspectos: [...] (e) El precio o su modo de fijación, o la existencia de una ventaja específica con respecto al precio».

Señala ZITTRAIN: «When something online is free, you're not the customer, you're the product».

Esta frase de ZITTRAIN, se ha convertido en una afirmación de referencia. Sin embargo, el mismo autor señala que él la tomó prestada de alguien que la utilizó previamente y ZITTRAIN realizó una pequeña investigación acerca de dónde surgió: Vid: *http://blogs.law.harvard.edu/futureoftheinternet/2012/03/21/meme-patrol-when-something-online-is-free-youre-not-the-customer-youre-the-product/*

Además de las pesquisas de ZITTRAIN, existe una entrada en el blog en que se atribuye una frase muy parecida a Noam Chomsky en 1990. En cualquier caso considero que la frase es muy gráfica.

[21] Se trata de la *Recommandation n° 2014-02 relative aux contrats proposés par les fournisseurs de services de réseaux sociaux*
http://www.clauses-abusives.fr/recom/14r02.htm

De entrada resulta relevante que dicha Comisión califica como contrato de adhesión aquel que se celebra entre el prestador de servicios de una red social y el consumidor que la utiliza. Dicha Comisión pone de relieve las características especiales de estos contratos: asimetría informacional, la puesta a disposición del servicio sin contrapartida dineraria, la instantaneidad de la adhesión del usuario y la multiplicidad de documentos con múltiples reenvíos a otros textos.

Dicha Comisión analizó distintos aspectos de este contrato: la legibilidad y redacción del contrato; la formación, contenido y ejecución del contrato y la resolución de conflictos. En cuanto al contenido, se detiene a analizar la que denomina como cláusula de gratuidad.

Se pone de relieve como la mayoría de servicios de redes sociales establecen cláusulas en que se afirma que los servicios proporcionados son gratuitos y que dichas cláusulas hacen creer al usuario que los servicios proporcionados carecen de toda contrapartida por su parte. Sin embargo, dicha Comisión declara que si se excluye toda contrapartida monetaria, aquello que constituye una contraprestación es toda la información, datos y contenidos que el usuario de dicha red social deposita en la misma. En consecuencia la Comisión considera que el hecho de afirmar el carácter gratuito constituye una ambigüedad de la cláusula relativa a la remuneración en la medida que hace creer al usuario que no proporciona ningún tipo de contrapartida por el servicio, cuando en realidad constituye dicha contraprestación el conjunto de datos personales e informaciones depositados. En consecuencia, una de las Recomendaciones de dicha Comisión es la de *eliminar* de los contratos propuestos por los proveedores de redes sociales las cláusulas que afirmen que los servicios de redes sociales son gratuitos[22].

Al hilo de estas argumentaciones, considero que determinados prestadores de servicios, como es el caso de las redes sociales o de otras plataformas que teóricamente ofrecen servicios gratuitos, deberían hacer constar cuál es el valor que consideran que tiene el servicio ofrecido.

La razón es que aquello que ofrecen tiene un coste e indirectamente se está cobrando por prestar dicho servicio. Se está cobrando

[22] Véase entre las Recomendaciones finales, § 14.

mediante los datos que se obtienen. Por lo tanto, este aspecto debería ponerse de relieve. Si se informa de que el servicio que presta una red social tiene un coste mensual de X, el usuario de algún modo podría deducir que el valor de su información personal que se halla en la red como mínimo asciende a dicho valor[23].

La exigencia de revelar el precio podría traducirse, en el contexto de tratamiento de datos personales, de dos maneras. Una de ellas sería la exigencia de que el prestador del servicio informara del coste real del servicio. La otra opción sería cuantificar el valor de la información personal del usuario/afectado por el tratamiento[24].

[23] Al respecto resulta muy interesante el artículo de Malgieri y Custers, *Pricing privacy - the right to know the value of your personal data*. Estos autores proponen una solución en el sentido de hacer que el afectado/consumidor sea consciente del valor que en el mercado tienen sus datos personales. Concretamente proponen, *de lege ferenda*, introducir un nuevo derecho de información respecto a los ya existentes en los arts. 13 y 14 RGPD. Se trataría del derecho a conocer el valor de los datos personales que son objeto del mercado digital. Estos autores ponen de relieve que la monetización de los datos personales es una realidad cada vez más patente y una práctica generalizada de muchos negocios digitales. Sin embargo el sujeto afectado en la mayoría de los casos no es consciente ni de la mercantilización de sus datos ni del valor económico de los mismos. Esta ignorancia le quita poder negociador. Malgieri y Custers consideran que es posible cuantificar el valor económico de los datos personales y hacen referencia a distintos mecanismos para llevarlo a cabo. También ponen de relieve como algunas iniciativas legislativas [Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a determinados aspectos de los contratos de suministro de contenidos digitales. Bruselas, 9.12.2015, COM (2015) 634 final. 2015/0287 (COD)] hacen referencia a la monetización de los datos personales. Sin embargo, la posibilidad de pagar con los datos en lugar de hacerlo con dinero consideran que es contraria al art. 7.4 RGPD. Por ello dichos autores proponen la introducción de un nuevo derecho, el derecho a conocer el valor de los datos personales. A pesar de ser conscientes de las dificultades prácticas, morales y cognitivas que su propuesta comporta, consideran que es un camino que debe continuar explorándose.
Vid G. Malgieri y B. Custers, *Pricing privacy - the right to know the value of your personal data*, Computer Law & Security Review, Volume 34, Issue 2, 2018, 289-303. Disponible en: *https://doi.org/10.1016/j.clsr.2017.08.006. http://www.sciencedirect.com/science/article/pii/S0267364917302819*

[24] Si Facebook declara por ejemplo que el servicio que presta de proporcionar la red social a sus usuarios tiene un coste de 20 € mensuales, de esta afirmación pueden extraer dos consecuencias: (i) que si no los exige está proporcionando el

4. Conclusiones

La aplicación, en los supuestos en que se trate información personal, del RGPD junto con el TRLCU comportará, entre otras consecuencias, que sea necesario proporcionar más información al afectado. Sustancialmente aquella que será más relevante es la relativa al *quién* y al *qué*.

En cuanto al *quién*, y desde el punto de vista del afectado/consumidor, ello puede generarle más confusión y desconcierto. El destinatario de la información puede percibirlo simplemente como una duplicidad de información (superpuesta), sin entender que ello obedece a obligaciones distintas. En este caso debería intentar unificarse la información proporcionada y simplificarse al máximo. Aquello que debería asegurarse es trasmitir adecuadamente la información relativa a quién dirigirse para ejercer los derechos reconocidos en cada ámbito normativo.

En cuanto al *qué*, considero indispensable hacer referencia tanto al tratamiento de los datos personales como al negocio concreto que pueda existir como sustrato del mismo. Entre otros extremos es preciso hacer referencia al precio concreto del bien o servicio proporcionado. En según que circunstancias, la referencia al carácter gratuito

servicio gratis (ii) o bien que obtiene algo a cambio, cfr los datos de los usuarios que utilizan el servicio. Esto es, no solo la información que estos proporcionan al darse de alta, sino también la que generan al utilizar la red social. El consumidor se da de alta en la red social y aporta una serie de datos que son imprescindibles para darse de alta en el servicio. Además, a medida que utiliza la red, constantemente aporta más información. Bien de forma consciente, al colgar fotos, poner determinados posts, o bien de forma no consciente, al navegar, escoger determinadas páginas, determinados amigos o bien establecer preferencias. Esta información tiene sin duda un gran valor. Considero que Facebook debería al menos declarar el valor que de forma aproximada atribuye a dicha información o bien poner un precio al servicio que presta.

Sin embargo, debe reconocerse que la determinación del precio/valor de los datos no es una cuestión pacífica. Así lo expone L. Kugler, *The War Over the Value of Personal Data*, en *Communications of the ACM*, february 2018, vol. 61, n. 2, 17-19. Este autor señala que «turning consumer data into dollars can be difficult. The real value of data may actually lie in its aggregation», cit, 18.

https://cacm.acm.org/magazines/2018/2/224626-the-war-over-the-value-of-personal-data/fulltext

de determinados negocios puede violar el TRLCU y la LCD. Esta última norma puede ser de gran ayuda, en la medida que la información y las conductas no adecuadas pueden constituir supuestos de prácticas comerciales desleales y en consecuencia ser sancionadas en base a la LCD y al TRLCU.

En conclusión, la aplicación conjunta del RGPD y el TRLCU comportará una mayor carga informativa para el responsable/empresario. Para el destinatario de la misma, más información que leer y entender. Y ello no es necesariamente positivo[25].

Si bien el contenido de la información que se ha ido desgranando es importante, el tener que transmitirla al afectado no garantizará una mejor ni mayor tutela del mismo. En definitiva, se constata una contradicción entre la finalidad de los deberes de información (garantizar la transparencia frente al afectado/reducir la asimetría) y la eficacia de los mismos. La abundancia de contenidos informativos puede ser contraproducente para el consumidor. El único aspecto que considero que sí puede aportar una mayor protección al afectado es la exigencia de tener que informar acerca del precio del producto o servicio proporcionado.

En cualquier caso, la aplicación conjunta de ambos textos normativos comporta una mayor carga informativa y ello una mayor probabilidad de que no sea leída ni pueda ser asimilada. En consecuencia, es preciso pensar en otros mecanismos para asegurar la protección del afectado, sin renunciar al deber de los responsables de ser transparentes en el tratamiento de los datos que lleven a cabo.

[25] Quizá la crítica más mordaz al elenco de ítems sobre los que debe informarse cabe atribuirla a Carrasco que califica dichos deberes de cáncer en el cuerpo del derecho de consumo. (A. Carrasco Perera, *Desarrollos futuros del derecho de consumo en España, en el horizonte de la transposición de la Directiva de derechos de los consumidores*, en S. Cámara Lapuente (dir.) y E. Arroyo Amayuelas, (coord.), *La Revisión de las normas europeas y nacionales de protección de los consumidores: más allá de la directiva sobre derechos de los consumidores y del Instrumento Opcional sobre un derecho europeo de la compraventa de octubre de 2011*, Civitas, 2012, 311-334, 314).

Por otro lado el exceso de información puede producir lo que se conoce como *fatiga informativa*. Así se pronuncia el Grupo del art. 29, WP 260 rev. 01, cit., § 8 y § 35.

Bibliografía

S. Cámara Lapuente, *Comentario al artículo 60 TRLCU*, en S. Cámara Lapuente (dir.), *Comentarios a las Normas de Protección de los Consumidores. Texto refundido (RDL 1/2007) y otras leyes y reglamentos vigentes en España y en la Unión Europea*, Madrid, Colex, 2011, 484-510.

A. Carrasco Perera, *Desarrollos futuros del derecho de consumo en España, en el horizonte de la transposición de la Directiva de derechos de los consumidores*, en S. Cámara Lapuente (dir.) y E. Arroyo Amayuelas (coord.), *La Revisión de las normas europeas y nacionales de protección de los consumidores: más allá de la directiva sobre derechos de los consumidores y del Instrumento Opcional sobre un derecho europeo de la compraventa de octubre de 2011*, Civitas, 2012, 311-334.

P. Grimalt Servera, *La formación del contrato celebrado por medios electrónicos*, en M.A. Parra Lucán (dir.) *Negociación y perfección de los contratos*, 1ª ed., Thomson Reuters, Aranzadi, Cizur Menor, 2014, 355-392.

Grupo del art. 29, WP 259 rev.01, *Guidelines on consent under Regulation 2016/679*, adoptadas el 28 de noviembre de 2017, revisadas y adoptadas el 10 de abril de 2018.

Grupo del art. 29, WP 260 rev.01, *Guidelines on transparency under Regulation 2016/679*, adoptadas el 29 de noviembre de 2017, revisadas y adoptadas el 11 de abril de 2018.

L. Kugler, *The War Over the Value of Personal Data*, Communications of the ACM, february 2018, vol. 61, n. 2, 17-19, disponible en:

https://cacm.acm.org/magazines/2018/2/224626-the-war-over-the-value-of-personal-data/fulltext

M.R. Llácer Matacás, *La autorización al tratamiento de información personal en la contratación de bienes y servicios*, Dykinson, Madrid, 2012.

G. Malgieri-B. Custers, *Pricing privacy - the right to know the value of your personal data*, en *Computer Law & Security Review*, vol. 34, Issue 2, 2018, 289-303. Disponible en: *https://doi.org/10.1016/j.clsr.2017.08.006*. *http://www.sciencedirect.com/science/article/pii/S0267364917302819*

M.J. Marín López, *El "nuevo" concepto de consumidor y empresario tras la Ley 3/2014, de reforma del TRLGDCU*, en *Revista CESCO de Derecho de Consumo*, nº 9, 2014, 9-16. ISSN-e 2254-2582.

M.J. Marín López, *La formación del contrato con consumidores*, en M.A. Parra Lucán (dir.), *Negociación y perfección de los contratos*, 1ª ed., Thomson Reuters, Aranzadi, Cizur Menor, 2014, 789- 848.

L.M. Miranda Serrano, *La protección del consumidor como ariete de la reforma del viejo Derecho privado; en especial, en la fase previa a la contratación de bienes y servicios*, en L.M. Miranda Serrano-J. Pagador López-M. Pino Abad (coord.), *La protección de los consumidores en tiempos de cambio*, Iustel, 1ª ed., Madrid, 2015, 37-64.

S. Wachter-B. Mittelstadt-L. Floridi, *Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation*, *International Data Privacy Law*, 2017. Disponible en SSRN: *https://ssrn.com/abstract=2903469* or *http://dx.doi.org/10.2139/ssrn.2903469*

J. Zittrain, *http://blogs.law.harvard.edu/futureoftheinternet/2012/03/21/meme-patrol-when-something-online-is-free-youre-not-the-customer-youre-the-product/*

Libertad de expresión y derechos digitales en el proyecto de Ley Orgánica de Protección de Datos en España*

Cristina Pauner Chulvi

Sommario: 1. Introducción: el conflicto entre libertad de expresión y privacidad – 2. El tratamiento de la libertad de expresión en el Reglamento General de Protección de Datos. Comparativa con la Directiva 95/46 – 3. La adaptación de la ley española al RGPD: la nueva Carta de Derechos Digitales en el proyecto de LOPD – 4. Referencias a la libertad de expresión en la Carta de Derechos Digitales: la problemàtica de las noticias falsas

I. Introducción: el conflicto entre libertad de expresión y privacidad

En el mundo de la comunicación existe una idea conocida por todos y es la relación de tensión que la libertad de expresión e información mantiene con el derecho a la protección de datos porque

* Este artículo reproduce la conferencia impartida en el Iº Encuentro de Estudio Italo-Español en materia de protección de los datos personales sobre "La entrada en vigor del Reglamento (UE) 2016/679: la reforma a la prueba de la praxis en Italia y España", celebrado en Pisa los días 8 y 9 de mayo de 2018. Quisiera agradecer la invitación que me cursaron a los profesores Dianora Poletti (Università de Pisa) y Alessandro Mantelero (Politecnico di Torino) y felicitarles por la excelente organización del encuentro.
En el momento de publicarse este artículo ya se ha aprobado en España la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (BOE núm. 294, de 6 de diciembre.)

precisamente la publicación de información consiste en la puesta a disposición del público de gran cantidad de datos que pueden incidir en derechos de los ciudadanos tales como su privacidad. Así, se afirma que los datos son la savia de la información.

En contraste con este derecho a la privacidad, como instancia fundamental de la libertad de expresión, el periodismo trata de recopilar, organizar y difundir una gran variedad de información a un público amplio y sin restricciones. Esta afirmación es sistemáticamente reproducida y avalada por la jurisprudencia europea que mantiene que «la difusión de eventos puede influir sobre la privacidad de la persona y el daño puede aumentar cuando (la difusión) se realiza a través de un medio social» (SSTEDH caso *Von Hannover c. Alemania*, caso *Mosley c. Reino Unido*).

Por ello, el régimen europeo de protección de datos y la libertad de expresión e información coexisten en un estado de permanente tensión[1]. A esta tensión hay que añadir, como afirma el Tribunal Europeo de Justicia en su sentencia C 131/12, de 13 de mayo de 2014, *Google Spain*, que la accesibilidad a cualquier otro dato personal en Internet es también publicación, pero además esa publicación tiene tal efecto multiplicador y diseminador que se llega a perder el control sobre los contenidos (parágrafos 63 y 84).

Con carácter general, la jurisprudencia europea ha defendido la posición prevalente de las libertades de la comunicación siempre que se trate de información veraz y de interés público en base al papel de "perro guardián de la democracia" que corresponde a los medios de comunicación (SSTEDH caso *Sunday Times c. Reino Unido*, caso *Jersild c. Dinamarca*).

Pero ambos derechos pueden coexistir en equilibrio y esto es precisamente lo que se refleja en las normas de protección de datos. Este equilibrio se ha logrado reconociendo una serie de exenciones o excepciones a la aplicación de la normativa sobre protección de datos y las dos más conocidas son, precisamente, la excepción periodística que se aplica a los medios de comunicación y les exime de la observancia de ciertos principios y reglas contenidas en las normas

[1] M. Arenas Ramiro, *El derecho a la protección de datos personales como garantía de las libertades de expresión e información*, en *Libertad en internet: la red y las libertades de expresión e información*, coord. L. Cotino, 2007, 355-386.

sobre protección de datos cuando el tratamiento de los mismos se realiza por un medio de comunicación y la excepción doméstica que puede aplicarse a los usos que algunos ciudadanos hacen de datos personales y gracias a la cual no les resulta de aplicación la normativa sobre protección de datos.

2. Libertad de expresión en el Reglamento General de Protección de Datos. Comparativa con la Directiva 95/46

El nuevo Reglamento (UE) 2016/679 se refiere explícitamente a la libertad de expresión e información en diversos preceptos: en el Considerando 4 donde proclama la inexistencia de derechos absolutos; en el Considerando 153 en el que determina el deber de conciliar las normas que regulan la libertad de expresión e información con el derecho a la protección de datos; en el artículo 17 que reconoce el novedosos derecho a la supresión o derecho al olvido[2] y en el artículo 85 que se refiere al tratamiento (de datos) y la libertad de expresión e información estableciendo la llamada "excepción periodística".

Esta figura ya se encontraba reconocida en el artículo 9 de la Directiva 96/45/CE aunque, a pesar de que el precepto se diseñó con el loable propósito de alcanzar un equilibrio obligatorio entre los derechos e intereses de protección de datos y el interés público en la libertad de expresión, la doctrina[3] había señalado una serie de fallos significativos en su regulación.

1. En primer lugar, el mencionado precepto **ha sido traspuesto en la legislación de los Estados miembros de forma muy diversa y no se ha alcanzado el objetivo de garantizar el libre flujo de información en el mercado interior europeo.** Advertimos que en algunos países no se prevé ninguna excepción formal para el ejercicio de la libertad de expresión e información en los medios frente a los requisitos exigidos por la normativa sobre protección de datos mientras que en

[2] A. Rallo Lombarte, *El derecho al olvido en Internet: Google versus España*, Madrid, CEPC, 2014.

[3] D. Erdos, *European Data Protection and Media Expression: Fundamentally Off Balance*, in *International and Comparative Law Quarterly*, vol. 65, 1, 2016, 139-183.

otros casos la expresión periodística se beneficia de una casi absoluta exención de aquellas exigencias pasando por países que aprovechan códigos deontológicos para encontrar un equilibrio entre las exigencias de protección de datos y la libertad de expresión e información

La fragmentación de la normativa de protección de datos y la falta de armonización en la aplicación de estas normas causa no pocos problemas a los medios de comunicación, muy especialmente, en el contexto actual con la expansión generalizada de los nuevos medios digitales y su difusión transfronteriza enfrentándolos a situaciones de inseguridad jurídica puesto que lo que no está admitido por la legislación sobre protección de datos de un país en relación con la recogida, almacenamiento y difusión de datos de carácter personal con fines periodísticos puede ser perfectamente legal en otro y a la inversa.

2. El artículo 9 solo proporciona una excepción para el tratamiento de datos para fines **«exclusivamente» periodísticos**. Se denuncia que este enfoque es demasiado restrictivo porque reduce los sujetos que se pueden beneficiar de la excepción, esto es, tan solo periodistas, artistas o escritores. En contraste, el artículo 10 CEDH así como el artículo 11 CDFUE garantizan a *toda* persona el derecho a la libertad de expresión e información.

Debe reconocerse que, con la aparición de las nuevas tecnologías, el periodismo profesional coexiste en la actualidad con muchos otros tipos de procesamiento de la información (p. ej. periodismo ciudadano, nuevas plataformas para blogs, etc.). Por ello, se ha denunciado que el artículo 9 tal y como está actualmente diseñado no cubre manifestaciones claras del derecho a la información que deberían beneficiarse de la excepción.

Frente a esta problemática que la regulación contenida en el artículo 85 RGPD (y su correlativo Considerando 153) supone un avance ya que trata de corregir algunas de las deficiencias señaladas del anterior artículo 9 de la Directiva.

En primer lugar, por el cambio de naturaleza de la norma. Tratándose de una normativa directamente aplicable reducirá el riesgo de fragmentación derivado del acto de trasposición de las Directivas y permitirá un mayor grado de armonización en el contexto europeo.

En segundo término, el texto final del artículo 85 RGPD se benefició de una mejora sustancial durante su tramitación en las instancias europeas dando lugar a un texto mucho más abierto y prepa-

rado para afrontar algunos de los retos que plantea actualmente la comunicación en el entorno digital. Concretamente,

El **apartado 1)** amplia el alcance de la excepción para permitir, y exigir, a los Estados miembros que realicen una ponderación general (equilibrio) entre protección de datos y libertad de expresión. Esta reformulación puede decirse que ha transformado la excepción para fines específicos en una cláusula de aplicación general. Consideramos además muy positiva este margen de apreciación nacional habida cuenta de las notables diferencias que existen entre los países a la hora de definir el contenido y alcance de la libertad de expresión y sus límites a pesar de que todos los Estados miembros suscriben unos principios básicos comunes. Este «margen de apreciación» aceptado por el TEDH se ha reconocido como discrecionalidad de los Estados por el TJUE, entre otros, en el caso Linqvist.

El **apartado 2)** clarifica el alcance de la expresión "periodismo".

En primer lugar, se ha eliminado del texto del artículo la expresión "exclusivamente" que perjudicaba a aquellas actividades informativas en las que había también otro fin unido al de transmitir información.

En segundo lugar, remite al artículo 11 CDFUE que reconoce la libertad de expresión, opinión y la libertad de recibir o de comunicar informaciones o ideas,

Finalmente, incluye la pauta de que, en atención a la importancia del derecho a la libertad de expresión en toda sociedad democrática, los conceptos relativos a la libertad de expresión deben ser interpretados en sentido amplio y pretende reconocer actividades como el *blogging* y la expresión de opiniones en las redes sociales.

La excepción periodística no se consagra como privilegio de los medios de comunicación y el Reglamento descarta que tenga que tratarse de «empresas de comunicación» lo que, unido a la aceptación de la comunicación *online*, pone el acento no tanto en el sujeto – particulares o medios de comunicación – como en la finalidad de los tratamientos.

Finalmente, el **apartado 3)** obliga a los Estados miembros a notificar las disposiciones adoptadas para establecer las exenciones y, sin dilación, cualquier modificación posterior de las mismas.

Así, el artículo 85 RGPD permite que los Estados miembros establezcan excepciones que suspenden la aplicación de sus previsiones a la actividad periodística. En concreto, este precepto declara inaplicables los siguientes principios:

1) el *principio de calidad* de los datos que supone que los datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley;

2) *reglas de transparencia* que incluyen la obligación de suministrar información al interesado en el momento de recabar sus datos así como cuando los datos se obtienen de terceras personas y el derecho de acceso a los datos del interesado cuando lo solicite;

3) *normas sobre categorías especiales de datos* en las que se incluyen aquellos datos que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como datos relativos a la salud o a la sexualidad.

Es fácilmente comprensible que el cumplimiento de estas obligaciones puede entrañar importantes restricciones al ejercicio de las libertades de expresión e información de los medios. Baste pensar en las implicaciones que la prohibición de tratamiento y **difusión de datos sensibles** supondrían para los medios que, entre otros pero muy mayoritariamente, cubren asuntos relacionados con información criminal o con opiniones políticas, por ejemplo. O las consecuencias que la **obligación de informar a los interesados** generaría para el periodismo de investigación o para las fuentes de información de los periodistas. Tampoco parece posible facilitar el **derecho de acceso a y la rectificación** de los datos personales durante la elaboración y redacción de la noticia y previamente a su publicación puesto que esto podría limitar gravemente la libertad de expresión. Finalmente, puede pensarse en lo inapropiada que resulta la **prohibición de transferencia de datos a terceros países** que no aseguren un nivel de protección adecuado para las actuales publicaciones electrónicas y versiones digitales de los medios de comunicación – periódicos, canales de televisión, emisoras de radio – y para los comunicadores *online* que gozan de difusión global.

Además, en el Reglamento se incluyen las conocidas como "cláusulas abiertas"[4] que permiten a un Estado miembro modificar las condiciones que determina el Reglamento, esto es, introducir una regulación más restrictiva del RGPD en su ley nacional de protección

[4] Alrededor de un 30% de los artículos del GDPR contienen *opening clauses* (más de 50 artículos).

de datos (por ejemplo, edad mínima para otorgar el consentimiento, poderes de la autoridad nacional de control, tratamiento de datos en el ámbito laboral, sobre ciertas categorías de datos sensibles incluyendo datos de salud, tratamiento de datos personales con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, obligación de secreto, sanciones a determinadas conductas, etc.).

3. La adaptación de la ley española al RGPD: la nueva Carta de Derechos Digitales en el proyecto de LOPD

En España, la principal norma que regula la protección de datos es la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos y no reconoce la excepción periodística como tampoco lo hace el proyecto LOPD, actualmente ya aprobada, a pesar de ser una cláusula abierta en el RGPD que permite que cada Estado miembro module el alcance de la misma. Es esperable que se sigan aplicando las pautas que la AEPD y la jurisprudencia ha mantenido hasta el momento (la información puede publicarse si la información es veraz, de relevancia pública y el dato necesario para la comprensión de la noticia).

En relación con este proyecto de LOPD, España inició en febrero de 2018, a 4 meses de la aplicación del RGPD, el primer debate del proyecto en el Parlamento.

España es un país en el que la cultura de protección de los datos tiene arraigo y se parte de un conocimiento efectivo de la normativa gracias a las normas publicadas desde 1992. La Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de Datos de carácter personal (LORTAD), la citada Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal (LOPD), el Real Decreto 994/1999 Reglamento de Medidas de Seguridad de los ficheros automatizados (RSM) y el Reglamento de desarrollo, Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba la LOPD (RLOPD) son el conjunto de leyes que han desarrollado el artículo 18.4 de la Constitución española de 1978 que establece que «la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y

el pleno ejercicio de sus derechos». Estas normas han consolidado las bases de un jurídico e institucional desarrollado y eficaz para la protección de datos en España.

Actualmente, el proyecto de Ley de modificación de LOPD está tramitándose en el Parlamento español y existe un acuerdo generalizado entre los principales grupos políticos para priorizar el proyecto y, a pesar del tiempo perdido, se confía en recibir la aprobación definitiva en septiembre-octubre de 2018. Posteriormente, se procederá a su publicación en el BOE y su inmediata entrada en vigor.

Una de las enmiendas más destacadas al proyecto de LOPD ha sido presentada por el grupo socialista que quiere transformar la ley en una norma de garantías digitales. Para ello la propuesta, impulsada por el diputado Artemi Rallo, exdirector de la Agencia de Protección de Datos, propone la adición de un nuevo Título X *Garantía de los derechos digitales* con 18 artículos (79 a 97, numeración definitiva) que refuerzan los derechos digitales de la ciudadanía y amplía a Internet la exigencia y aplicación de los derechos y libertades reconocidos por la Constitución y los Tratados Internacionales.

La propuesta toma ejemplo de normativa similar aprobada en países de nuestro entorno que bien en legislaciones específicas, bien normas sectoriales, bien en cartas de naturaleza declarativa han reconocido algunos de estos derechos. Entre otros ejemplos, la Ley para una República digital promulgada en Francia el 7 de octubre de 2016[5], el derecho a la desconexión laboral introducido en el Código de Trabajo francés[6] o la Declaración italiana de Derechos en Internet[7]. En la Exposición de motivos de la propuesta socialista se explica que, a falta de una deseable reforma de la Constitución que reconozca una nueva generación de derechos digitales, es necesario que el le-

[5] *Loi n° 2016-1321, du 7 octobre 2016, pour une République numérique* (https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000033202746&dateTexte=&categorieLien=id).

[6] Con efectos desde el uno de enero de 2017, el artículo 55.I.2 de la *Loi 2016-1088, du 8 août 2016 relative au travail, à la modernisation du dialogue social et à la sécurisation des parcours professionnels*, introduce un nuevo apartado 7 en el artículo L. 2242-8 del Código de Trabajo francés dentro del Capítulo II "Adaptación del derecho laboral a la era digital".

[7] http://www.camera.it/application/xmanager/projects/leg17/attachments/upload_file/upload_files/000/000/187/dichiarazione_dei_diritti_internet_pubblicata.pdf

gislador aborde el reconocimiento de un sistema de garantía de los derechos digitales de manera integral y unificada[8].

La enmienda plantea las siguientes medidas:

1. Derecho a la **neutralidad de Internet** en la medida que los proveedores de servicios de internet deben procurar una oferta transparente de servicios sin discriminación técnica o económica.

2. Derecho de **acceso universal a Internet** con carácter universal, asequible, de calidad y no discriminatorio.

3. Derecho a la **educación digital** garantizado al alumnado mediante el aprendizaje de un uso seguro de los medios digitales y la formación del profesorado.

4. Derecho a la **seguridad digital** que implica la garantía de la privacidad y seguridad de las comunicaciones que circulan en Internet a partir de la información a los usuarios y el establecimiento de sistemas de denuncia sencillos.

5. Derecho al **olvido** que postula que los datos personales sean cancelados "cuando, con el tiempo, puedan devenir inadecuados, no pertinentes o excesivos en relación con los fines para los que se recogieron". En esos supuestos, el gestor de un motor de búsqueda estaría obligado a eliminar de la lista de resultados los vínculos a páginas. También, a petición del interesado, se suprimirían datos personales facilitados por menores de edad.

6. Derecho de **portabilidad** que permite a las personas recibir y transmitir los datos que haya proporcionado en redes sociales y servicios de la sociedad de la información equivalentes.

7. Derecho a la **intimidad y uso de dispositivos digitales en el ámbito laboral** que protege a los trabajadores y empleados públicos de invasiones en su intimidad a través de los dispositivos digitales que le facilita la empresa.

8. Derecho a la **desconexión digital** de los trabajadores para garantizar el respeto de descanso y vacaciones así como de su intimi-

[8] Brasil cuenta con una propuesta similar: el Marco Civil de Internet que introduce el respeto a los derechos civiles en el uso de Internet en Brasil incorporando los derechos de neutralidad de la red, limitación de responsabilidad para los intermediarios, libertad de expresión y garantías de privacidad de los usuarios de internet (Ley nº 12.965, de 23 de abril de 2014, *http://participacao.mj.gov.br/marcocivil/sistematizacao/*).

dad personal y familiar. Para ello, la empresa elaborará una política interna en la que definirá las modalidades de ejercicio del derecho a la desconexión en atención a la naturaleza y objeto de la relación laboral y concretará acciones de formación y sensibilización sobre un uso razonable de dispositivos digitales evitando el riesgo de fatiga informática.

9. Derecho a la **intimidad ante la utilización de sistemas audiovisuales o de geolocalización en el ámbito laboral** que regula el tratamiento de los datos obtenidos por los empleadores a través de sistemas de videovigilancia o geolocalización exclusivamente para funciones de control laboral y previa información a los trabajadores acerca de su existencia y de sus derechos de acceso, rectificación y cancelación de datos.

10. **Derechos digitales en la negociación colectiva** que reconoce la posibilidad de que los Convenios colectivos establezcan protecciones adicionales, más específicas y garantías de derechos y libertades en el tratamiento de datos personales de los trabajadores.

11. **Protección de los menores en Internet** que impulsa una serie de medidas que garantizan los derechos del menor y contemplan el impacto de Internet en los derechos de los menores con el objeto de promover garantías de su seguridad e integridad.

12. **Libertad de expresión** de todos los usuarios en Internet garantizando la veracidad informativa a través de la adopción y ejecución de "protocolos efectivos" para que los responsables de las redes sociales, plataformas digitales y servicios similares, en caso de detectarse, eliminen «contenidos que atenten contra el derecho constitucional a comunicar o recibir libremente información veraz por cualquier medio de comunicaciónz»[9]. Asimismo, se reclaman garantías para el derecho al honor y a la imagen en las redes sociales, plataformas digitales y servicios equivalentes de la sociedad de la información, e insta a que los responsables de esos servicios estén obligados a adoptar los protocolos necesarios para "preservar la dignidad humana" y "garantizar la identificación de los usuarios que los vulneren".

13. Derecho al **testamento digital** que permitirá a las personas vinculadas a la persona fallecida o sus herederos acceder a los da-

[9] A. Rallo Lombarte-R. Martínez, *Derecho y Redes sociales*, Pamplona, Thomson Reuters, 2013, 2ª ed.

tos del fallecido e impartir instrucciones sobre su utilización, destino o supresión.

4. Referencias a la libertad de expresión en la Carta de Derechos Digitales: la problemática de las noticias falsas

Del catálogo de derechos enumerados en la Carta, hay dos que inciden directamente en el ejercicio de las libertades comunicativas: el derecho al olvido (artículo 93 y 94, numeración definitiva), al que no me referiré en profundidad en estas líneas puesto que ha sido objeto de discusión en otras intervenciones, y el reconocimiento de la libertad de expresión de todos los usuarios de Internet (artículo 86).

En la regulación de las libertades comunicativas en el entorno digital,[10] el mencionado artículo 86 se centra en el deber de ofrecer una información exacta y veraz.

Así, en primer lugar, garantiza la libertad de expresión de todos los usuarios de Internet la exactitud y veracidad de la información y el respeto al derecho al honor y la propia imagen mediante la adopción de protocolos necesarios para preservar la dignidad humana y garantizar la identificación de los usuarios que los vulneren.

En segundo término, exige los datos publicados en los nuevos soportes digitales sean exactos y actualizados y establece una obligación de *aggiornamento* de las noticias. En concreto, obliga a los medios de comunicación digitales a admitir, a petición del interesado, la publicación en sus archivos digitales de un aviso aclaratorio sobre noticias que le conciernan y cuya noticia original no refleje la situación actual del individuo causándoles perjuicio. En particular, procederá la inclusión de dicho aviso cuando las informaciones se refieran a actuaciones policiales o judiciales que hayan sido revocadas por decisiones posteriores.

[10] Sobre el cambio en el proceso de elaboración de la información, puede verse J. De Miguel Bárcena, *Las transformaciones del derecho a la información en el contexto del ciberperiodismo*, en *Revista de Estudios Políticos*, n. 173, 2016, 141-168 y G. Brock, *Out of Print: Newspapers, Journalism and the Business of News in the Digital Age*, Philadelphia, PA, and London, UK, Kogan Page, 2013.

Finalmente, aborda el importante problema de las noticias falsas o *fake news* y determina que los responsables de redes sociales de Internet garantizarán la veracidad informativa[11]. A tal fin, se adoptarán y ejecutarán protocolos efectivos de eliminación de los contenidos que atenten contra el derecho constitucional a comunicar o recibir libremente información veraz por cualquier medio de comunicación.

El proyecto de LOPD[12] hace responsables a las redes sociales de esta obligación de control de la información que ayudan a difundir ya que el análisis del fenómeno de la difusión de noticias falsas debe partir de la identificación de dos sujetos que intervienen en su propagación. En primer lugar, las plataformas o sitios web que crean esas noticias falsas y, en segundo término, las redes sociales que contribuyen a su difusión viral. Por lo que se refiere a los sitios web, gran cantidad de noticias falsas son originariamente fabricadas por *spammers* que pretenden engañar a los usuarios de la Red y lucrarse de ingresos publicitarios por cada clic que hagan esos usuarios. Se trata de falsos periódicos o páginas con apariencia informativa que actúan deliberadamente cuando publican bulos o propaganda pretendiendo ser noticias reales. En una segunda fase, la viralización de esas noticias falsas se produce a través de las redes sociales como Facebook o Twitter en lo que se ha venido a bautizar como "cascada informativa"[13]. Así, en la actualidad, el control sobre la distribución de las noticias ya no está en manos de los medios de comunicación sino de las redes sociales que son las que las seleccionan y filtran las informaciones mediante algoritmos y plataformas que son complejas, opacas e impredecibles.

[11] Sobre esta cuestión, véase entre otros C. Pauner Chulvi, *Noticias falsas y libertad de expresión e información. El control de los contenidos informativos en la red*, en *Teoría y Realidad Constitucional*, n. 41, 2018, 297-331.

[12] Muchos países europeos han optado por legislar en contra de las noticias falsas: Francia, Italia o Alemania ya cuentan con leyes para luchar contra la proliferación de las *fake news*. La Comisión Europea presentó el informe del Grupo de Expertos (High-Level-Group) de estudio contra la desinformación, *A multidimensional approach to disinformation – Report of the independent High level Group on fake news and online disinformation*, marzo de 2018.

[13] S. Vosoughe-D. Roy-S.Aral, *The spread of true and false news online*, en *Science*, n. 359, 2018, 1146–1151. *http://science.sciencemag.org/content/sci/359/6380/1146.full.pdf*

Las soluciones propuestas para la lucha contra las noticias falsas se articulan en torno a tres acciones: la acción de verificación humana a través de equipos de *fact-checking*, la solución colaborativa que permite a los usuarios denunciar contenidos que consideran inexactos mediante el etiquetado de las noticias que las califica según su criterio, y la solución algorítmica mediante fórmulas que modifican los algoritmos de selección de noticias de forma que otorguen mayor peso a las páginas consideradas más fiables y hagan menos visibles los contenidos de baja credibilidad.

La doctrina[14] ha señalado que la eficacia de esta propuesta es limitada y hay que ser conscientes de que un algoritmo, por definición, nunca va a ser capaz de distinguir lo verdadero de lo falso y que no es posible diseñar un "algoritmo de la verdad" aunque puede resultar un instrumento útil si ayuda, por ejemplo, a valorar la calidad de las páginas web de las que surge la noticia en función de la veracidad de los datos que contiene, destacando aquellos datos de las noticias que el usuario ha de contrastar para formarse una opinión o señalando las noticias falsas y contextualizándolas.

[14] J.C. Fondevilla Gascón, *Algoritmos sobre el impacto de los medios de comunicación en medios sociales: estado de la cuestión*, en *Icono 14*, vol. 15, 1, 2017, 21-41.

Profili del contesto europeo

La responsabilità civile per il trattamento illecito dei dati personali*

Salvatore Sica

Sommario: 1. La continuità di fondo tra la direttiva 95/46/CE e il Regolamento UE 2016/679 – 2. Le tappe dell'evoluzione normativa in tema di responsabilità civile per il trattamento illecito dei dati personali – 3. Considerazioni sul modello di responsabilità vigente

1. La continuità di fondo tra la direttiva 95/46/CE e il Regolamento UE 2016/679

Il tema, di per sé già stimolante, della responsabilità civile da trattamento illecito dei dati personali risulta di ulteriore interesse se riguardato in relazione al recente mutato quadro legislativo di derivazione europea. In effetti, più che interrogarsi sul solo impatto prodotto dal Regolamento 2016/679/UE[1] – meglio noto come GDPR – e dal decreto legislativo di attuazione[2]

* Il presente contributo riproduce, con integrazione di note e delle modifiche apportate dal d.lgs. n. 101/2018 di adeguamento dell'ordinamento italiano al GDPR, la relazione svolta in occasione del convegno *L'entrata in vigore del Regolamento (UE) 2016/679: la riforma alla prova della prassi in Italia e in Spagna*, tenutosi a Pisa nei giorni 8-9 giugno 2018.

[1] Pubblicato in GUUE del 4 maggio 2016, L 119, entrato in vigore il 24 maggio 2016, con applicazione diretta agli Stati membri dal 25 maggio 2018.

[2] Decreto legislativo 10 agosto 2018, n. 101, recante *Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione*

(d.lgs. n. 101/2018), pare opportuno vagliare, in via preliminare, se la filosofia che emerge dal GDPR presenti un qualche mutamento rispetto alla *policy* che è sottesa alla nota direttiva 95/46/CE[3], nonché ai successivi provvedimenti europei e nazionali in materia di protezione dei dati personali[4].

In effetti tale approccio, rivolto innanzitutto agli obiettivi di politica legislativa, è ineludibile, a meno che non si vogliano considerare le regole di responsabilità civile come mere norme rimediali rispetto al danno, dunque rilevanti esclusivamente in ordine alla patologia conseguente alla violazione dei precetti. Al contrario, si è convinti che la stessa struttura della responsabilità civile sia sempre emanazione della sua *funzione*[5]. Quest'ultima, dal canto suo, non può che essere diretta espressione della filosofia che il legislatore per quel determinato ambito ha inteso seguire. Gli esempi che potrebbero farsi sono così numerosi da essere persino superflui.

Basti por mente al *corpus* degli artt. 2048-2054 cod. civ. Come noto, tali norme nascono come statuti di responsabilità "speciali", ma, in seguito, nel formante giurisprudenziale, hanno ricevuto nuova linfa, *vivendo* come regole di responsabilità con funzioni molte-

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 (regolamento generale sulla protezione dei dati), pubblicato in GU del 4 settembre 2018, n. 205. Tra i primi commenti a questa normativa si segnala quello di V. Cuffaro, *Quel che resta di un codice: il d.lgs. 10 agosto 2018, n. 101 detta le disposizioni di adeguamento del codice della privacy al Regolamento sulla protezione dei dati*, in *Corr. giur.*, 2018, 1181 ss.

[3] Pubblicata in GUCE del 23 novembre 1995, L 281.

[4] Per un'attenta ricostruzione, si rinvia a: S. Sica-V. D'Antonio-G.M. Riccio (a cura di), *La nuova disciplina europea della privacy*, Padova, Cedam, 2016, *passim*; F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali*, Torino, Giappichelli, 2016, *passim*. Si rinvia altresì a: V. Cardarelli-S. Sica-V. Zeno-Zencovich (a cura di), *Il codice dei dati personali. Temi e problemi*, Milano, Giuffrè, 2004; S. Sica-P. Stanzione (a cura di), *La nuova disciplina della privacy*, Bologna, Zanichelli, 2005; C.M. Bianca-F.D. Busnelli (a cura di), *La protezione dei dati personali*, Padova, Cedam, 2007; R. Pardolesi (a cura di), *Diritto alla riservatezza e protezione dei dati personali*, Milano, Giuffrè, 2003; V. Cuffaro-V. Ricciuto-V. Zeno-Zencovich (a cura di), *Trattamento dei dati e tutela della persona*, Milano, Giuffrè, 1998.

[5] Sul punto sia consentito il rinvio a S. Sica, *La responsabilità civile tra struttura, funzione e "valori"*, in *Resp. civ. prev.*, 1994, 543 ss.; Id., *Note in tema di sistema e funzione della regola aquiliana*, in *Danno e resp.*, 911 ss.

plici, tutt'altro che settoriali e di certo non riducibili a mere norme di inversione dell'onere probatorio[6].

Se si asseconda la proposta ricostruttiva che muove dalla filosofia del legislatore europeo, pare potersi affermare che le nuove regole per la protezione dei dati personali non mutino la prospettiva di fondo del precedente impianto: l'intera costruzione del Regolamento 2016/679/UE, continua infatti a rimanere basata sul principio del consenso informato, proprio come negli impianti normativi ad essa precedenti.

Non possono che valere allora le perplessità già espresse da autorevole dottrina rispetto alla idoneità di tale principio a rispondere ai bisogni di tutela di cui sono portatori gli interessati. In proposito, non è senza significato ricordare quanto già sottolineava nel 1997 Guido Calabresi, il quale, in occasione di un convegno promosso dall'Osservatorio Giordano Dell'Amore di Stresa[7], a ridosso dell'entrata in vigore della legge n. 675/1996, rimarcava che solo in apparenza la più efficiente delle regole è quella del consenso informato; tuttavia, come dimostrano le sue applicazioni nella materia dei trattamenti sanitari, nei casi concreti esso rivela di non essere il più affidabile dei modelli di riferimento, realizzando spesso una tutela meramente apparente[8].

[6] Per un approfondimento si vedano: S. Sica, *Circolazione stradale e responsabilità: l'esperienza francese e italiana*, Napoli, Edizioni Scientifiche Italiane, 1990; G.M. Riccio-G. Giannone Codiglione, *Responsabilità da attività pericolose*, in P. Stanzione (a cura di), *Trattato della responsabilità civile*, *Le responsabilità speciali*, Padova, Cedam, 2012, 549 ss. Nonché si rinvia, *ex multis*, ai contributi di: G. Gentile, *Responsabilità per l'esercizio di attività pericolose*, in *Resp. civ. prev.*, 1950, 101 ss.; E. Bonvicini, *La responsabilità civile per fatto altrui*, Milano, Giuffrè, 1976; A. De Cupis, *Dei fatti illec*iti, in *Comm. cod. civ. Scialoja e Branca*, Libro IV, Delle obbligazioni, artt. 2043-2059, Bologna-Roma, 1971; P. Trimarchi, *Rischio e responsabilità oggettiva*, Milano, Giuffrè, 1961; M. Comporti, *Esposizione al pericolo e responsabilità civi*le, Milano, Morano, 1965.

[7] Gli atti di questo convegno sono raccolti in Aa. Vv., *Società dell'informazione. Tutela della riservatezza*, Atti del Convegno di Stresa, 16-17 maggio 1997, presso l'Osservatorio Giordano Dell'Amore sui rapporti tra diritto ed economia, Milano, 1998.

[8] Da tempo – e non soltanto nell'ambito della protezione dei dati personali –, aumentano le perplessità rispetto alla convinzione secondo cui il consenso informato rappresenti la miglior forma di tutela per chi vede i propri interessi protetti incisi dall'altrui attività. V., ad esempio, R. Caterina, *Cyberspazio*,

L'architettura delle nuove norme di matrice europea rimane dunque basata sull'informativa, nonché sulla manifestazione del consenso. Tuttavia, non si tiene adeguatamente in considerazione che la fase dell'informativa il più delle volte risulta contraddistinta da un'asimmetria tra la capacità di cognizione del soggetto cui i dati si riferiscono e chi procede alla loro acquisizione, svuotandosi così quella tutela che il principio del consenso informato, in linea teorica, vuole apprestare.

Pur non negandosi che il Regolamento abbia apportato alcune innovazioni significative – si pensi, per tutte, al consenso del minore[9] –, oltre alla centralità del principio del consenso informato, pare potersi ravvisare un ulteriore elemento di continuità con il passato. Le norme del GDPR sottendono la convinzione, già alla base della direttiva 95/46/CE, dell'ineluttabilità della circolazione dei dati, vista l'impossibilità di bloccarne il flusso ininterrotto, a meno che non si voglia arrivare alla paralisi dell'economia di massa e dell'*Information and Communication Society*[10].

La stessa convinzione è in realtà sottesa anche alla direttiva 2000/31/CE[11] sul commercio elettronico, ove proprio per questo motivo si arrivò a privilegiare il modello dell'"irresponsabilità" del

social network e teoria generale del contratto, in *AIDA*, Milano, 2011, 96; S. Sica-G. Giannone Codiglione, *I social network sites e il "labirinto" della responsabilità*, in *Giur. merito*, 2012, 2714.

[9] V. art. 8, nonché il considerando 38; G. Spoto, *Disciplina del consenso e tutela del minore*, in S. Sica-V. D'Antonio-G.M. Riccio (a cura di), *La nuova disciplina*, cit., 111 ss.

[10] Come si evince chiaramente dal considerando n. 8: «La rapidità dell'evoluzione tecnologica e la globalizzazione comportano nuove sfide per la protezione dei dati personali. La portata della condivisione e della raccolta di dati personali è aumentata in modo significativo. La tecnologia attuale consente tanto alle imprese private quanto alle autorità pubbliche di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività. Sempre più spesso, le persone fisiche rendono disponibili al pubblico su scala mondiale informazioni personali che li riguardano. La tecnologia ha trasformato l'economia e le relazioni sociali e dovrebbe facilitare ancora di più la libera circolazione dei dati personali all'interno dell'Unione e il loro trasferimento verso paesi terzi e organizzazioni internazionali, garantendo al tempo stesso un elevato livello di protezione dei dati personali».

[11] Pubblicata in GUCE del 17 luglio 2000, L 178.

provider[12], di derivazione tedesca[13], mentre viceversa Francia e Inghilterra si orientavano per l'individuazione di forme di responsabilità per rischio d'impresa[14]. Alla base della scelta per il primo modello non vi fu altro che la constatazione di come questa fosse l'unica soluzione compatibile con il *Digital Millennium Copyright Act* del 1998, per evitare di estromettere dal mercato globale le imprese europee.

Alla luce di quanto riferito sulla diffusa convinzione dell'ineluttabilità della circolazione dei dati personali, acquistano ancora più rilevanza le norme del sistema sanzionatorio. Esse vengono ad essere l'unico contrappeso possibile a un fenomeno che non può conoscere divieti. Di conseguenza, si spiega quanto affermato in apertura circa l'impossibilità di ridurle a mere norme rimediali; in altre e più esplicite parole, se si muove dall'idea di fondo in base alla quale i dati *devono* circolare, ovvio che l'unico contrappeso possibile sia un sistema di tutela, a questo punto, postuma soltanto sul piano cronologico, ma parte piena di un disegno volto a bilanciare i diversi interessi, individuali e collettivi, in gioco.

Ciò appare ancora più significativo ove si considerino taluni profili di contesto generale, da non pretermettere per un'analisi seria e non "abbagliata" dai molteplici aspetti di disciplina di dettaglio. Si assiste infatti contestualmente ad un fenomeno senza precedenti costituito dalla concentrazione di potere in mano ai privati[15], dall'intensità tale da mettere quasi in discussione la dicotomia pubblico-privato nei termini tradizionali in cui è stata concepita e da

[12] Vedasi, per un approfondimento, S. Sica, *Commercio elettronico e categorie civilistiche*, Milano, Giuffrè, 2002.

[13] A partire dalla celebre *Volksahlungsurteil* (BVferG, 15 dicembre 1983 - 1 BvR 209/83, in *NVwZ*, 1984, 167).

[14] G.M. Riccio, *La responsabilità degli internet providers nel d.lgs. n. 70/03*, in *Danno e resp*., 2003, 1557.

[15] Sul tema della concentrazione di risorse informazionali in pochi soggetti privati, che arrivano a formare un oligopolio, si rinvia a: S. Sica-G. Giannone Codiglione, *La libertà fragile: pubblico e privato al tempo della rete*, Napoli, Edizioni Scientifiche Italiane, 2014; G. Giannone Codiglione, *Libertà d'impresa, concorrenza e neutralità della rete nel mercato transnazionale dei dati personali*, in *Dir. inf.*, 2015, 909 ss.; N.S. Kim-J. Telman, *Internet Giantsas Quasi-Governmental Actors and the Limits of ContractualConsent*, in *Mo. L. Rev.*, 2015, 80, 723.

imporre un adattamento della nota riflessione di Norberto Bobbio sul controllo dei controllori[16].

Di questo fenomeno il giurista è ben consapevole, già solo prendendo atto del dover fare i conti con un ambito contraddistinto, si è detto, da un'alluvione di *regole*, ma che allo stesso tempo rivela una carenza di *diritto*. La legislazione europea in generale, incluso il GDPR, muove nella logica della moltiplicazione della regola di dettaglio. In ciò può ravvisarsi un (ulteriore) indice dell'impotenza del diritto, inteso come sintesi di valori ed emanazione di una sfera pubblica, variamente fondata o condivisa, ma comunque *pubblica*, nel senso che sin dal diritto romano concepiamo.

2. Le tappe dell'evoluzione normativa in tema di responsabilità civile per il trattamento illecito dei dati personali

Le considerazioni finora svolte consentono di affermare che le nuove regole sul trattamento dei dati personali costituiscono la manifestazione di due fenomeni: da un lato vi è l'ineluttabilità della loro circolazione e, dall'altro, la progressiva perdita di capacità del diritto di governare i processi a dispetto della moltiplicazione delle regole di dettaglio. Rispetto a tutto ciò, occorre chiedersi se le regole di responsabilità siano idonee a far fronte ad un simile quadro. Al fine di comprendere questo, è necessario ripercorrere – seppure brevemente – la regolamentazione in materia, fino ad arrivare all'art. 82 del Regolamento 2016/679/UE.

La prima norma a venire in rilievo è l'art. 23 della direttiva 95/46/CE, che imponeva agli Stati membri di prevedere nelle loro legislazioni che chiunque subisse un danno cagionato da un trattamento illecito o da qualsiasi altro atto incompatibile con le disposizioni nazionali di attuazione della direttiva avesse il diritto di ottenere il risarcimento del pregiudizio subito dal responsabile del trattamento.

Tale disposizione presenta un esordio neutrale, quasi di principio, contenente un'affermazione di responsabilità, seguito dall'eccezione per cui il responsabile del trattamento può essere esonerato in

[16] N. Bobbio, *Il futuro della democrazia*, Torino, Einaudi, 1984.

tutto o in parte dalla stessa se prova che l'evento dannoso non gli è imputabile[17]. È quindi evidente la consapevolezza del legislatore europeo di muoversi sempre più dalla privacy alla *protection*[18].

La riferita affermazione di principio dell'art. 23 è stata declinata dal legislatore italiano nell'art. 18 della legge n. 675/1996[19], la quale, a parere di chi scrive, riprendendo le categorie già impiegate, può essere valutata come una legge di sistema ed emanazione di *diritto*, nonostante l'apparenza di "regola".

Ai sensi dell'art. 18, chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell´articolo 2050 cod. civ. La norma diede luogo a una riflessione dottrinaria intensa. Per la verità, più che la questione se, per effetto di questa norma, il trattamento dei dati personali diventasse un'attività pericolosa *in re ipsa*[20], è interessante analizzare le implicazioni

[17] Nel relativo considerando la prova della non imputabilità si faceva coincidere *segnatamente* nella dimostrazione *di un errore della persona interessata* o *di un caso di forza maggiore*, secondo un filone già presente nella produzione comunitaria.

[18] Nonostante nel linguaggio comune si assista ad una convergenza terminologica per i concetti di privacy e *data protection*, trattasi di due categorie distinte, che possono però intersecarsi. La prima tendenzialmente comprende la seconda, senza però esaurirsi in essa. La seconda, dal suo canto, opera anche quando non si sia realizzata una violazione della privacy. Non è allora un caso che la Carta dei diritti fondamentali dell'Unione europea tuteli la vita privata e familiare all'art. 7, mentre assicuri la protezione dei dati personali con l'art. 8. Sulla distinzione, v.: J. Kokott-C. Sobotta, *The Distinctionbetween Privacy and Data Protection in the Jurisprudence of the CJEU and the ECHR*, in *3 International Data Privacy Law*, 2013, 4, 222; F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, Torino, Giappichelli, 2016; G. Finocchiaro, *La giurisprudenza della Corte di Giustizia in materia di dati personali da Google Spain a Schrems*, in *Dir.inf.*, 2015, 779 ss.

[19] S. Sica, *Sub. art. 18*, in E. Giannantonio-M.G. Losano-V. Zeno-Zencovich (a cura di), *La tutela di dati personali. Commentario alla L. 675/96*, Padova, Cedam, 1999, 174 ss. Il tema del risarcimento dei danni da trattamento illecito dei dati è stato molto battuto dalla dottrina. In particolare e tra gli altri, si segnalano i seguenti contributi: D. Carusi, *La responsabilità*, in V. Cuffaro-V. Ricciuto (a cura di), *La disciplina del trattamento dei dati personali*, Torino, Giappichelli, 1997, 351; G. Comandè, *"Privacy" informatica: prospettive e problemi*, in *Danno e resp.*, 1997, 143.

[20] Sull'evoluzione della nozione di attività pericolosa, v.: P. Trimarchi, *Rischio*, cit., 43 ss.; S. Rodotà, *Il problema della responsabilità civile*, Milano, Giuffrè, 1964, 175 ss.; P.G. Monateri, *La responsabilità civile*, in *Tratt. dir. civ. Sacco*, Torino, 1998,

connesse alla circostanza che il legislatore avesse ritenuto preferibile il meccanismo dell'inversione dell'onere della prova e dell'esonero dalla responsabilità soltanto con la dimostrazione di aver adottato le misure idonee. Ciò pare ancora più interessante se si prende in considerazione un consolidato orientamento giurisprudenziale, di legittimità e di merito e che non ha subito arretramenti, secondo cui, se le misure fossero state idonee, il danno non si sarebbe affatto prodotto[21].

La norma in esame, in realtà, a ben riflettere, non pare condurre ad una responsabilità a base soggettiva, né a dimensione oggettiva *tout court*, perché, ancorché in via residuale, c'è la possibilità di andare esenti da responsabilità attraverso la dimostrazione di un fatto terzo con carattere di inevitabilità e di imprevedibilità, idoneo a interrompere il nesso causale. Si tratta, per la verità, della forma più avanzata di responsabilità civile, in grado di guardare alla fattispecie dalla prospettiva della vittima, che è esposta a un'attività socialmente pericolosa.

L'art. 18 presentava anche un altro grande merito. Esso, attraverso il richiamo al meccanismo dell'art. 2050 cod. civ., consentiva di prevenire tutti i dibattiti dottrinali e giurisprudenziali sulla qualificazione dell'attività come pericolosa o meno.

La prospettiva che si è tentato di mettere in evidenza risultava richiamata anche nell'art. 15 del d.lgs. 196/2003, abrogato dal d.lgs. 101/2018. Non soltanto il primo comma prevedeva che chiunque cagionasse danno ad altri per effetto del trattamento di dati personali fosse tenuto al risarcimento ai sensi dell'articolo 2050 cod. civ., ma il secondo comma arrivava ad ammettere esplicitamente la risarcibilità del danno non patrimoniale.

1011 ss.; M. Franzoni, *L'illecito*, Milano, Giuffrè, 2010, 400 ss.; G. Alpa, *La responsabilità civile. Parte generale*, Torino, Utet, 2010, 293 ss.

[21] Cass. 18 luglio 2011, n. 15733, in *Foro it.*, 2012, I, c. 1560: «In materia di responsabilità extracontrattuale, in ordine alla presunzione di responsabilità per chi esercita attività pericolose, il fatto del terzo o dello stesso danneggiato può avere effetto liberatorio solo quando abbia reso, per la sua sufficienza, giuridicamente irrilevante il fatto di chi esercita detta attività, ma non quando abbia semplicemente concorso nella produzione del danno per essersi inserito in una situazione già di per sé pericolosa, senza la quale l'evento non si sarebbe verificato, a causa dell'inidoneità delle misure preventive adottate».

Si trattava di una norma, al pari della precedente, adeguatamente esplicativa, rivelatrice del fatto che il legislatore può ancora essere efficacemente didascalico, se lo vuole[22]. Si imponeva al giudice di prendere come regime di riferimento quello contenuto all'art. 2050 cod. civ., dovendo questi poi applicarlo tenendo conto non soltanto del formante legislativo, ma che la norma è anche il risultato del formante giurisprudenziale. Vi è di più: per sgomberare il campo da qualsiasi dubbio, si esplicitava la risarcibilità del danno non patrimoniale. Non si trattava soltanto di indicazioni di contenuto, ma di una precisa *policy*, mirante ad assicurare una tutela rafforzata della vittima, muovendo dal presupposto che un'asimmetria di posizioni tra i soggetti coinvolti nel trattamento dei dati è inevitabile, ma non per questo la vittima può rimanere sprovvista di tutela.

Si consideri poi che la precisazione in ordine alla risarcibilità del danno non patrimoniale non era tanto necessaria rispetto all'evoluzione – in quegli anni era già in essere – circa il superamento di ogni barriera applicativa dell'art. 2059 cod. civ.[23], quanto piuttosto perché il legislatore era consapevole che il danno non patrimoniale è spesso l'unica voce di danno possibile, atteggiandosi, quindi, quasi a danno-sanzione rispetto alla violazione dei profili non patrimoniali del soggetto che vede non protetti i suoi dati personali.

A conferma di questa maggiore attenzione nei confronti di chi subisce la violazione, non sfugga, tra le altre cose, che l'art. 1 della legge n. 675/1996[24] risultava profondamente superato dal d.lgs. n. 196/2003.

[22] Un'operazione analoga è stata compiuta dal legislatore all'art. 7 della c.d. legge Gelli-Bianco, ove la norma prevede che al medico dipendente ospedaliero si applichi l'art. 2043 cod. civ., indicando quindi esattamente al giudice la fattispecie di riferimento. Sarà interessante conoscere la posizione dei giudici di legittimità su questa norma. Di certo, un recupero indiretto della teoria del contatto sociale vanificherebbe del tutto le finalità di una disciplina che aveva lo scopo di frenare la medicina difensiva. Sul tema, si rinvia a B. Meoli-S. Sica, *Sub. art. 7. Responsabilità civile della struttura e dell'esercente la professione sanitaria*, in B. Meoli-S. Sica-P. Stanzione (a cura di), *Commentario alla legge 8 marzo 2017, n. 24*, Napoli, Edizioni Scientifiche Italiane, 2018, 109 ss.

[23] Trib. Milano, 13 aprile 2000, in *Dir. inf.*, 2000, 371, con nota di S. Sica, *Danno morale per lesione della* privacy; v. pure S. Sica, *Danno morale e legge sulla privacy informatica*, in *Danno e resp.*, 282 ss.

[24] «La presente legge garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone

Ai sensi dell'art. 1 di quest'ultimo testo di legge, chiunque ha diritto alla protezione dei dati personali che lo riguardano. Si compie così il passaggio dalla strumentalità del diritto alla protezione dei dati personali alla sua autonomia: da un diritto tutelato se ed in quanto presupposto della violazione di un altro diritto fondamentale della persona, ad un diritto tutelabile *ex se*.

3. Considerazioni sul modello di responsabilità vigente

Si è tentato di tratteggiare il modello di responsabilità anteriore al *GDPR*, il quale, a parere di chi scrive, è ben riuscito nel suo intento di realizzare una forte tutela per chi subisca una violazione nel trattamento dei propri dati personali. Si arriva così al regime delineato all'art. 82 del GDPR[25], nonché alle sue disposizioni attuative contenute nel d.lgs. n. 101/2018.

Incidentalmente sia detto che la disciplina risultante dal combinato disposto del Regolamento, del decreto legislativo e dal residuo testo del Codice del 2003 (si è infatti smarrita l'occasione di arrivare a due sole "fonti" della materia) non ha avuto il coraggio di superare la logica della sanzione penale come strumento di repressione del trattamento illecito dei dati. In realtà, è dal 2001 che è stato avviato un processo di depenalizzazione della materia. Allo stato, la depenalizzazione era ancor più inevitabile, oggi ancor più attuale e sensata visto il potenziamento della sanzione amministrativa[26]. In ogni caso, ove si fosse voluto procedere a un ripristino della responsabilità penale, sarebbe stato necessario procedere a un'attenta operazione di scrittura delle fattispecie incriminatrici, per evitare un'elasticità di nozioni, foriera potenzialmente perfino di problemi di legittimità costituzionale.

fisiche, con particolare riferimento alla riservatezza e all´identità personale; garantisce altresì i diritti delle persone giuridiche e di ogni altro ente o associazione».

[25] Sul quale v. G. Giannone Codiglione, *Risk-basedapproach e trattamento dei dati personali*, in S. Sica-V. D'Antonio-G.M. Riccio (a cura di), *La nuova disciplina*, cit., 55 ss.

[26] Art. 83 GDPR, rubricato "Condizioni generali per infliggere sanzioni amministrative pecuniarie". V. G. Giannone Codiglione, *op. ult. cit.*, 73.

Comunque anche nel nuovo quadro normativo la responsabilità civile rimane l'asse portante.

La soluzione per il recepimento delle nuove norme europee è stata quella di abolire *tout court* l'art. 15, ormai ampiamente ricompreso nell'art. 82 del GDPR. Ivi si prevede che chiunque subisca un danno, materiale o immateriale, causato da una violazione del Regolamento, ha diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento[27].

Il secondo e il terzo comma dell'art. 82, invece, costituiscono una trasposizione del regime di cui all'art. 2050 cod. civ.[28]. Aderendo a questa ricostruzione, non può che derivarne che si andrà esenti da responsabilità nel momento in cui si sia in grado di dimostrare *di aver adottato le misure idonee*.

Tuttavia, si è convinti che la disciplina possa ricevere una doppia implementazione giurisprudenziale, sia in punto di *an*, che in punto di *quantum*. Quanto all'*an*, come più volte ribadito dalla Corte di Cassazione, se le misure fossero idonee, il danno non si produrrebbe affatto, *ergo* deve ritenersi necessaria l'allegazione di un fatto terzo interruttivo del nesso causale, con carattere di inevitabilità e imprevedibilità[29].

[27] L'art. 82, per come formulato, prevede anche un meccanismo di obbligazione solidale (quarto comma), salvo regresso (comma quinto), che è l'ennesima riprova di un *favor* verso il danneggiato.

[28] Tali commi recitano: «2. Un titolare del trattamento coinvolto nel trattamento risponde per il danno cagionato dal suo trattamento che violi il presente regolamento. Un responsabile del trattamento risponde per il danno causato dal trattamento solo se non ha adempiuto gli obblighi del presente regolamento specificatamente diretti ai responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento. 3. Il titolare del trattamento o il responsabile del trattamento è esonerato dalla responsabilità, a norma del paragrafo 2 se dimostra che l'evento dannoso non gli è in alcun modo imputabile».

[29] Si veda, ad esempio, Cass. 10 gennaio 2016, n. 222, in *Dir. giust.*, 2016, 3, relativa a un caso di smarrimento di documenti contenenti dati supersensibili, in cui si è escluso il diritto al risarcimento del danno se manca la prova che i dati siano entrati in possesso di persone estranee alla funzione amministrativa deputata al loro esame: «pur dando per provato il fatto storico dell'ascrivibilità dello smarrimento della documentazione contenente i dati supersensibili alla struttura pubblica sanitaria, appare del tutto arbitrario (sul piano logico e

L'obiezione mossa alla ricostruzione proposta è quella che paventa il rischio di un abuso della norma, come accaduto con quel filone giurisprudenziale, soprattutto dei giudici di pace, che riconoscevano somme simboliche per ogni spamming ricevuto[30]; quel fenomeno – anche se non da solo – ha fatto da premessa alla necessità di sistemazione della teorica del danno non patrimoniale operato dalle ben note *sentenze di San Martino*[31].

Sicché si ritiene che il modello verso cui propendere è quello di una fattispecie orientata sulla vittima, che è esposta a un'attività socialmente pericolosa. Al contempo pare necessario porre un limite, al fine di prevenire un abuso della regola. Esso si sostanzia nel rifiuto del riconoscimento di un danno *in re ipsa*, perché occorre anche per la voce di danno non patrimoniale la dimostrazione dell'elemento aggiuntivo della lesione di un diritto costituzionalmente rilevante.

storico) pretendere di inferire dal fatto in sé e per sé considerato, con un salto logico evidente, l'avvenuta conoscenza di tali dati da parte di persone estranee alla funzione amministrativa deputata al loro esame, potendo essere varie e molteplici le evenienze risolventesi in una dispersione dei documenti (contenenti i dati supersensibili) priva del danno lamentato (o, ancor meglio, solo ipotizzato)».

30 Giudice di pace Bari, 22 dicembre 2003, in *Danno e resp*., 2004, 880 ss., con nota di L. Caputi, *Cassette per la corrispondenza piene e danno esistenziale*; Giudice di pace Napoli, 7-10 giugno 2004, in *Danno e resp*., 2005, 659 ss., con nota di E.O. Policella, *Il danno da spamming*. Di recente, v. Cass. 8 febbraio 2017, n. 3311, che ha ribadito la necessità della verifica della "gravità della lesione" e della "serietà del danno" per il risarcimento del danno non patrimoniale *ex* art. 15 d.lgs. n. 196/2003.

31 Cass. 11 novembre 2008, nn. 26972, 26973, 26974, 26975, in *Giust. civ.*, 2009, 913 ss., con nota di M. Rossetti; in *Danno e resp.*, 2009, 19 ss., con nota di A. Procida Mirabelli di Lauro. Tra i molteplici contributi sul tema, si rinvia, in particolare, a: G. Ponzanelli, *La prevista esclusione del danno esistenziale e il principio di integrale riparazione del danno: verso un nuovo sistema di riparazione del danno alla persona*, in *Nuova giur. civ. comm.*, 2009, 90 ss.; P.G. Monateri, *Il pregiudizio esistenziale come voce del danno non patrimoniale*, in *Resp. civ. prev.*, 2009, 56 ss.; E. Navarretta, *Il valore della persona nei diritti inviolabili e la complessità dei danni non patrimoniali*, in *Resp. civ. prev.*, 2009, 63 ss.; M. Franzoni, *Il danno non patrimoniale del diritto vivente*, in *Corr. Giur.*, 2009, 1 ss.; F.D. Busnelli, *Le Sezioni Unite e il danno non patrimoniale*, in *Riv. dir. civ.*, 2009, 97 ss.; S. Patti, *Le Sezioni Unite e la parabola del danno esistenziale*, in *Corr. Giur.*, 2009, 415 ss.; C. Castronovo, *Danno esistenziale: il lungo addio*, in *Danno e resp.*, 2009, 5 ss.

Del resto, anche la giurisprudenza di merito e di legittimità si erano orientate in tal senso[32].

In questa prospettiva, l'art. 82 del GDPR potrebbe presentarsi anche come unica norma di riferimento per la responsabilità civile da illecito trattamento dei personali. D'altronde, un'interpretazione che tenga conto dei presupposti e che si orienti in una logica sostanziale di tutela dell'interessato non ha bisogno di esplicazioni ulteriori, ma ravvisa nell'art. 82 le *sembianze* dell'art. 2050 cod. civ.

Tuttavia non si può ignorare che si corre il rischio di affidare un ambito così delicato esclusivamente alla valutazione del giudice del caso concreto. Ecco perché in fase di dibattito anteriore all'adozione del decreto legislativo si è auspicato, ormai si può dire, invano la previsione di una norma di collegamento tra l'art. 82 e la fattispecie dell'art. 2050 cod. civ.; è sì vero che l'art. 82 è direttamente applicabile, ma è anche necessario trasferire il suo contenuto in un contesto di cultura giudiziaria dove i giudici sono abituati da tempo immemore a qualificare le ipotesi di danno in una delle ipotesi di riferimento del codice civile.

In conclusione, c'è da augurarsi che la giurisprudenza trovi nell'art. 82 il fondamento diretto della condanna risarcitoria, ma la circostanza che questa previsione non si applichi alle materie non coperte dal GDPR crea il pericolo che per esse torni ad avere vigenza esclusivamente l'art. 2043 cod. civ. e, quindi, una tutela che a parere di chi scrive è insufficiente[33].

In termini più generali, se è consentita una riflessione di portata più estesa, a volte si ha la sensazione che la protezione dei dati personali non esista nella misura in cui essa venga affidata

[32] V. Cass. 13 maggio 2015, n. 9785, in *Fam. dir.*, 2016, 469, che ha riconosciuto la responsabilità civile di una pubblica amministrazione per la lesione del diritto alla riservatezza quando non si adoperi con tutte le misure necessarie ad evitare il danno ovvero la diffusione dei dati personali, perché l'art. 18 della legge n. 675/1996 segue la disciplina dell'art. 2050 cod. civ. Nel caso di specie veniva riconosciuto il risarcimento del danno patito per la lesione del diritto alla riservatezza di un soggetto che aveva cambiato sesso, perché l'ufficio elettorale del Comune aveva trasmesso non soltanto il dato anagrafico, ma l'intero dossier comprensivo del procedimento di mutamento di sesso, non essenziale ai fini della nuova iscrizione anagrafica nel Comune di trasferimento.

[33] Cfr. G. Giannone Codiglione, *op. ult. cit.*, 77.

esclusivamente alla valutazione di rischio ed alla predisposizione di rimedi preventivi su base predittiva. Al giorno d'oggi vi è la tendenza ad abbandonare la nozione di *pericolo*, che è propria delle società prescientiste, per quella di *rischio*, che sottende la standardizzazione e la prevedibilità assoluta[34]. Ma nel caso del trattamento dei dati personali c'è il *pericolo*, non il *rischio*. Da ciò deriva la convinzione della necessità di regole di responsabilità il più possibile orientate verso la tutela della vittima, esposta a un *pericolo* e non a un *rischio* prevedibile *tout court*: l'"imprevedibile" è sempre dietro l'angolo e non può che farsene carico chi trae vantaggio dall'attività pericolosa.

[34] Il tema, di grande fascino soprattutto in prospettiva storica ed antropologica, risulta affrontato in relazione al principio di "precauzione", da ultimo, in M.G. Stanzione, *Principio di precauzione, tutela della salute e responsabilità della P.A. Profili di diritto comparato*, in *Comp.dir.civ*, 2016, 1-34, al quale si rinvia con la molteplice bibliografia *ivi* indicata.

Il nuovo Regolamento europeo sulla privacy tra bilanciamento del diritto alla protezione dei dati, esigenze di sicurezza e Stato di diritto

Emma A. Imparato

Sommario: 1. Il nuovo Regolamento europeo: alcune novità per garantire un "adeguato livello di sicurezza" – 2. Il diritto alla protezione dei dati ed esigenze di sicurezza tra Corte di Giustizia dell'Unione europea e principio di proporzionalità – 3. Le condizioni di liceità del trattamento dei dati e il trattamento "necessario" – 4. La sicurezza pubblica tra nuove competenze del diritto UE e tutela della privacy – 5. Il caso francese. Brevi conclusioni

1. Il nuovo Regolamento europeo: alcune novità per garantire un "adeguato livello di sicurezza"

Il nuovo Regolamento europeo 2016/679 sulla protezione dei dati[1] non è solo un atto che detta la normativa sulla protezione delle persone fisiche con riguardo al trattamento dei loro dati personali a tutela di un diritto fondamentale come riconosciuto, tra l'altro, dall'art. 8

[1] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016. Per le principali novità contenute nel regolamento, vedi, *ex plurimis*, G. Finocchiaro, *Introduzione al regolamento europeo sulla protezione dei dati*, in *Nuove leggi civ. comm*., XL, 2017, 1 e ss. Più in generale, sul processo di approvazione, v. L. Bolognini, E. Pelino, *Il Regolamento privacy europeo*, Milano, Giuffrè, 2016; F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, vol. I, Torino, Giappichelli, 2016.

della Carta dei diritti fondamentali dell'UE[2], quale parametro 'costituzionale' fondamentale di interpretazione[3], nonché dall'art. 16 del Trattato sul Funzionamento dell'UE (TFUE)[4]. È altresì un testo sulla sicurezza informatica cui è dedicata un'intera sezione (sez. 2, cap. IV). Anche in questo caso però l'obiettivo principale sembra essere quello di assicurare il diritto alla 'riservatezza' dei dati personali (considerando 83), da intendere, in quest'ultima accezione, in termini più ristrettivi rispetto al diritto alla protezione dei dati come diritto di un soggetto di "controllare" il complesso delle informazioni che allo stesso si riferiscono[5].

Alla luce anche della Convenzione europea dei Diritti dell'uomo[6], la riservatezza, quale sinonimo di privacy, impone in definitiva una

[2] Secondo, il comma 1 e 2 di tale articolo specificamente dedicato alla "Protezione dei dati di carattere personale": «1. Ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano. 2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica».

[3] Così anche la Corte di Giustizia UE, in particolare nella sentenza del 13 maggio 2014, *Google Spain, Google Inc. e Agencia Española de Protección de Datos (AEPD)*, (causa C-131/12), punto 68. V., in merito, per un commento in dottrina, 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, 569 ss. In generale, sull'utilizzo sempre più crescente nel tempo della Carta dei diritti come parametro autonomo, v. L. Trucco, *Carta dei diritti fondamentali e costituzionalizzazione dell'Unione europea*, Torino, Giappichelli, 2013, 117 ss. nonché A. Spadaro, *La «cultura costituzionale» sottesa alla Carta dei diritti fondamentali dell'UE. Fra modelli di riferimento e innovazioni giuridiche*, in *Dir. pubbl. comp. eur.*, n. 2/2016, in particolare 297 laddove si parla di "auto-applicatività" delle disposizioni della Carta in tema di diritti fondamentali.

[4] Al par.1 dell'art. 16 TFUE si legge che: «Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano».

[5] Cfr. G. Finocchiaro, *La giurisprudenza della Corte di Giustizia in materia di dati personali da Google Spain a Schrems*, in V. Zeno Zenovich-G. Resta (a cura di), *La protezione trasnazionale dei dati personali dai safe harbour principles a privacy shield*, Roma, RomaTre-Press, 2016, 118.

[6] Secondo l'art. 8 della Convenzione, comma 2: «Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è

tutela specifica che non riguarda tutta una serie di altri diritti – quale è quello, ad esempio, di accesso, di rettifica, di cancellazione, di ricevere idonea informativa, ben tutelati invece nel caso più generale della "protezione dei dati" – ma più limitatamente il diritto alla natura 'confidenziale' della comunicazione.

La finalità è la protezione della sfera personale dell'individuo che comunica con un altro affinché non vi sia diffusione all'esterno delle informazioni e la comunicazione possa svolgersi "senza ingerenze" da parte di terzi. In quest'ottica il nuovo regolamento, volendo assicurare un "adeguato livello di sicurezza" in grado di prevenire un trattamento non consentito dalla normativa, richiede l'adozione di diverse misure di protezione. Tra queste si pone anche l'obbligo di notifica all'autorità competente. Al fine di migliorare "effettivamente" la tutela della riservatezza dei dati personali, questa comunicazione non riguarda più peraltro, a differenza della disciplina pregressa, qualunque tipo di trattamento ma soltanto quei trattamenti che «potenzialmente presentano un rischio elevato per i diritti e le libertà delle persone fisiche, per loro natura, ambito di applicazione, contesto e finalità».

Riproducendo l'impianto normativo precedente, recepito poi nel nostro "Codice in materia di protezione dei dati personali"[7] – cosiddetto Codice della Privacy – l'attuale regolamento si mostra così rispetto al testo normativo precedente molto più dinamico e flessibile, pur rilevandosi al contempo anche molto più complesso. È proprio in considerazione di questa aumentata complessità che nell'individuare i requisiti che deve possedere il soggetto denominato "data protection officer" – ovvero, il responsabile della protezione dei dati – introdotto per la prima volta all'art. 37, il testo europeo mette l'accento principalmente sulle sue competenze giuridiche. In particola-

necessaria per la sicurezza nazionale, per la pubblica sicurezza, per il benessere economico del paese, per la difesa dell'ordine e per la prevenzione dei reati, per la protezione della salute o della morale, o per la protezione dei diritti e delle libertà altrui».

[7] Adottato con d.lgs. 30 giugno 2003, n. 196, tale codice regolamenta in maniera organica, quale testo unico, la materia sostituendo i diversi interventi legislativi succedutesi nel tempo. V. F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, Torino, Giappichelli, 2016.

re qui, al comma 5, si prevede che il responsabile della protezione dei dati deve avere "conoscenza specialistica della normativa" oltre che della prassi e pratiche in materia di protezione dei dati nel controllo del rispetto a livello interno del Regolamento. Quale deve essere il "livello necessario di conoscenza specialistica" si specifica in precedenza. Tra i considerando, al punto 97, si stabilisce che questo livello è determinato in particolare «in base ai trattamenti di dati effettuati e alla protezione richiesta per i dati personali trattati dal titolare del trattamento o dal responsabile del trattamento»[8]. Peraltro in considerazione del livello di rischio, connesso al trattamento dei dati, occorrerà effettuare in via preventiva – ovvero prima del trattamento – la "valutazione d'impatto" sulla protezione dei dati che pure vedrà interessato il responsabile della protezione dei dati in una 'consultazione preventiva' con l'autorità competente di controllo (art. 36).

2. Il diritto alla protezione dei dati ed esigenze di sicurezza tra Corte di Giustizia dell'Unione europea e principio di proporzionalità

Già dalla rapida panoramica quanto ad alcune novità giuridiche introdotte dal Regolamento appaiono chiare le non poche criticità che le diverse innovazioni normative porranno ai titolari dei trattamenti andando a coinvolgere diversi profili e funzioni aziendali, a partire appunto da quello giuridico-legale. Il fine principale è comunque l'adozione di misure e garanzie necessarie per proteggere i diritti e le libertà degli interessati con particolare riguardo al trattamento dati.

A quest'ultimo proposito, è lo stesso Regolamento a chiarire tuttavia il carattere non assoluto del diritto alla protezione dei dati di carattere personale, indubbiamente derogabile quand'anche soltanto in via eccezionale e temporanea. Questa visione corrisponde peraltro pienamente anche a quella affermata da lungo tempo dalla Corte di Giustizia dell'Unione europea.

[8] Il Garante per la protezione dei dati personali ha elaborato una versione integrata con i "Considerando" di riferimento in grado di offrire una lettura razionalizzata delle nuove disposizioni, reperibile on line all'indirizzo: *http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/6264597*

A più riprese i giudici di Lussemburgo hanno dichiarato che non è affatto esclusa l'ingerenza in tale diritto sia pure precisando però che ciò è possibile soltanto qualora «effettivamente limitata a quanto strettamente necessario»[9]. In questo senso, come si diceva, lo stesso regolamento europeo, in uno dei suoi primi considerando sui ben 173, conferma la regola per cui il diritto alla protezione dei dati personali non è prerogativa assoluta ma da contemperare con altri diritti fondamentali (considerando 4). Qui sebbene si specifichi che il «trattamento dei dati personali dovrebbe essere al servizio dell'uomo», ben si puntualizza poi che il diritto alla tutela dei dati, considerato «alla luce della sua funzione sociale», deve trovare una conciliazione, in un rapporto di bilanciamento, con altri diritti fondamentali, in ossequio al principio di proporzionalità[10].

Quest'ultimo principio può così comportare, secondo pure la Carta dei diritti dell'Unione europea, limitazioni all'esercizio dei diritti e delle libertà riconosciuti. Anche in questo caso si chiarisce però che tali restrizioni sono applicabili "solo laddove siano necessarie" e che deroghe alle libertà fondamentali devono comunque rispondere «effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui» (art. 52, par. 1 della Carta).

[9] V., in particolare, Corte di giustizia, 8 aprile 2014, cause riunite C-293/12 e C-594/12, *Digital Rights Ireland e Seitlinger*. Con tale decisione la Corte ha dichiarato invalida la direttiva 2006/24/CE del Parlamento europeo e del Consiglio, del 15 marzo 2006, giacché, tra le altre motivazioni, non prevedendo «norme chiare e precise che regolino la portata dell'ingerenza nei diritti fondamentali sanciti dagli articoli 7 e 8 della Carta, comporta un'ingerenza nei suddetti diritti fondamentali di vasta portata e di particolare gravità nell'ordinamento giuridico dell'Unione senza che siffatta ingerenza sia regolamentata con precisione da disposizioni che permettano di garantire che essa sia effettivamente limitata a quanto strettamente necessario». L'eccezionalità delle limitazioni al diritto alla protezione dei dati personali è affermata, peraltro, anche da CGUE, 11 dicembre 2014, causa C-212/13, *Ryneš*. Per un'elencazione dettagliata delle diverse pronunce emesse in merito e un commento di alcune di esse, v. 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 Federalismi.it, n. 15/2017 nonché G. Finocchiaro, *op. cit*.

[10] In tema di applicazione del principio di proporzionalità nel giudizio costituzionale interno, nella difficoltà di definirne i contorni, si v. F. Modugno, *La ragionevolezza nella giustizia costituzionale*, Napoli, Editoriale Scientifica, 2007, (III ristampa).

In quest'ottica, il *test* di proporzionalità è stato pienamente applicato, ai fini della decisione dell'interesse prevalente, dalla stessa Corte di Giustizia da cui peraltro lo stesso principio di proporzionalità discende. In più occasioni si è trovata a dover contemperare, nel giudizio di bilanciamento, il diritto alla sicurezza – intesa come prevenzione dei reati e contrasto al terrorismo – con quello alla protezione dei dati. In queste ipotesi, soprattutto in alcuni casi recenti particolarmente rilevanti avendo portato alla dichiarazione di invalidità degli atti normativi europei, l'ago della bilancia è finito col tendere sempre a favore della privacy. Ricorrente, in tutti i casi, è la causa d'invalidità: la portata dell'ingerenza nel diritto alla privacy non è limitata «effettivamente allo stretto necessario»[11]. Ovvero, secondo la lettura consolidata della giurisprudenza della Corte, il principio di proporzionalità non è stato rispettato giacché la tutela del diritto fondamentale al rispetto della vita privata a livello dell'Unione «esige che le deroghe e le restrizioni alla tutela dei dati personali intervengano entro i limiti dello stretto necessario»[12].

Addirittura talora, consentendosi un accesso generalizzato e senza alcuna discriminazione, si è ritenuto che fosse stata legittimata una invasione illimitata della privacy, laddove nessuna disposizione puntuale era stata dettata al fine di 'delimitare in maniera oggettiva' l'accesso da parte delle autorità pubbliche.

Secondo costante giurisprudenza della Corte sono invero sempre necessarie "regole chiare e precise" quanto alla definizione delle misure che comportano un'ingerenza nel diritto alla protezione dei dati affinché, nel determinarsi la portata della limitazione all'esercizio di tale diritto, si possa offrire un'effettiva tutela contro eventuali abusi e violazioni arbitrarie dei pubblici poteri. In caso contrario non garantendosi un adeguato livello di protezione dei dati, si finisce con il pregiudicare il "contenuto essenziale" del diritto fondamentale al rispetto della vita privata, tutelato dall'articolo 7 della Carta[13] nonché,

[11] CGUE, *Digital Rights Ireland*, cit., punto 65.

[12] Ancora, CGUE, *Tele 2 Sverige AB c. Post-och telestyrelsen*, cit., par. 96.

[13] CGUE (Grande sezione), 6 ottobre 2015, causa C-362-14, *Maximilian Schrems c. Data Protection Commissioner*, in particolare, par. 94 e 95. Con tale sentenza la Corte, rivendicando a sé il potere di controllo di legittimità degli atti UE, ha annullato la decisione n. 2000/250 della Commissione europea sull'adeguatezza della protezione – fondata sui *Safe Harbour Principles ovvero* sui principi dell'"ap-

in ultimo, del diritto fondamentale ad una "tutela giurisdizionale effettiva", quale sancito all'articolo 47 della Carta non prevedendosi, in quest'ultima ipotesi specifica, alcuna possibilità per l'individuo di avvalersi di efficaci rimedi giurisdizionali al fine di accedere, rettificare o, ancora, sopprimere i dati personali che lo riguardano. La conseguenza grave è quella che, minandosi l'esistenza di un controllo giurisdizionale effettivo, si può finire con l'attentare – osserva la Corte UE – la stessa "esistenza di uno Stato di diritto".

Peraltro, secondo l'interpretazione offerta dalla Corte, il principio di proporzionalità non è applicabile solo all'ambito delle attività pubbliche.

Il *test* di bilanciamento e proporzionalità può trovare applicazione anche direttamente all'attività dei soggetti privati che, quali titolari del trattamento, sono tenuti a valutare se, alla luce del principio di necessità del trattamento (e dunque di proporzionalità), i dati sono ancora necessari «in rapporto alle finalità per le quali sono stati raccolti o trattati»: il permanere della necessità delle limitazioni della riservatezza dell'individuo può venir meno qualora «i dati risultino inadeguati, non siano o non siano più pertinenti, ovvero siano eccessivi in rapporto alle finalità suddette e al tempo trascorso»[14].

In ogni caso, a prescindere dall'ambito delle attività, il requisito di necessità e quello di proporzionalità si mostrano in stretta connessione, confondendosi l'uno nell'altro[15]: affinché possa essere

prodo sicuro" – che consentiva *ex* art. 25 della Direttiva 95/46 il trasferimento dati personali di cittadini europei verso gli Stati Uniti d'America. V., per un commento specifico, in una nota a commento, v. M. Casali, *Un bilanciamento tra diritti contrapposti: privacy vs Sicurezza nazionale*, in G. Alpa-G. Conte (a cura di), *Casi decisi dalla Corte di Giustizia dell'Unione europea sui diritti*, Torino, Giappichelli, 2018, 65 e ss.

[14] CGUE (Grande sezione), 13 maggio 2014, causa C-131/12, *Google Spain SL, Google Inc. c. Agencia Española de Protección de Datos (AEPD), Mario Costeja González*. Per un commento, in dottrina, v. *ex plurimis*, F. Pizzetti, *La decisione della Corte di giustizia sul caso Google Spain: più problemi che soluzioni*, in Federalismi.it, n. 1/2014; 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 *Diritto dell'informazione e dell'Informatica*, n. 4-5/2014.

[15] V., in merito le conclusioni dell'avvocato generale Henrik Saugmandsgaard Øe presentate il 19 luglio 2016 nelle Cause riunite C-203/15 e C-698/15, *Tele 2 Sverige AB c. Post-och telestyrelsen*, in particolare al punto 223.

adottata una misura derogante al principio della riservatezza delle comunicazioni occorre che essa sia «necessaria, opportuna e proporzionata all'interno di una società democratica»[16], in rapporto agli obiettivi perseguiti dalla normativa.

Insomma, secondo questa visione, necessità e proporzionalità appaiono condizioni pienamente sovrapponibili.

In realtà, i due termini sono ben differenziabili, per quanto l'operazione di distinzione si riveli piuttosto complessa come del resto affatto semplice e oggettiva si mostra, soprattutto alla luce degli sforzi di individuazione compiuti dalle corte costituzionali nazionali, la stessa definizione dei "criteri" di applicazione del test di proporzionalità. Nulla si rivela «più opinabile della valutazione di proporzionalità»[17].

Un tentativo di distinzione delle condizioni e definizione dei criteri potrebbe essere quello che, nell'ambito della "sequenza altamente formalizzata"[18] quanto alla proporzionalità, veda il termine della necessità quale elemento della fase di valutazione antecedente a quella relativa alla proporzionalità, esprimendo il primo l'idea della 'efficacia' della misura[19]: quest'ultima potrebbe, cioè, essere conside-

[16] V. CGUE, 21 dicembre 2016, *Tele 2 Sverige AB c. Post-och telestyrelsen*, Cause riunite C-203/15 e C-698/15, par. 95 laddove la Corte richiama, ai fini interpretativi, l'articolo 15, paragrafo 1, prima frase, della direttiva 2002/58. Per una nota a commento, v. S.F. Giovannangeli, *Data retention. Il caso Tele2 sverige ab e Watson e altri: la Corte di Giustizia UE fornisce gli standard da seguire*, in G. Alpa-G. Conte (a cura di), *Casi decisi dalla Corte di Giustizia dell'Unione europea sui diritti*, *op. cit.*, 94 e ss.

[17] Cfr S. Staiano, *Diritto alla riservatezza e potere pubblico*, in Federalismi.it, n. 17/2017, 9. L'A. effettua, commentandola, una lucida e approfondita ricostruzione delle tecniche argomentative utilizzate dai giudici costituzionali nazionali – in particolare quanto al *test* di proporzionalità – ponendole in analogia con quelle consolidate nella giurisprudenza del giudice sovranazionale europeo, sia pure nella chiara consapevolezza della varietà dei termini messi a confronto, diversi a seconda dei diversi contesti costituzionali.

[18] Così, S. Staiano, *op. cit.*, 9, richiamandosi, in particolare, alla teoria generale elaborata da R. Alexy.

[19] Cfr., J. Rivers, *Proportionality and variable intensity of review*, in *Cambridge Law Journal*, 65/2006, 198, in particolare laddove sostiene che «the test of necessity thus expresses the idea of efficiency or Pareto-optimality. A distribution is efficient or Pareto-optimal if no other distribution could make at least one person

rata necessaria soltanto in assenza di qualsiasi altra misura che sia altrettanto adeguata pur essendo "meno restrittiva"[20]. Di conseguenza qualora la misura risulti inefficiente, dovrebbe essere respinta e non si potrebbe passare a valutarne, secondo la sequenza logica valutativa, la condizione di proporzionalità relativa più in particolare allo scopo normativo. Qui l'indagine dovrebbe guardare, insomma, più specificamente al rapporto che intercorre tra lo scopo previsto dalla normativa che pone i limiti al diritto e i mezzi previsti per raggiungere tale scopo[21].

La valutazione di proporzionalità, secondo questa visione, si traduce in un'operazione di bilanciamento complessa tra il beneficio nell'adempiere allo scopo normativo e il danno causato dalla restrizione o deroga del diritto costituzionale.

3. Le condizioni di liceità del trattamento dei dati e il trattamento "necessario"

Il trattamento dei dati può trovare condizioni di liceità in altre ipotesi diverse dal consenso dell'interessato, variabili a seconda del tipo di dati, ovvero, a seconda si tratti di dati comuni oppure rientranti nella categoria di dati particolari.

Nel caso dei dati comuni, all'art. 6, vengono riprese esattamente le stesse cinque condizioni di liceità – ulteriori rispetto al consen-

better off without making any one else worse off. Likewise an act is necessary if no alternative act could make the victim better off in terms of rights-enjoyment without reducing the level of realisation of some other constitutional interest».

[20] V., CGUE, 22 gennaio 2013, C-283/11, Sky Österreich, punto 54 nonché CGUE, 13 novembre 2014, C-443/13, *Reindl*, punto 39 e CGUE, 16 luglio 2015, C-83/14, *CHEZ Razpredelenie Bulgaria*, punto 120. In dottrina, v. in particolare, B. Pirker, *Proportionality Analysis and Models of Judicial Review*, Groningen, Europa Law Publishing, 2013, 29 e ss.

[21] V., più specificamente, A. Barak, *Proportionality: Constitutional Rights and their Limitations*, Cambridge, Cambridge University Press, 2012, 344 secondo cui: «The first three components of proportionality deal mainly with the relation between the limiting law's purpose and the means to fulfil that purpose. [...]. The test of proportionality stricto sensu is different. [...] It focuses on the relation between the benefit in fulfilling the law's purpose and the harm caused by limiting the constitutional right. It is based on balancing».

so – disciplinati nel testo precedente, presenti peraltro, quasi tutte, nel nostro testo codicistico, sia pure con una differenza importante quanto alla 'natura' connessa.

Nella normativa europea, invero, tali condizioni sono legate per lo più, a differenza del testo italiano che si riferisce alla natura soggettiva dell'organo che tratta i dati, al tipo di finalità perseguite dal titolare del trattamento, ovvero, tra gli altri, il conseguimento del "legittimo interesse" da considerare secondo un giudizio di bilanciamento con i diritti dell'interessato (*lett. f)*. Peraltro, quest'ultima valutazione deve essere effettuata – e questa costituisce un'ulteriore novità – non più dall'Autorità ma dallo stesso titolare del trattamento: in armonia con la nuova visione introdotta dal Regolamento, l'accento qui è sulla "responsabilizzazione" – *accountability* nell'accezione inglese – dei titolari del trattamento dei dati.

Per l'ipotesi delle "categorie particolari di dati personali" di cui all'art. 9 del Regolamento, caratterizzate da particolare natura che impone una protezione maggiore, pur vigendo un esplicito divieto generale di trattamento, si deve evidenziare un ampliamento del ventaglio delle possibili condizioni di liceità. Questa categoria riguardante, oltre ai dati biometrici e giudiziari, i cosiddetti dati sensibili declinati peraltro nel caso europeo in maniera meno estensiva del nostro testo[22], conta oggi invero ben 10 ipotesi di liceità del trattamento oltre a quella del consenso. Alcune di quelle nuove rientrano nel caso di trattamento necessario per "motivi di interesse pubblico", al quale pure l'ultima bozza italiana del maggio 2018 di adattamento riserva una disposizione specifica.

Innanzitutto si deve citare la categoria generale prevista alla lett. *g* dell'art. 9 – ovvero il trattamento necessario "per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri" (lett. *g*) – contemplata altresì nella direttiva precedente (e quindi in qualche modo anche nel nostro Codice) e tuttavia

[22] All'art. 4, lett. *d* del nostro Codice Privacy nel dettare una definizione di tali dati si amplia in maniera indeterminata le convinzioni attraverso il riferimento ad "altro genere", ovvero: «i dati personali idonei a rivelare l´origine razziale ed etnica, le convinzioni religiose, filosofiche *o di altro genere*, le opinioni politiche, l´adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale».

nel testo attuale, a differenza di quello pregresso, meglio garantito, ben individuandosi oggi il parametro di valutazione delle eventuali contrapposte esigenze dato dal "principio di proporzionalità". Poi la specifica e nuova categoria relativo al settore della sanità pubblica (lett. *i*).

Le ipotesi ascrivibili a quest'ultima categoria, stante il proemio e in particolare i considerando nn. 55 e 56, includono le nuove condizioni sottese ai trattamenti ritenuti necessari allorché effettuati dalle autorità pubbliche allo scopo di realizzare fini di associazioni religiose, oppure di raccogliere dati sulle opinioni politiche delle persone. Nulla si dice tuttavia qui della sicurezza nazionale o pubblica. A questo profilo è dedicata specifica parte riguardante, stante l'intitolazione della sezione, le 'limitazioni' alla disciplina (art. 23).

4. La sicurezza pubblica tra nuove competenze del diritto UE e tutela della privacy

A questo punto è necessario effettuare un chiarimento sulla competenza del diritto UE in merito alla sicurezza, sia pure solo per rapidi accenni.

Se la direttiva pregressa registrava, tra i considerando, l'incompetenza dell'ordinamento UE nel campo della pubblica sicurezza, affidando, per tali casi, esclusivamente agli Stati membri il potere di dettare 'eventuali deroghe' alle norme sul trattamento, nel Regolamento attuale si prende atto delle modifiche dell'atto istitutivo, intervenute in particolare col trattato di Lisbona. Oggi, all'art. 4, lo "spazio di libertà, sicurezza e giustizia" è attribuito – quale fine fondamentale dell'UE – alla competenza concorrente UE sia anche non intendendosi sottrarre, ai sensi dell'art 72 del Trattato medesimo, il mantenimento della sicurezza interna "all'esercizio delle responsabilità incombenti agli Stati membri". Lo stesso Trattato prevede, su questa linea, la possibilità per taluni Stati membri di rafforzare la reciproca collaborazione in materia di difesa istituendo una cooperazione strutturata permanente (*Permanent Structured Cooperation*-PESCO).

In quest'ottica, oltre al "piano di attuazione in materia di sicurezza e difesa del dicembre 2016", che delinea la via da seguire per lo sviluppo della politica della sicurezza UE, il Consiglio europeo ha adot-

tato, nel dicembre 2017, una decisione che istituisce la struttura c.d. PESCO a cui partecipano tutti gli Stati membri dell'UE ad eccezione di tre, ovvero Danimarca, Malta e Regno Unito. Con le conclusioni del 22 giugno 2017, lo stesso Consiglio poi, oltre ad accogliere con favore la comunicazione della Commissione relativa a un Fondo europeo per la difesa, rivolge un'esortazione in particolare al legislatore UE. L'auspicio è che siano adottate in futuro norme che consentano ai sistemi di "rimuovere automaticamente contenuti volte ad incitare atti terroristici" e di controllare da parte delle autorità pubbliche le comunicazioni criptate «salvaguardando al contempo i benefici che tali sistemi comportano per la protezione della privacy, dei dati e delle comunicazioni».

Per la verità però è già con il Regolamento qui in esame che si provvede a dettare alcune disposizioni in merito alla sicurezza a partire dall'estensione e ampliamento dell'elenco dei diritti e dei principi che possono essere soggetti a restrizioni.

A differenza del passato, il catalogo dei diritti non include più solo o comunque soprattutto il diritto di accesso e di informazione. Il testo attuale ritiene che possa essere inciso, in nome della sicurezza, qualunque diritto a partire da quello di informazione, di accesso e cancellazione dati, per arrivare al diritto alla portabilità dei dati, al diritto di opporsi, alle decisioni basate sulla profilazione.

Si specifica inoltre che qualunque misura legislativa possa essere adottata per la salvaguardia della sicurezza pubblica, laddove questa comporti limitazioni ai diritti alla protezione dei dati, sia pure nel rispetto della loro "essenza", dovrà comunque dettare, quale misura "necessaria e proporzionata in una società democratica", disposizioni specifiche riguardanti, tra gli altri aspetti, i "periodi di conservazione e le garanzie applicabili" (art. 23, comma 2, lett. *f*).

5. Il caso francese. Brevi conclusioni

Quest'ultimo profilo, quello della conservazione, può in verità incontrare le maggiori criticità ben potendosi porre in netto contrasto, tra gli altri, con il principio generale di cui all'art. 5, che stabilisce che i dati non debbono essere conservati, in una forma che consenta l'identificazione degli interessati, più a lungo del necessario, cioè oltre il conseguimento delle finalità per le quali sono

trattate. Del resto è la stessa giurisprudenza della Corte di Giustizia Ue nonché di diverse corti nazionali a dimostrare la 'vulnerabilità' dell'attività di conservazione.

In questo senso, a riprova della difficoltà di conciliare la tutela dell'interesse alla sicurezza pubblica con quello della protezione della privacy, quanto al processo di conservazione, si può richiamare l'ordinamento francese, conoscendo quest'ultimo da lungo tempo lo stato d'urgenza: la preminenza del potere esecutivo-amministrativo, a discapito delle garanzie dei diritti derivanti anche dal controllo preventivo dell'autorità giudiziaria qui messo fuori gioco in particolare nelle attività di perquisizioni domiciliari, ha evidenziato forti problematiche quanto alla capacità di tutelare la sicurezza nazionale nel rispetto del diritto alla protezione della vita privata.

A partire dalla pronuncia n. 2016-536, il *Conseil constitutionnel* ha incominciato a denunciare, dichiarando incostituzionali le norme dettate in particolare nel caso di perquisizione domiciliare ai fini della sicurezza, la mancata osservanza del dovere di prevedere idonee 'garanzie' a tutela dei diritti fondamentali.

Con un'altra decisione 2016-600 ritornando sul tema e specificamente sulla conservazione, la stessa corte francese ha ritenuto poi che la normativa interna dovesse prevedere un termine massimo definito di conservazione dei dati e non generico, corrispondente ai 3 mesi (salvo non venisse constata una violazione).

Il caso francese è piuttosto emblematico dimostrando le difficoltà che si incontrano nel tentativo di dettare disposizioni in grado di conciliare le esigenze di sicurezza e la tutela della privacy.

Qui, ma lo stesso vale per il diritto di qualunque altro paese e più in generale per il diritto UE, l'obiettivo perseguito deve essere invero sempre quello di garantire "una connessione equilibrata" – per usare le parole della Corte francese – tra l'obiettivo costituzionale di preservare l'ordine pubblico e il diritto al rispetto della vita privata. Perché nel gioco del bilanciamento volto ad assicurare un equilibrio effettivo tra queste due esigenze, in bilico si possono trovare non solo i diritti ma – per riprendere le considerazioni dei giudici di Lussemburgo – lo stesso Stato di diritto.

L'attuazione del Regolamento europeo in tema di protezione dei dati personali: aspetti comparatistici

Fiore Fontanarosa

Sommario: 1. Premessa – *2.* La portata unificatrice del regolamento n. 679/2016 – 3. Divergenze giuridiche in tema di protezione dei dati personali nei Paesi dell'Unione europea – 4. Conclusioni

1. Premessa

La protezione dei dati personali nell'Unione europea è disciplinata, in gran parte, dalla legislazione comunitaria. La direttiva n. 46/1995 è rimasta in vigore fino al 25 maggio 2018, poiché da tale data il regolamento n. 679/2016 (*General Data Protection Regulation)* si occupa di disciplinare, in maniera prevalente, la materia in discorso. Il GDPR si discosta dal precedente intervento normativo, sia nella veste formale, che in quella sostanziale. Invero, il GDPR mira a migliorare, non solo il livello di protezione dei dati personali, bensì anche l'armonizzazione del loro trattamento in tutta l'UE[1].
Nonostante si sia in presenza di un atto normativo che si pone l'obiettivo di raggiungere il massimo grado di armonizzazione possibile, ci si chiede se l'implementazione del regolamento varierà tra gli Stati membri, a causa delle differenze, giuridiche e culturali, rinvenibili nei diversi ordinamenti nazionali. L'obiettivo del presente

[1] Sul punto v. C. Tikkinen-Piri-A. Rohunen-J. Markkula, *EU General Data Protection Regulation: Changes and implications for personal data collecting companies*, in *Computer law & security review*, 2018, 34, 135.

saggio è dunque quello di indagare qual è la posizione dei vari Stati europei riguardo alla tematica della protezione dei dati personali, al fine di tentare di prevedere l'impatto che l'attuazione del regolamento produrrà nei diversi Paesi UE. La questione concernente i tempi e i modi di applicazione del regolamento n. 679/2016 costituisce un importante banco di prova per verificare la capacità del legislatore europeo di rispondere alle sfide, economiche, giuridiche e tecnologiche, imposte dalla società digitale. Inoltre, le modalità di attuazione del GDPR rappresenteranno un attendibile indicatore del livello di integrazione giuridica raggiunto dall'Unione europea, poiché l'implementazione del regolamento in questione fornirà importati indicazioni in ordine alla reale capacità delle istituzioni UE di realizzare una unificazione del diritto all'interno dello spazio giuridico comunitario.

2. La portata unificatrice del regolamento n. 679/2016

A livello comunitario, il diritto alla protezione dei dati personali ha fatto il suo ingresso con la direttiva n. 46/1995, la quale ha adottato un modello di disciplina in virtù del quale la protezione dei dati è funzionale alla garanzia della privacy[2]. Tuttavia, la direttiva, a 20 anni dalla sua attuazione, non era più in grado di fornire il livello di armonizzazione richiesto tra gli Stati membri dell'UE, né l'efficienza nel garantire il diritto alla protezione dei dati personali nell'attuale contesto digitale. Ecco perché la Commissione europea ha deciso di approntare una riforma fondamentale del quadro giuridico di protezione dei dati nell'ambito comunitario.

Il GDPR rappresenta una importante opera di riorganizzazione e di riformulazione del diritto europeo sulla protezione dei dati personali a un livello di generalizzazione adeguato a un testo normativo che mira ad essere il fulcro della legislazione comunitaria in materia[3]. Se si vogliono comprendere lo spirito e la finalità del re-

[2] G. González Fuster-S. Gutwirth, *Opening up personal data protection: A conceptual Controversy*, in *Computer law & security review*, 2013, 29, 535.

[3] F. Piraino, *Il regolamento generale sulla protezione dei dati personali e i diritti dell'interessato*, in *Nuove leggi civili commentate*, 2017, 375.

golamento *de quo* è necessario "leggere tra le righe" dei considerando. Utile, nell'ambito del discorso che si sta svolgendo, è l'analisi del considerando n. 4, secondo cui il diritto alla protezione dei dati personali non è un diritto assoluto e «deve essere considerato alla luce della sua funzione sociale»; da ciò deriva che, nell'ottica del bilanciamento tra l'interesse della persona e il profilo della circolazione dei dati, il GDPR sarebbe 'sbilanciato' in favore di quest'ultimo, il che sarebbe confermato dalla finalità dichiarata di favorire un clima di fiducia per lo sviluppo dell'economia digitale in tutto il mercato interno[4].

Venendo al tema della unificazione della disciplina in materia di tutela dei dati personali, l'utilizzo di un regolamento, in luogo della direttiva, è significativo del mutamento di approccio del legislatore europeo, il quale ha avvertito la necessità di sostituire l'obiettivo originario dell'armonizzazione con quello, certamente più ambizioso, dell'uniformazione, sebbene non manchino incisivi rinvii ai legislatori nazionali[5]. Sotto questo profilo, è indubbio che lo strumento del regolamento sia funzionale a conseguire un elevato livello di unificazione, sebbene la disciplina preveda, in taluni casi, un certo margine di manovra degli Stati membri che, secondo il considerando n. 10 del regolamento, «dovrebbero rimanere liberi di mantenere o introdurre norme nazionali al fine di specificare ulteriormente l'applicazione del presente regolamento», né si esclude che «il diritto degli Stati membri stabilisca le condizioni per specifiche situazioni di trattamento, anche determinando con maggiore precisione le condizioni alle quali il trattamento di dati personali è lecito».

Dunque, il regolamento lascia margini consistenti alle autonome scelte dei diritti nazionali. In primo luogo, si pensi alla 'delega' ad individuare le ipotesi di trattamenti fondati sulla necessità di adempiere a un obbligo legale al quale è assoggettato il titolare (art. 6, par. 1, lett. c), reg. n. 679/2016). In secondo luogo, si pensi alle ipotesi di trattamenti necessari per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito

[4] A. Iuliani, *Note minime in tema di trattamento dei dati personali*, in *Europa e diritto privato*, 2018, 306.

[5] A. Iuliani, *op. cit.*, 304 e s.

il titolare (art. 6, par. 1, lett. e), reg. n. 679/2016)[6]. Inoltre, si pensi all'art. 9, par. 4, il quale consente ai diritti nazionali di mantenere o di introdurre ulteriori condizioni, comprese limitazioni, per quanto concerne il trattamento dei dati genetici, biometrici e relativi alla salute. Infine, sempre rimanendo in materia di dati 'sensibili', tra le fattispecie di liceità del trattamento di quest'ultimi ve ne è una che compariva già nella dir. n. 46/1995, sebbene sotto forma di possibilità rimessa agli Stati membri, vale a dire quella del trattamento necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato. Secondo alcuni questa previsione normativa cozzerebbe con lo spirito uniformatore del regolamento, rappresentando una fonte di potenziale frammentazione del quadro giuridico europeo, poiché il concetto di interesse pubblico rilevante è rimesso alla valutazione degli Stati membri, con la conseguenza che potrebbero registrarsi interpretazioni divergenti nei vari Paesi membri[7]. Del resto, la stessa proporzionalità alla finalità perseguita, ovvero il rispetto dell'essenza del diritto costituiscono concetti che ben si prestano ad interpretazioni 'autarchiche' da parte degli Stati comunitari, il che potrebbe produrre contenziosi con la Commissione europea in ordine alla corretta applicazione del regolamento[8].

Oltre che per le numerose 'deroghe' previste in favore della disciplina nazionale, il GDPR è stato criticato dai primi commentatori anche sotto il profilo definitorio: basti pensare che la nuova disciplina non precisa ulteriormente la nozione di dati personali, che rimane piuttosto ambigua se si fa riferimento soltanto al testo dispositivo, laddove indicazioni interpretative possono essere rinvenute nel Preambolo, nonostante quest'ultimo sia privo di valore giuridico vincolante[9].

[6] F. Piraino, *op. cit.*, 372.

[7] M. Granieri, *Il trattamento di categorie particolari di dati personali nel Reg. UE 2016/679*, in *Nuove leggi civili commentate*, 2017, 174.

[8] In tal senso M. Granieri, *op. loc. cit.*

[9] M.G. Stanzione, *Il regolamento europeo sulla privacy: origini e ambito di applicazione*, in *Europa e diritto privato*, 2016, 1260.

Le considerazioni finora espresse inducono quindi a riflettere circa la reale portata unificatrice del regolamento, facendo sorgere il dubbio che il legislatore comunitario abbia voluto porre l'accento, non tanto sull'obiettivo dell'unificazione (o armonizzazione totale) del settore, quanto piuttosto su quello di apprestare garanzie volte a proteggere, quindi in un certo senso a favorire, la libera circolazione dei dati personali. Nonostante le criticità appena esposte in ordine alla questione dell'uniformazione giuridica, alcuni ritengono che il "cambio di passo" delle istituzioni comunitarie, riscontrabile in *subiecta materia*, non riguardi tanto l'aspetto 'sostanziale', quanto quello 'formale', essendo cioè rappresentato proprio dal 'passaggio' dallo strumento della direttiva a quello del regolamento[10]. Tuttavia, anche dal punto di vista contenutistico una parte della dottrina, particolarmente quella straniera, ritiene che il GDPR abbia una forte portata unificatrice, poiché esso regolerebbe, in maniera uniforme, le questioni più importanti, lasciando dei poteri di specificazione, 'limitati' ed 'eccezionali', agli Stati, i quali devono comunque sempre giustificare le previsioni normative eventualmente introdotte nell'ordinamento interno che si distaccano dall'obiettivo comunitario, quest'ultimo rappresentato dal raggiungimento di un quadro giuridico pienamente armonizzato[11].

3. Divergenze giuridiche in tema di protezione dei dati personali nei Paesi dell'Unione europea

Nell'ambito dell'Unione europea il riconoscimento effettivo del diritto alla protezione dei dati personali non dipende soltanto dal quadro giuridico, ma anche dalla interpretazione ed applicazione della normativa comunitaria da parte dei giudici e delle Autorità garanti della protezione dei dati (DPA). Invero, la legislazione in tema di protezione dei dati personali contiene molte norme 'aperte', le quali richiedono una ulteriore 'traduzione' in regole e pratiche concrete, a seconda del settore di riferimento. A causa delle differenze riscontrabili nel contesto giuridico, ma anche culturale, dei vari Paesi membri dell'Unio-

[10] J.P. Albrecht, *How the GDPR Will Change the World*, in *EDPL*, 2016, 3, 287.

[11] J.P. Albrecht, *op. loc. cit.*

ne europea, la direttiva n. 46/1995 è stata implementata in maniera diversa negli Stati comunitari. Sebbene il GDPR abbia l'obiettivo di armonizzare ulteriormente la normativa esistente nella materia *de qua*, molti ritengono che le descritte divergenze continueranno ad esistere[12]. I dubbi espressi circa la capacità uniformatrice del GDPR si basano, sostanzialmente, sulla scarsa uniformazione raggiunta dall'Unione europea nel settore della protezione dei dati personali, prodotta dalla implementazione della direttiva n. 46/1995. Questo perché, secondo alcuni, le differenze giuridiche riscontrabili nei diversi Stati costituirebbero un importante e forse insormontabile ostacolo al raggiungimento di una armonizzazione totale del settore in discorso.

Di seguito si analizzeranno alcune evidenti divergenze riscontrabili in tema di diritto alla protezione dei dati personali negli ordinamenti dei Paesi membri, nonché le principali novità introdotte dal GDPR le quali, invece di smussare le citate differenze, potrebbero addirittura acuirle. Un primo aspetto riguarda le fonti del diritto alla protezione dei dati personali ed in particolare la 'concorrenza' tra strumenti di *hard law* e quelli di *soft law*. Invero, molti Paesi hanno una legislazione settoriale che protegge ulteriormente il trattamento dei dati personali: si pensi all'assistenza sanitaria, alle telecomunicazioni, alla finanza, al diritto penale, al settore pubblico. In alcuni Stati, poi, pur non esistendo una legislazione di settore sono presenti alcuni strumenti giuridici, quali 'linee guida', codici di condotta o altre forme di *soft law*, volti a regolamentare il trattamento dei dati personali. Ai sensi dell'art. 27 della direttiva n. 46/1995 gli Stati membri avrebbero dovuto incoraggiare l'uso dei codici di condotta e di autoregolamentazione. Anche il GDPR incoraggia all'utilizzo dei codici di condotta (art. 40, parr. 1 e 2, reg. n. 679/2016). Il fatto è che proprio su questo punto si registrano, tra gli Stati comunitari, notevoli divergenze. Si pensi che, ad esempio, la Svezia e il Regno Unito sono Paesi che hanno una lunga tradizione nel campo della autoregolamentazione ed hanno sviluppato, di conseguenza, codici di autoregolamentazione nel settore della privacy mentre altri Stati, come ad

[12] B. Custers-F. Dechesne-A.M. Sears-T. Tani-S. van der Hof, *A comparison of data protection legislation and policies across the EU*, in *Computer law & security review*, 2018, 34, 235.

esempio i Paesi Bassi, la Germania, l'Irlanda e la Francia, utilizzano, nel settore del trattamento dei dati personali, una combinazione di forme di autoregolamentazione e di regolamentazione governativa; altri ancora, quali la Romania, l'Italia e la Spagna, si sono maggiormente orientati verso forme di regolamentazione governativa[13].

Un'altra novità introdotta dal GDPR riguarda la previsione della figura del responsabile della protezione dei dati. Quest'ultimo è un soggetto incaricato di vigilare sul rispetto della normativa in materia di privacy e di fungere da punto di contatto con l'autorità di controllo. In realtà, tale figura non costituisce una novità 'assoluta' nel contesto europeo, poiché essa era già prevista dalle disposizioni normative nazionali di diversi Stati membri, fra cui Germania, Svezia, Paesi Bassi, Francia e Lussemburgo, mentre la maggior parte dei Paesi UE non contemplava, finora, la figura del *Data Protection Officer* (DPO). In ogni caso, nei Paesi appena citati la figura del responsabile della privacy non era considerata obbligatoria, ad eccezione della Germania, Paese nel quale i responsabili della privacy sono richiesti per le organizzazioni aventi più di 10 dipendenti. Del resto, la Germania è stata anche il primo Paese, nel 1970, ad istituire la figura del *Data Protection Officer*[14]. Certo è che con l'entrata in vigore del GDPR molte aziende e Pubbliche Amministrazioni avranno l'obbligo di nominare il responsabile della protezione dei dati[15]. Questi responsabili della privacy non sono richiesti solo all'interno dell'UE, ma anche in altri Paesi, nelle ipotesi in cui le aziende (extra-comunitarie) cooperano o commerciano con organizzazioni che si trovano all'interno del territorio comunitario.

Un terzo elemento di potenziale divergenza nell'implementazione del GDPR riguarda l'applicazione di quest'ultimo da parte delle Autorità nazionali garanti della protezione dei dati, per le questioni di loro competenza. Questo perché le *Data protection agencies* (DPA) hanno poteri diversi, nonché opzioni divergenti, nel sanzionare le violazioni delle leggi dettate nella materia in discorso. Del resto, la

[13] B. Custers-F. Dechesne-A.M. Sears-T. Tani-S. van der Hof, *op. cit*., 240.

[14] Sul punto v. B. Custers-F. Dechesne-A.M. Sears-T. Tani-S. van der Hof, *op. loc. cit*.

[15] Si stima che in tutto il mondo saranno necessari circa 75.000 addetti alla privacy.

precedente legislazione comunitaria ha subìto un'opera di 'frammentazione' in tutta l'Unione europea a causa della diversa interpretazione ed applicazione della direttiva n. 46/1995 operata dagli Stati membri proprio sul versante sanzionatorio. Infatti, nei Paesi comunitari le sanzioni attualmente previste in materia di trattamento dei dati personali variano ampiamente. Alcuni Paesi, come la Spagna, dispongono di un sistema sanzionatorio fortemente repressivo delle violazioni commesse in *subiecta materia*, mentre altri Paesi, quali la Francia, hanno optato per un regime sanzionatorio più mite. Nei Paesi Bassi, in Romania e in parte anche in Italia, le DPA hanno la possibilità di imporre sanzioni che dipendono dal fatturato annuo delle aziende, un tipo di sanzione che è ora applicabile in tutti gli Stati UE, in conseguenza dell'entrata in vigore del GDPR. In termini assoluti, le ammende massime sono molto elevate in Francia (massimo 3 milioni di euro) e più basse in Romania (22.000 euro). Anche le sanzioni penali, nei Paesi nei quali è prevista la loro irrogazione, variano notevolmente, con pene detentive massime che vanno dai 6 mesi ai 5 anni[16].

Una quarta criticità, che è stata espressa dalla dottrina nei riguardi della capacità unificatrice del regolamento n. 679/2016, concerne il trattamento di quelli che vengono correntemente designati con l'espressione 'dati sensibili', cioè di quei dati che, nell'ambito della categoria dei dati personali, occupano una posizione di speciale rilevanza e 'delicatezza' in ragione della loro particolare 'natura'. Ebbene, dal punto di vista comparatistico ancora oggi permangono differenze di disciplina normativa riguardo alla categoria di informazioni inquadrabili come dati sensibili. Questo perché l'art. 8 della direttiva n. 46/1995, dopo aver stabilito, al co. 2, le ipotesi di deroga al divieto di trattare i dati personali idonei a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché il trattamento dei dati relativi alla salute e alla vita sessuale, prevedeva, al co. 4, che gli Stati membri potevano, per motivi di interesse pubblico rilevante, stabilire ulteriori deroghe oltre a quelle previste dalla direttiva stessa, sulla base della legislazione nazionale o di una decisione dell'autorità di controllo. Sebbene la maggior parte degli Stati comunitari si sia limitata ad

[16] B. Custers-F. Dechesne-A.M. Sears-T. Tani-S. van der Hof, *op. cit*., 241.

una integrale trasposizione della norma di cui all'art. 8, senza prevedere ulteriori fattispecie di deroghe, oltre a quelle, cioè, tipizzate dalla direttiva, tuttavia alcuni Stati hanno deciso di apprestare forme 'rafforzate' di tutela riguardo ad ulteriori 'particolari' informazioni personali, non comprese nel citato articolo, il che ha, ovviamente, determinato una divergenza nell'attuazione del provvedimento comunitario rispetto alla categoria dei dati sensibili[17]. Il regolamento del 2016 riproduce, sostanzialmente, la disposizione della direttiva del 1995 prevedendo, infatti, che: «Gli Stati membri possono mantenere o introdurre ulteriori condizioni, comprese limitazioni, con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute». A nostro avviso, tale disposizione si attaglia perfettamente allo spirito armonizzante della direttiva, piuttosto che a quello uniformante del regolamento europeo. Questo perché la possibilità rimessa agli Stati membri di 'rafforzare' la tutela prevista in favore dei dati sensibili, se da un lato mira ad elevare il livello protettivo di tale particolare categoria di informazioni personali, dall'altro 'sconta' delle criticità sul versante della unificazione della disciplina nella materia in esame.

Un ultimo elemento di differenziazione nell'attuazione del GDPR, elemento che, per la verità, era emerso già all'indomani dell'emanazione del regolamento, avvenuta nel 2016, dunque molto prima della sua entrata in vigore, concerne la disciplina in materia di consenso prestato dai soggetti minori d'età al trattamento dei dati personali. Invero, la direttiva n. 46/1995 non conteneva disposizioni specifiche per i minori d'età; quindi, i responsabili del trattamento dei dati dovevano rispettare gli stessi requisiti legali, indipendentemente dall'età degli interessati[18]; invece, il GDPR ha introdotto, all'art. 8, una specifica previsione volta a proteggere i minori d'età, definendo le condizioni che rendono 'legittimo' il consenso prestato da costoro alla elaborazione dei dati personali[19].

[17] Sul punto v. *amplius* M. D'amico, *Il trattamento "pubblico" dei dati sensibili: la disciplina italiana a confronto con il modello europeo*, in *Diritto comunitario e degli scambi internazionali*, 2002, 820.

[18] E. Lievens-V. Verdoodt, *Looking for needles in a haystack: Key issues affecting children's rights in the General Data Protection Regulation*, in *Computer law & security review*, 2018, 34, 270.

[19] E. Lievens-V. Verdoodt, *op. cit.*, 271.

La necessità di regolamentare l'interazione fra i minori e la c.d. società dell'informazione è stata da tempo avvertita Oltreoceano. La legislazione federale statunitense, già dal 1998, con il *Children's Online Privacy Protection Act* (COPPA), ha disciplinato il trattamento *online* dei dati personali concernenti i minori, fissando a 13 anni l'età per il consenso al trattamento (c.d. consenso digitale). Ad imitazione della disciplina statunitense il legislatore comunitario, all'art. 8 del GDPR, sancisce che qualora la liceità del trattamento presupponga il consenso dell'interessato, ai sensi dell'art. 6, par. 1, lett. *a*), «per quanto riguarda l'offerta diretta di servizi della società dell'informazione ai minori, il trattamento di dati personali del minore è lecito ove il minore abbia almeno 16 anni. Ove il minore abbia un'età inferiore ai 16 anni, tale trattamento è lecito soltanto se e nella misura in cui tale consenso è prestato o autorizzato dal titolare della responsabilità genitoriale». In ogni caso, l'ultimo capoverso dell'art. 8, par. 1, rende flessibile il limite d'età per il consenso digitale, prevedendo la possibilità, per gli Stati membri, di stabilire per legge un'età inferiore, purché non al di sotto dei 13 anni. Tale previsione, pur opportuna, secondo alcuni, a garanzia dei diritti fondamentali del bambino, quali la libertà di espressione, di associazione e di riunione, sanciti dagli artt. 13 e 15 della Convenzione sui diritti dell'infanzia e dell'adolescenza, potrebbe ingenerare non pochi problemi applicativi, in assenza di una armonizzazione delle discipline nazionali[20].

Come si è visto, l'art. 8 consente agli Stati membri di abbassare la soglia d'età di 16 anni ad un minimo di 13 anni. Se gli Stati membri dovessero utilizzare tale opzione, il risultato sarebbe l'applicazione, in materia di consenso digitale espresso dai minori, di soglie d'età differenziate nei Paesi dell'Unione europea. Ciò implica che le società che forniscono servizi *online* in più Stati comunitari dovranno rispettare regole diverse nei vari Stati membri, il che richiede sforzi e investimenti supplementari, in particolare per le aziende più piccole[21]. I primi dibattiti in ordine alla questione in esame sono già emersi in diversi ordinamenti giuridici e alcuni legislatori nazionali o le Autorità per la protezione dei dati (DPA) hanno espresso il loro

[20] F. Naddeo, *Il consenso al trattamento dei dati personali del minore*, in *Dir. informazione e informatica*, 2018, 44 e s.

[21] E. Lievens-V. Verdoodt, *op. cit.*, 272.

parere in merito. Nei Paesi Bassi, ad esempio, la legge nazionale sulla protezione dei dati conteneva già un limite di 16 anni per il trattamento dei dati personali dei minori basato sul consenso. La recente proposta di legge, che dà attuazione al GDPR, non si discosta da questo limite d'età. Al contrario, altri Stati membri stanno prendendo in considerazione l'adozione di un'età inferiore. In Spagna, sebbene l'Autorità garante della protezione dei dati personali ha dichiarato, immediatamente dopo l'adozione del GDPR, che l'età prevista per il consenso dei minori sarebbe stata mantenuta a 14 anni, l'attuale progetto che dà attuazione al regolamento n. 679/2016 stabilisce il limite a 13 anni[22]. In Austria, il Parlamento ha recentemente adottato emendamenti alla legge austriaca sulla protezione dei dati, che ora prevede che i minori possano acconsentire al trattamento dei dati in relazione ai servizi erogati della società dell'informazione, a partire dai 14 anni. In Belgio, l'Autorità garante ha sottolineato che le aziende che elaborano dati personali dei soggetti minorenni dovrebbero sviluppare meccanismi di verifica, sia dell'età dell'individuo, che del consenso espresso dei genitori. La Commissione per i diritti dei bambini ha emanato un parere in cui raccomanda al governo belga di ridurre l'età del consenso a 13 anni; secondo la Commissione, infatti, una soglia d'età elevata metterebbe troppe responsabilità nelle mani dei genitori dei soggetti minorenni[23]. Infine, in Italia il decreto legislativo di adeguamento al GDPR ha fissato in 14 anni l'età minima per l'accesso ai servizi offerti dalla società dell'informazione nei casi previsti dall'art. 8 del regolamento comunitario.

4. Conclusioni

A conclusione del presente saggio si vuol tentare di offrire una risposta all'interrogativo posto in premessa e cioè se il regolamento n. 679/2016 possa contribuire a favorire una maggiore uniformazione della disciplina della protezione dei dati personali all'interno dello spazio giuridico comunitario, anche alla luce delle considerazioni espresse da coloro che ipotizzano che il GDPR possa addirittura

[22] E. Lievens-V. Verdoodt, *op. cit.*, 272 e s.

[23] E. Lievens-V. Verdoodt, *op. cit.*, 273.

costituire un modello ideale per giungere ad una armonizzazione globale della materia in esame[24]. È noto che, a differenza della direttiva, il regolamento è direttamente applicabile in tutti gli Stati membri dell'Unione europea, senza la necessità di atti di recepimento, prestandosi dunque a conseguire l'obiettivo, non già di una semplice armonizzazione, ma di una unificazione del diritto degli Stati comunitari. Ciononostante, alcuni, partendo dal presupposto che la direttiva n. 46/1995 non è riuscita a produrre una armonizzazione totale della materia, essendo stata implementata in maniera diversa nei vari Paesi UE, ritengono che le descritte divergenze giuridiche, ravvisabili nei Paesi membri, continueranno ad esistere, sia a livello legislativo, che a livello di prassi[25]. Tali considerazioni fanno sorgere dei dubbi circa la volontà del legislatore europeo di operare, mediante l'emanazione del GDPR, una unificazione della materia *de qua*. La risposta, forse, potrebbe essere trovata, come si è accennato in premessa, analizzando i 'considerando', piuttosto che le disposizioni normative del regolamento comunitario. Il GDPR, dopo aver ricordato che l'obiettivo della direttiva n. 46/1995 era quello «di armonizzare la tutela dei diritti e delle libertà fondamentali delle persone fisiche rispetto alle attività di trattamento dei dati e assicurare la libera circolazione dei dati personali tra Stati membri» (considerando n. 3), non contiene un esplicito riferimento all'obiettivo dell'unificazione, poiché nel considerando n. 2 sottolinea come la disciplina comunitaria vuol contribuire a realizzare uno spazio di libertà, sicurezza e giustizia, una unione economica, il progresso economico e sociale, il rafforzamento e la convergenza delle economie nel mercato interno, nonché il benessere delle persone fisiche. In tale considerando traspare il forte accento che il regolamento pone sulla valenza economica del 'trattamento', ma soprattutto del 'trasferimento' dei dati. Certo, il GDPR tiene conto, al considerando n. 10, che è opportuno assicurare un'applicazione coerente e omogenea delle norme a protezione dei diritti e delle libertà fondamentali delle persone fisiche con riguardo al trattamento dei dati personali in tutta l'Unione; tut-

[24] In tal senso T. Curtiss, *Privacy harmonization and the developing world: the impact of the EU's General Data Protection Regulation on developing economies*, in *Washington Journal of Law, Technology & Arts*, 2016, 12, 119.

[25] B. Custers-F. Dechesne-A.M. Sears-T. Tani-S. van der Hof, *op. cit.*, 243.

tavia anche in tale considerando emerge come il raggiungimento di una uniformità nella disciplina del trattamento dei dati nel contesto comunitario è funzionale a rimuovere gli ostacoli alla circolazione di quest'ultimi all'interno dell'Unione europea (oltre che ad assicurare la tutela delle persone fisiche). L'obiettivo dell'unificazione del diritto pare dunque retrocedere rispetto alla necessità di garantire, soprattutto a livello extracomunitario, un efficace ed elevato livello di protezione della libera circolazione dei dati personali.

Un'ultima considerazione attiene alla omogeneità giuridica riscontrabile nell'ambito dell'Unione europea, sia dal punto vista 'quantitativo', che 'qualitativo'. Invero, con riferimento al primo aspetto, l'osservazione elementare è che allorquando venne emanata la direttiva n. 46/1995 l'UE contava 15 Stati, mentre oggi i Paesi membri sono 28. Ovviamente, le difficoltà di raggiungere una piena armonizzazione giuridica in questo come in altri settori del diritto non sono legate soltanto all'allargamento dell'Unione europea, ma soprattutto alla disomogenità giuridica riscontrabile nei vari Stati, anche in virtù della compresenza delle tradizioni giuridiche di *civil law* e di *common law*. Il fatto è che, sebbene la maggior parte dei Paesi membri abbia un sistema giuridico romanistico, il GDPR risulta fortemente permeato dal pensiero giuridico maturato nella cultura anglosassone, le cui 'tracce' si ritrovano, non soltanto nel nuovo approccio al rischio basato sul principio della *accountability* e sul conseguente modello di responsabilità, ma anche nella introduzione del criterio di ragionevolezza[26]. Tali scelte di politica legislativa pongono delicati problemi di interpretazione o, meglio, di trasposizione dei concetti giuridici all'interno delle categorie dogmatiche del giurista domestico, contribuendo a perpetuare le divergenze riscontrabili all'interno degli ordinamenti nazionali ed ostacolando, in tal modo, il raggiungimento di una reale unificazione in materia di diritto alla protezione dei dati personali all'interno del contesto comunitario.

[26] In tal senso G. Finocchiaro, *Introduzione al regolamento europeo sulla protezione dei dati*, in *Nuove leggi civili commentate*, 2017, 16.

La circolazione dei dati personali nella proposta di Direttiva UE sulla fornitura di contenuti digitali

Alberto De Franceschi

Sommario: 1. Introduzione – 2. Il ruolo del consenso al trattamento dei dati personali nel diritto dei contratti – 3. Il ruolo del consenso al trattamento dei dati personali e gli aspetti critici del requisito della «prestazione attiva» di dati personali nella proposta di direttiva UE sulla fornitura di contenuti digitali – 4. I dati personali come oggetto del contratto: la necessità di una rilettura, in chiave evolutiva, della nozione di "prezzo" e degli obblighi di informazione precontrattuale – 5. Conclusioni

1. Introduzione

La progressiva crescita del numero di contratti basati sullo scambio e l'elaborazione di dati, ed in particolare di dati personali, ha fatto sì che i dati stessi siano in misura crescente divenuti parte della promessa obbligatoria[1]. Peraltro, i contratti che hanno ad oggetto la fornitura di beni o servizi verso il trasferimento di dati personali vengono spesso qualificati come gratuiti. Tuttavia, ciò in molti casi significa più propriamente che la fornitura di beni o servizi viene eseguita a fronte di una controprestazione diversa dal denaro, e nel-

[1] Sul punto v. in particolare G. Resta-V. Zeno-Zencovich, *Volontà e consenso nella fruizione dei servizi in rete*, in *Riv. trim. dir. proc. civ.*, 2018, 411 ss. Nella letteratura straniera v. ad es. A. Metzger, *Dienst gegen Daten: Ein synallagmatischer Vertrag*, in *Archiv civ. Praxis*, 2016, 817 ss.

la specie a fronte della fornitura di dati personali, o altri dati, e della contestuale autorizzazione al loro trattamento[2].

Accanto ai già cennati contratti di fornitura di beni o servizi, ulteriori ipotesi di modelli contrattuali che prevedono una remunerazione non sotto forma di denaro, bensì di dati personali, sono non solo i contratti per l'utilizzo di motori di ricerca *online* e dei *social networks*[3], bensì anche un numero crescente di contratti di assicurazione. Con sempre maggiore frequenza, le società di assicurazione offrono infatti ai propri clienti una riduzione dell'ammontare del premio a fronte della fornitura di dati personali da parte dell'assicurato e dell'autorizzazione al loro trattamento: ciò accade tipicamente nell'ambito dei contratti di assicurazione per la c.d. responsabilità civile automobilistica oppure dei contratti di assicurazione sulla vita. Nel contesto degli schemi contrattuali testé richiamati è dato commisurare effettivamente il valore dei dati personali di cui l'assicurato autorizza il trattamento da parte dell'altro contraente[4].

I dati personali di cui sia stato autorizzato il trattamento in cambio della fornitura di beni o servizi vengono poi utilizzati per gli scopi più vari, come ad esempio per la realizzazione di azioni pubblicitarie mirate, la creazione di profili di utente, le funzioni di c.d. *dynamic pricing*[5], la valutazione delle funzionalità e dei deficit di un determinato prodotto, o – come accade nei cennati modelli dei contratti di assicurazione – l'adeguamento del profilo di rischio dell'assicurato[6].

[2] A tale proposito v. ad es. C. Langhanke-M. Schmidt-Kessel, *Consumer Data as Consideration*, in *Journal of European Consumer and Market Law*, 2015, 218 ss.; M. Schmidt-Kessel-A. Grimm, *Unentgeltlich oder Entgeltlich? Der vertragliche Austausch von digitalen Inhalten gegen personenbezogene Daten*, in *Zeitschr. für die gesamte Privatrechtswissenschaft*, 2017, 84 ss.

[3] Sul punto v. C. Perlingieri, *Profili civilistici dei* social networks, Napoli, Edizioni Scientifiche Italiane, 2014, 66 ss.

[4] S. e.g. M. Helmes, *Verkehrstelematik und Versicherung: Technik – Datenschutz – Versicherungsprodukte*, in *Versicherungsrecht*, 2015, 1096; K. Kinast-C. Kühnl, *Telematik und Bordelektronik – Erhebung und Nutzung von Daten zum Fahrverhalten*, in *Neue jur. Wochenschr.*, 2014, 3057.

[5] V. in proposito l'analisi di M. Ebers, *Dynamic Algorithmic Pricing: Abgestimmte Verhaltensweise oder rechtmäßiges Parallelverhalten?*, in *Neue Zeitschr. für Kartellrecht*, 2016, 554 ss.

[6] Alcuni valori indicativi si mostrano in proposito utili: il valore di ciascun account in occasione dell'acquisto di *Whatsapp* da parte di *Facebook* è stato stimato

La disciplina relativa alla protezione dei dati personali, sino ad oggi modellata sull'esigenza di tutelare il diritto fondamentale dell'individuo al rispetto della propria sfera privata, scolpito, tra l'altro, nell'art. 8 della Carta dei Diritti fondamentali dell'Unione europea, non è in grado di fornire risposte convincenti alle questioni che toccano il cuore del diritto dei contratti, dal momento che esso non ha tanto di mira la regolazione di rapporti patrimoniali, quanto di rapporti di *status*[7].

2 Il ruolo del consenso al trattamento dei dati personali nel diritto dei contratti

Alla base di un'obbligazione avente ad oggetto la trasmissione di dati personali[8] si colloca necessariamente il consenso dell'interessato al trattamento dei dati stessi, mentre il loro materiale trasferimento ha in realtà un valore sussidiario[9].

in una cifra pari a ca. 40 Dollari USA; il valore medio di un profilo *Facebook* è stimato in circa 88 Euro (Deutsche Bank Research, *Big Data – Die ungezähmte Macht*, 2014, 18 ss.; Organisation for Economic Co-operation and Development, *Exploring the Economics of Personal Data. A Survey of Methodologies for Measuring Monetary Value*, 2013, 18 ss.

[7] In proposito v. ad es. G. Resta, *Autonomia privata e diritti della personalità*, Napoli, Jovene, 2005, 250 ss.

[8] Per un'analisi delle criticità di questo fenomeno, v. European Data Protection Supervisor, *Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content*, 14 marzo 2017, 7: «There might well be a market for personal data, just like there is, tragically, a market for live human organs, but that does not mean that we can or should give that market the blessing of legislation. One cannot monetise and subject a fundamental right to a simple commercial transaction, even if it is the individual concerned by the data who is a party to the transaction».

[9] Sul consenso al trattamento dei dati v. ad es. V. Carbone, *Il consenso, anzi i consensi, nel trattamento informatico dei dati personali*, in *Danno e resp.*, 1998, vol. I, 28; V. Cuffaro, *Il consenso dell'interessato*, in V. Cuffaro-V. Ricciuto (a cura di), *La disciplina del trattamento dei dati personali*, Torino, Giappichelli, 1997, 204 ss.; S. Patti, *Il consenso dell'interessato al trattamento dei dati personali*, *Riv. dir. civ.*, 1999, 456 s.; G. Resta, *Autonomia privata e diritti della personalità*, cit., 271 ss.; S. Sica, *Il consenso al trattamento dei dati personali: metodi e modelli di qualificazione giuridica*, in *Riv. dir. civ.*, 2001, vol. II, 621 ss.; S. Thobani,

Peraltro, il consenso al trattamento dei dati personali fornito mediante la manifestazione di volontà rilevante ai fini della disciplina sulla tutela dei dati personali può considerarsi oggetto del contratto solo nell'ipotesi in cui l'elaborazione dei dati personali non sia già consentita in forza di legge[10].

In proposito deve richiamarsi l'art. 6, par. 1, lett. b del regolamento UE n. 679/2016 (di seguito: GDPR)[11], che autorizza il trattamento dei dati personali necessario all'esecuzione di un contratto di cui l'interessato sia parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso. Tale previsione ricomprende solo i dati che siano necessari per la conclusione e per l'esecuzione del contratto, non invece gli ulteriori dati che vengano eventualmente considerati dalle parti come autonomo oggetto della prestazione all'interno del rapporto contrattuale. Per questa ragione, l'obbligo di ottenere il consenso al trattamento dei dati personali ai fini della loro circolazione si estende solo ai dati personali che non debbano già essere forniti in forza di legge.

I requisiti del consenso al trattamento dei dati personali, Santarcangelo di Romagna, Maggioli, 13 ss.; V. Zeno-Zencovich, *Profili negoziali degli attributi della personalità*, in *Il diritto dell'informazione e dell'informatica*, 1993, 545 ss. Per una critica del ruolo del consenso come strumento di tutela dell'interessato, v. Rodotà, *Protezione dei dati e circolazione delle informazioni*, in *Riv. crit. dir. priv.*, 1984, 732 ss.; G. Mirabelli, *Le posizioni soggettive nell'elaborazione elettronica dei dati personali*, in *Dir. inf.*, 1993, 324. Nella letteratura straniera v. ad es. E. Kosta, *Consent in European Data Protection Law*, Leiden, Brill, 2013, 235 ss.; R. Janal, *Fishing for an Agreement: Data Access and the Notion of Contract*, in S. Lohsse-R. Schulze-D. Staudenmayer (a cura di), *Trading Data in the Digital Economy: Legal Concepts and Tools*, Baden Baden-Oxford, Nomos-Hart, 2017, 271; A. Ohly, "*Volenti non fit iniuria*". *Die Einwilligung im Privatrecht*, Tübingen, Mohr Siebeck, 2002, 11 ss., 237 ss.; B. Buchner, *Die Einwilligung*, in *Datenschutz und Datensicherheit*, 2010, 39; C. Langhanke-M. Schmidt-Kessel, *Consumer Data*, cit., 220; M. Schmidt-Kessel-K. Erler-A. Grimm-M. Kramme, *Die Richtlinienvorschläge der Kommission zu Digitalen Inhalten und Online-Handel – Teil 2*, *Zeitschrift für das Privatrecht der Europäischen Union*, 2016, 59.

[10] C. Langhanke-M. Schmidt-Kessel, *Consumer Data*, cit., 220.

[11] Regolamento UE n. 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.

Tuttavia, tali schemi contrattuali vanno soggetti anche ad importanti limiti fissati dal legislatore. Il consenso al trattamento dei dati personali deve infatti essere prestato sempre in modo sufficientemente preciso, in modo tale da individuare chiaramente lo scopo per cui tali dati vengono raccolti[12]. Da ciò segue che, in ragione del requisito della necessaria determinatezza o determinabilità dell'oggetto del contratto, il titolare dei dati personali non possa obbligarsi a trasferire una quantità illimitata di dati. Oltre a ciò, il titolare dei dati personali non può considerarsi facultizzato a rinunciare al diritto di revocare in ogni momento il consenso al trattamento di tali dati[13], in ragione del rilievo secondo cui la tutela della personalità trova fondamento costituzionale anche nella tutela dei dati personali e che non sarebbe dato rinunciare in modo permanente a siffatta tutela[14].

Rimane da chiarire la portata dei numerosi divieti di offerta congiunta sanciti dalla disciplina a tutela dei dati personali. L'art. 7, par. 4 GDPR fa proprio tale divieto, ma solo con intensità ridotta, prevedendo che nel valutare se il consenso sia stato liberamente prestato, debba tenersi «nella massima considerazione» l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto[15]. Tali divieti non si pongono peraltro necessariamente in contrasto con la configurabilità dei dati personali come oggetto del contratto[16].

[12] V. l'art. 6, par. 1, n. 1 GDPR ed il *considerando* n. 32 GDPR. Cfr. ad es. A. Fici-E. Pellecchia, *Il consenso al trattamento*, in R. Pardolesi (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, Milano, Giuffrè, 2003, 509 s.

[13] V.C. Langhanke-M. Schmidt-Kessel, *Consumer Data*, cit., 220.

[14] V. in proposito anche l'art. 8 della Carta dei diritti fondamentali dell'Unione europea e l'art. 8 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali.

[15] Cfr. il *considerando* n. 43 GDPR, che contiene una formulazione molto più incisiva. Cfr. art. 6, 8 della Proposta di Regolamento del Parlamento Europeo e del Consiglio relativo al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettroniche e che abroga la direttiva 2002/58/CE.

[16] In tal senso v. anche G. Spindler, *Verträge über digitale Inhalte*, in *Multimedia und Recht*, 2016, 150.

In assenza di un'autorizzazione da parte del legislatore, solo a partire dal momento della comunicazione dell'autorizzazione al trattamento dei dati personali questi assumono un apprezzabile valore economico per colui che li ha ricevuti o li riceverà, in quanto è proprio grazie al consenso che costui sarà autorizzato ad utilizzare i dati[17].

3. Il ruolo del consenso al trattamento dei dati personali e gli aspetti critici del requisito della «prestazione attiva» di dati personali nella proposta di direttiva UE sulla fornitura di contenuti digitali

Sul versante del diritto dei contratti, il quadro normativo è destinato a mutare sensibilmente, quantomeno con riguardo ai contratti di fornitura di contenuti digitali, non appena il Parlamento europeo avrà approvato la proposta di direttiva presentata dalla Commissione europea il 9 dicembre 2015[18], relativa a determinati aspetti dei contratti di fornitura di contenuto digitale (di seguito: DCD): a tale proposito, infatti, una delle novità più rilevanti coincide con la circostanza che nell'ambito di applicazione di tale strumento normativo vengono espressamente inclusi anche quei contratti che prevedono una controprestazione non tanto e non solo in denaro, bensì sotto forma della fornitura dati e, in particolare, di dati personali[19].

L'art. 3 DCD stabilisce infatti che la direttiva deve considerarsi applicabile anche nel caso di esecuzione di una prestazione diversa dal pagamento di un prezzo in danaro, nella misura in cui il consumatore si obblighi ad eseguire «attivamente» una prestazione diversa da quella consistente nel versamento di una somma di denaro, sotto forma della fornitura di dati personali o altri dati. Indicazioni

[17] C. Langhanke-M. Schmidt-Kessel, *Consumer Data*, cit., 220; G. Spindler, *Verträge über digitale Inhalte*, cit., 150.

[18] Commissione europea, 9 dicembre 2015, Proposta di direttiva del Parlamento europeo e del Consiglio relativa a determinati aspetti dei contratti di fornitura di contenuti digitali, COM (2015) 634 final.

[19] Per una decisa critica a tale impostazione, v. European Data Protection Supervisor, *Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content*, 14 marzo 2017, 7.

relative al concetto di "fornitura attiva dei dati personali" sono contenute nel *considerando* n. 14 DCD, ai sensi del quale la direttiva non è suscettibile di applicarsi alle ipotesi in cui il professionista entri nella disponibilità dei dati personali[20] senza che il consumatore li abbia «attivamente» forniti, posto che l'accettazione di *Cookies* da parte del consumatore non potrebbe essere qualificata come fornitura "attiva" di dati personali. In proposito, non è peraltro chiaro per quale motivo il riferimento sia solo ad una specifica modalità di acquisizione dati.

Sussistono inoltre rilevanti dubbi in merito all'adeguatezza dell'esclusione delle ipotesi da ultimo menzionate dall'ambito di applicazione della DCD, dal momento che anche in tali casi l'offerente approfitta in misura rilevante dei dati e delle informazioni messe a disposizione dal consumatore[21]. In relazione a ciò, ci si chiede in particolare per quale motivo un soggetto non possa considerarsi meritevole di tutela ogniqualvolta l'offerente raccolga i dati personali senza alcuna cooperazione del loro titolare[22].

In particolare, anche qualora il consumatore si limiti semplicemente ad accettare il prelievo dei propri dati mediante i c.d. *Cookies*, si può a mio avviso affermare che egli stia fornendo «attivamente» dati personali[23].

La DCD non contiene purtroppo alcuna precisa indicazione in merito all'interazione della disciplina di tutela dei dati personali con quella volta a disciplinare la loro circolazione in via contrattuale.

[20] Critica pesantemente tale soluzione G. Spindler, *Verträge* über *digitale Inhalte*, cit., 149.

[21] V. in tal senso ad es. R. Schulze, *Supply of Digital Content. A New Challenge for European Contract Law*, in A. De Franceschi (a cura di), *European Contract Law and the Digital Single Market. The Implications of the Digital Revolution*, Cambridge-Antwerp-Portland, Intersentia, 2016, 141; B. Lurger, *Anwendungsbereich und kaufvertragliche Ausrichtung der DIRL- und FWRL-Entwürfe*, in C. Wendehorst-B. Zöchling-Jud (a cura di), *Ein neues Vertragsrecht für den digitalen Binnenmarkt*, Vienna, Manz, 2016, 35.

[22] Così V. Mak, *The new proposal for harmonised rules on certain aspects concerning contracts for the supply of digital content*, Study for the JURI-Committee of the European Parliament, 2016, 9.

[23] V. a tal proposito H. Beale, *Scope of application and general approach of the new rules for contracts in the digital enviroment*, Study for the JURI-Committee of the European Parliament, 2016, 13.

Tale strumento si limita infatti, nel *considerando* n. 22, a dichiarare illimitatamente applicabili le disposizioni in merito alla protezione dei dati personali.

L'art. 7, comma 2 GDPR sulla protezione dei dati personali prevede che la richiesta di consenso dell'interessato debba essere presentata in modo chiaramente leggibile e distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Qualora parti della dichiarazione rappresentino una violazione del regolamento sulla protezione dei dati personali, e precisamente della disposizione testé richiamata, esse non saranno vincolanti. Ciò sarà ancor più vero nell'ipotesi in cui l'intera dichiarazione rappresenti una violazione del menzionato obbligo di trasparenza[24]. Naturalmente, l'onere della prova graverà sul professionista.

La formulazione della menzionata norma deve intendersi riferita sia ai dati che l'utilizzatore trasmetta in occasione della sua registrazione sul sito *Internet* del professionista, sia agli ulteriori dati che il consumatore "depositi" all'interno dello stesso sito in occasione dell'utilizzo dei contenuti digitali e/o di ulteriori prestazioni offerte dal professionista[25].

A tale proposito, si pone il quesito se anche i dati trasmessi dal cliente successivamente al primo accesso ai contenuti digitali messi a disposizione dal professionista possano essere considerati come (parte della) prestazione e se tali dati possano essere ricompresi nell'art. 3, comma 1, DCD.

L'art. 3, comma 4, DCD esclude dall'ambito di applicazione della direttiva le ipotesi di fornitura di contenuti digitali verso dati personali, qualora la controparte pretenda dal consumatore dati personali la cui elaborazione sia necessaria per l'esecuzione del contratto (come ad es. l'inserimento della localizzazione geografica che sia necessaria per il corretto funzionamento di una applicazione mobile: così v. ad es. il *considerando* n. 14 DCD), oppure qualora l'accesso ai dati personali del consumatore si renda necessario al

[24] Cfr. art. 9 della Proposta di Regolamento del Parlamento Europeo e del Consiglio relativa al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettroniche e che abroga la direttiva 2002/58/CE.

[25] Cfr. B. Lurger, *Anwendungsbereich*, cit., 35.

fine di rispettare delle prescrizioni di legge (eccezione già prevista dall'art. 7, comma 1, lett. b, dir. 1995/46/CE e dall'art. 6, comma 1, lett. b, GDPR) ed egli non elabori tali dati in un modo compatibile con tale scopo[26].

La direttiva trova tuttavia di nuovo applicazione, e la trasmissione di dati personali deve essere di nuovo considerata come "oggetto del contratto", qualora i dati non vengano elaborati in un modo compatibile con l'obiettivo dell'adempimento del contratto. Lo stesso vale qualora il professionista utilizzi per scopi commerciali i dati che esso abbia richiesto al consumatore affermando che essi sarebbero stati necessari al fine di assicurare la conformità al contratto dei contenuti digitali. Peraltro, anche la concreta determinazione dell'ammontare di dati di cui il professionista necessiti al fine di accertare che i contenuti digitali siano conformi al contratto o che essi rispondano alle prescrizioni di legge può, nel caso concreto, creare ulteriori dubbi[27].

In relazione a ciò non è in particolare chiaro se l'elemento della "necessarietà" dei dati per l'adempimento del contratto e/o la loro quantità debbano valutarsi in senso soggettivo (nella prospettiva di colui che mira all'acquisizione di tali dati) oppure in senso oggettivo[28]. In ogni caso, l'elemento della "necessarietà" deve a nostro avviso essere interpretato in misura quanto più possibile restrittiva[29].

4. I dati personali come oggetto del contratto: la necessità di una rilettura, in chiave evolutiva, della nozione di "prezzo" e degli obblighi di informazione precontrattuale

I dati personali rivestono un valore economico sempre maggiore e coloro che mirano all'accesso di beni o servizi sono in misura crescente abituati a "pagare" mediante il consenso al trattamento dei

[26] Cfr. art. 6, comma 1, lett. b della proposta di Regolamento del Parlamento Europeo e del Consiglio relativo al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettroniche e che abroga la direttiva 2002/58/CE.

[27] Cfr. B. Lurger, *Anwendungsbereich*, cit., 36.

[28] Sottolinea tale profilo ad es. V. Mak, *The new proposal*, cit., 9.

[29] Il *considerando* n. 42 GDPR.

propri dati personali piuttosto che per mezzo di denaro[30]. Ciò non significa tuttavia che il soggetto sia consapevole che egli in tal modo stia "pagando", ovvero eseguendo una prestazione a cui è attribuibile un valore economico. Infatti, nella maggior parte dei casi, il consumatore è indotto a considerare tale trasferimento di dati come gratuito.

In considerazione dell'evoluzione della realtà degli scambi, è pertanto particolarmente auspicabile che a livello europeo si giunga ad un'equiparazione del trattamento dei modelli contrattuali in cui una fornitura di beni o servizi venga effettuata verso un corrispettivo in danaro con quelli in cui tale fornitura venga eseguita verso l'autorizzazione al trattamento dei dati personali.

Tuttavia, finora né il legislatore europeo né quello nazionale avevano proposto né tantomeno adottato una disciplina che regolasse lo scambio di prestazioni verso la trasmissione e l'autorizzazione al trattamento di dati personali. La proposta di direttiva della Commissione europea del 9 dicembre 2015 sulla fornitura di contenuti digitali è il primo strumento normativo che si occupa direttamente ed espressamente dello schema negoziale "contenuti digitali verso dati personali". Tale sviluppo merita di essere accolto con particolare favore[31].

Peraltro, nonostante la Commissione europea si sia impegnata, mediante la proposta di direttiva sulla fornitura dei contenuti digitali, ad approfondire e migliorare l'interazione tra la disciplina di tutela dei dati personali e la disciplina relativa ai profili contrattuali aventi ad oggetto la circolazione dei dati stessi, manca un adeguato coordinamento con le regole sulla conclusione dei contratti a distanza e, specificamente, con quelle contenute nella direttiva 2011/83/UE sui diritti dei consumatori, trasposta in Italia negli artt. 45 ss. c.cons.[32].

[30] Il valore medio di un account *Facebook* è stimato in ca. 88 Euro: v. Deutsche Bank Research, *Big Data – Die ungezähmte Macht*, 2014, 20.

[31] V. peraltro i profili critici di tale sviluppo evidenziati dallo European Data Protection Supervisor, *Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content*, 14 marzo 2017, 7.

[32] V. in proposito per tutti G. D'Amico (a cura di), *La riforma del codice del consumo. Commentario al d.lgs. n. 21/2014*, Padova, Cedam, 2015.

In particolare, la DCD non prende in considerazione la disciplina degli obblighi di informazione precontrattuale e merita riprovazione[33] la circostanza che tale aspetto non venga affrontato neppure nella "coeva" proposta di direttiva relativa a determinati aspetti dei contratti di vendita *online* e di altri tipi di vendita a distanza di beni[34].

Peraltro, in relazione al profilo del carattere oneroso della fornitura di contenuti digitali trovano applicazione le disposizioni di recepimento della direttiva 2011/83/UE sui diritti dei consumatori.

Prima che il consumatore sia vincolato da un contratto o da una corrispondente offerta contrattuale, il professionista deve, ai sensi dell'art. 48, comma 1, lett. c e dell'art. 49, comma 1, lett. e c.cons. informare il consumatore in modo chiaro e comprensibile in merito (tra l'altro) al prezzo finale di beni e servizi[35].

Tuttavia, né la direttiva 2011/83/UE né la normativa italiana di recepimento contengono alcuna disposizione che si occupi della nozione di "prezzo". A tale proposito è stato sostenuto che dal contesto della dir. 2011/83/UE sarebbe chiaramente ricavabile che solo una somma di danaro, dovuta al professionista, potrebbe essere qualificata come "prezzo"[36].

In relazione a ciò è particolarmente utile osservare il *considerando* n. 13 DCD, secondo il quale l'applicabilità delle disposizioni della DCD non dovrebbe dipendere «dal pagamento o meno di un prezzo per il contenuto digitale in questione». Alla luce di tale sviluppo sarebbe pertanto a nostro avviso adeguato interpretare in modo evolutivo il concetto di "prezzo" e/o dettarne in proposito una nozione più ampia nell'ambito della direttiva sulla fornitura di contenuti digitali, affinché possa esservi ricompresa ogni prestazione avente un valore economico[37].

[33] In tal senso C. Wendehorst, *Consumer Contracts and the Internet of Things*, in R. Schulze - D. Staudenmayer (a cura di), *Digital Revolution: Challenges for Contract Law in Practice*, Nomos-Hart, Baden-Oxford, 2016, 193.

[34] Proposta di Direttiva del Parlamento Europeo e del Consiglio relativa a determinati aspetti dei contratti di vendita online e di altri tipi di vendita a distanza di beni COM (2015) 635.

[35] F. Rende, *sub art. 48 c.cons.*, in G. D'Amico (a cura di), *La riforma del codice del consumo. Commentario al d.lgs. n. 21/2014*, cit., 108 ss.

[36] C. Wendehorst, *Consumer Contracts*, cit., 193.

[37] Cfr. il *considerando* n. 14 DCD.

In tale contesto si pone il quesito in merito all'applicabilità dell'art. 51, c.cons., che ha recepito in Italia l'art. 8, par. 2, dir. 2011/83/UE sui diritti dei consumatori, norma che prevede una sanzione che si ripercuote sull'essenza stessa di una pattuizione che sia stata conclusa in violazione di determinati "requisiti formali" (*rectius*: obblighi di informazione).

In tal senso, l'art. 51, comma 2, primo periodo, c.cons. obbliga il professionista, in relazione ad ogni contratto distanza stipulato in via elettronica a richiamare – «in modo chiaro ed evidente [...] direttamente prima che il consumatore inoltri l'ordine» – l'attenzione del consumatore agli elementi essenziali del contratto (cfr. art. 49, comma 1, lett. a, e, q, e r, c.cons.). Tale concetto, ed in particolare il concetto di "ordine", dovrebbe considerarsi idoneo a ricomprendere ogni manifestazione di volontà del consumatore volta all'ottenimento di beni o servizi[38].

L'art. 51, par. 2, secondo periodo, c.cons. prevede inoltre che il professionista debba provvedere a che il consumatore, in occasione della manifestazione di volontà destinata all'ottenimento del bene o servizio, confermi espressamente che da tale manifestazione di volontà scaturirà un obbligo di pagamento. In particolare, per il caso in cui l'ordine implichi l'attivazione di un pulsante o di una funzione equivalente, tale pulsante o funzione equivalente dovranno essere chiaramente leggibili e contrassegnati solo dalle parole «ordine con obbligo di pagamento» o da una corrispondente analoga e inequivocabile formulazione, cosicché il consumatore sia posto nelle condizioni di sapere che dall'ordine scaturirà un obbligo di pagamento[39]. La stessa previsione stabilisce inoltre che qualora il professionista non rispetti tale previsione, il consumatore non sarà vincolato dal contratto o dall'ordine.

Anche nell'ipotesi della fornitura di contenuti digitali, che non venga effettuata né gratuitamente né contro il versamento di una somma di denaro, bensì verso il trasferimento di dati personali e la manifestazione del consenso al loro trattamento (che non siano già dovuti per disposizione di legge, secondo quanto dispone l'art. 3,

[38] V. in proposito S. Pagliantini, *sub art. 51 c.cons.*, in G. D'Amico (a cura di), *La riforma del codice del consumo. Commentario al d.lgs. n. 21/2014*, cit., 108 ss.

[39] V. in proposito il *considerando* n. 36, dir. 2011/83/UE.

par. 4, DCD), l'offerente dovrà rispettare gli obblighi contenuti nelle summenzionate disposizioni (tra cui l'obbligo di indicare il prezzo: v. *considerando* n. 50 e art. 49, par. 1, lett. e, c.cons.). Nella misura in cui la fornitura di contenuti digitali debba dunque considerarsi "a titolo oneroso", si applica l'art. 51, par. 2, c.cons.: la disposizione testé menzionata troverà infatti applicazione in tutte le ipotesi in cui il professionista non chiarisca il carattere oneroso del contratto. Alla conseguenza della non vincolatività del consenso al trattamento dei dati personali si potrebbe peraltro giungere anche facendo applicazione dell'art. 7, par. 2 GDPR.

Nell'ipotesi di asserita gratuità, ma di effettiva onerosità della prestazione in ragione della trasmissione di dati personali e dell'autorizzazione al loro trattamento, sarà necessario verificare se nel comportamento del professionista debbano ravvisarsi i caratteri di una pratica commerciale scorretta, in particolar modo di una pratica ingannevole.

5. Conclusioni

Ai dati personali viene riconosciuto un valore economico crescente e gli individui sono sempre più abituati a "pagare", in luogo che con il trasferimento di una somma di danaro, mediante il trasferimento e/o l'autorizzazione al trattamento dei propri dati personali. Ciò non significa tuttavia che colui che a tal fine trasferisca e/o autorizzi il trattamento dei propri dati personali sia consapevole della circostanza che egli stia in tal modo eseguendo una prestazione avente un valore patrimoniale paragonabile a quello proprio di una somma di danaro. Al contrario, colui che, a fronte della fornitura di un bene o di un servizio trasferisce e/o autorizza il trattamento dei propri dati personali, nella maggior parte delle ipotesi ritiene che la controprestazione venga eseguita a titolo gratuito.

Alla luce di tale evoluzione della realtà socio-economica e del crescente valore economico dei dati personali è pertanto particolarmente auspicabile che si giunga in tempi rapidi ad una assimilazione tra il "pagamento effettuato mediante denaro" e i "pagamenti" effettuati mediante il trasferimento e/o l'autorizzazione al trattamento dei propri dati personali. Il modello contrattuale che prevede il pagamento mediante dati personali è infatti una realtà

consolidata nel mondo digitale ed è necessario in proposito delineare un assetto che garantisca l'equilibrio degli interessi delle parti contraenti.

La chiave di volta ai fini dell'inquadramento dei dati personali come oggetto del contratto è l'autorizzazione al loro utilizzo da parte del titolare degli stessi. Peraltro, in ragione dell'insopprimibile esigenza di tutela della persona umana e dei suoi diritti fondamentali – tra cui va annoverato il diritto alla protezione dei dati personali – è necessario garantire il diritto del titolare dei dati personali, che abbia legittimamente manifestato il consenso al loro trattamento, a revocare il consenso stesso.

Il carattere irrinunciabile della facoltà di revoca del consenso al trattamento dei dati personali rende precari gli accordi contrattuali aventi ad oggetto tale consenso e le obbligazioni da essi scaturenti. Esse non sono infatti suscettibili di esecuzione in forma specifica e non giustificano alcuna pretesa al risarcimento del danno, che il "creditore dei dati" abbia a subire in conseguenza di tale revoca. In proposito è pertanto auspicato un chiarimento da parte del legislatore. In considerazione della lacunosità della proposta di direttiva UE sulla fornitura di contenuti digitali, tali incertezze sembrano destinate a protrarsi pur successivamente all'adozione di tale strumento normativo, anche in ragione della circostanza che tale direttiva non intende toccare le disposizioni degli Stati membri in materia contrattuale, quali le norme sulla formazione, validità o efficacia del contratto, comprese le conseguenze della risoluzione del contratto, nella misura in cui gli aspetti in questione non siano disciplinati dalla direttiva stessa.

Per giungere ad una soluzione coerente delle numerose questioni relative ai modelli contrattuali che prevedono lo scambio di beni e servizi verso il consenso al trattamento di dati personali è infatti necessario riflettere sull'impatto sul nostro sistema giuridico della nuova disciplina generale della protezione dei dati personali contenuta nel reg. UE 679/2016, nonché sulla crescente interrelazione tra disciplina relativa alla protezione dei dati personali e diritto delle obbligazioni e dei contratti. Sarà ad esempio necessario effettuare un coordinamento delle nuove previsioni del menzionato regolamento con gli esistenti obblighi informativi precontrattuali, nonché con i criteri di operatività del diritto di recesso. Si rende inoltre opportuno provvedere ad un'interpretazione in chiave evolutiva delle

nozioni di "pagamento" e di "prezzo", al fine di tenere conto delle peculiarità dell'ambiente digitale.

Complessivamente, il diritto delle obbligazioni e dei contratti si trova dinanzi ad un'importante sfida: la capacità di affrontarla adeguatamente e di fornire efficaci soluzioni a nuovi problemi con radici antiche rappresenta un elemento fondamentale al fine di garantire la sinergia tra la nuova disciplina posta a tutela dei dati personali e quella che regola la loro circolazione sul piano contrattuale, assicurando un'effettiva tutela all'individuo e una sempre più piena valorizzazione della persona umana.

L'impatto del trattamento sui diritti e le libertà delle persone fisiche: una valutazione alla luce della giurisprudenza delle autorità garanti italiana e spagnola

Maria Samantha Esposito

Sommario: 1. Il rischio nella disciplina del trattamento dei dati personali – 2. La recente elaborazione del rischio derivante dall'uso dei dati a livello europeo – 3. L'impatto del trattamento nella giurisprudenza delle autorità garanti italiana e spagnola – 4. Conclusioni

1. Il rischio nella disciplina del trattamento dei dati personali

L'approccio tradizionale in materia di analisi e gestione del rischio, nel contesto della tutela dei dati personali, è caratterizzato dall'attenzione rivolta prevalentemente alla dimensione individuale e, in particolare, alla tutela del riserbo e delle informazioni personali inerenti al singolo interessato[1].

[1] Per una puntuale analisi dei diversi scenari tecnologici e normativi susseguitesi nel tempo a partire dall'introduzione dei primi elaboratori elettronici, cfr., A. Mantelero, *Il nuovo approccio della valutazione del rischio nella sicurezza dei dati. Valutazione di impatto e consultazione preventiva (artt. 32-39)*, in G. Finocchiaro (a cura di), *Il nuovo regolamento europeo sulla* privacy *e sulla protezione dei dati personali*, Bologna, Zanichelli, 2017, 287 ss.; Id., *The future of consumer data protection in the E.U. Re-thinking the "notice and consent" paradigm in the new era of predictive analytics*, in *Computer law & Security Review*, 2014, XXX, 647 ss.

L'esame dell'attuale contesto tecnologico e informatico, contraddistinto dalla presenza di innovazioni sempre più complesse, rende, tuttavia, evidenti i limiti derivanti da una simile impostazione, costringendo a riflettere sulla necessità di valutare i nuovi potenziali pregiudizi che possono derivare dall'uso dei dati[2].

In particolare, le nuove tecnologie consentono di raccogliere e analizzare grandi masse di dati (c.d. *Big Data analytic*s), di trarne informazioni di carattere predittivo in merito alle scelte e ai comportamenti degli interessati e di dar luogo a sistemi informatizzati di supporto alle decisioni ed a processi decisionali automatizzati. Tale progressivo ricorso ai dati ed alla loro elaborazione attraverso algoritmi a fini decisionali può condurre a conseguenze negative per i diritti e le libertà fondamentali dei soggetti coinvolti, con riferimento alla libertà di autodeterminazione ed al diritto al rispetto della dignità umana[3].

Nella maggior parte dei casi, inoltre, l'obiettivo principale dell'analisi non è più il singolo e la profilazione dello stesso sulla base dei suoi comportamenti, quanto, piuttosto, la società nel suo insieme o determinate comunità sociali e gruppi di individui. I *software* per l'analisi dei Big Data vengono, infatti, per lo più impiegati per individuare caratteristiche comuni, preferenze o abitudini di una determinata collettività, al fine di predirne i futuri comportamenti ovvero di adottare decisioni che interessano tutta la comunità considerata.

Ciò comporta l'emergere di un interesse rispetto ad un corretto uso delle informazioni raccolte che va al di là dell'individuo e, di conseguenza, l'esigenza di riconoscere, accanto alla dimensione individuale della tutela dei dati, che ha riguardo ai diritti del singolo individuo e alla tutela delle informazioni che lo riguardano, altresì,

[2] In merito ai vantaggi offerti e alle questioni sollevate dall'impiego dei *big data*, cfr., tra gli altri, V. Mayer-Schönberger-Y. Padova, *Regime Change? Enabling Big Data trough Europe's New Data Protection Regulation*, in *Columbia Science and Technology Law Review*, 2016, XVII, 315 ss.

[3] Al riguardo v., altresì, European Union Agency for Fundamental Rights, *Handbook on European data protection law*, 2018, 347 ss., spec. 354, consultabile all'indirizzo: *http://fra.europa.eu/en/publication/2014/handbook-european-data-protection-law-2014-edition*. Con riferimento al rischio di discriminazione derivante dall'uso predittivo delle informazioni cfr., altresì, S. Barocas-A.D. Selbst, *Big Data's Disparate Impact*, in *California Law Review*, 2016, CIV, 671 ss.

una dimensione collettiva. Quest'ultima è legata ai pregiudizi – il più delle volte di natura discriminatoria o invasiva – che possono colpire le categorie di soggetti interessati dal trattamento[4].

Le sfide poste dal trattamento dei dati, inoltre, non riguardano solo forme intensive di trattamento, quali quelle derivanti dall'analisi dei Big Data e dall'impiego di sistemi di intelligenza artificiale, ma anche nuove opportunità ed applicazioni di tecnologie più tradizionali, sovente anche meno costose rispetto alle prime e, di conseguenza, potenzialmente maggiormente diffuse. In questo senso vengono in considerazione, ad esempio, gli strumenti utilizzati per la raccolta di dati di carattere biometrico, i sistemi di videosorveglianza intelligente, i sistemi RFID ovvero i sistemi GPS o, ancora, i *wereable devices*.

In proposito, possono richiamarsi, ad esempio, i sistemi di localizzazione dei veicoli aziendali impiegati nell'ambito del rapporto di lavoro, al fine di rendere maggiormente efficienti determinate attività e/o di garantire la sicurezza dei lavoratori ovvero degli stessi veicoli contro eventuali furti[5].

Tali sistemi, stante la loro capacità di dar luogo a forme di controllo a distanza, possono invero risolversi – anche in considerazione delle modalità con le quali vengono in concreto impiegati – in forme di condizionamento, tali da incidere, tra l'altro, sulla libertà di autodeterminazione e di movimento dei lavoratori[6].

Quanto fin qui osservato mette pertanto in luce i limiti che caratterizzano l'approccio tradizionale in materia di analisi e gestione del rischio e, di conseguenza, l'esigenza di elaborare differenti modelli operativi che tengano conto dei nuovi e più ampi pregiudizi che possono venire in considerazione in occasione di particolari trattamenti.

[4] In proposito, cfr., tra gli altri, A. Mantelero, *Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection*, in *Computer law & Security Review*, 2016, XXXII, 241 ss.

[5] Cfr., *ex multis*, Garante per la protezione dei dati personali, 7 ottobre 2010, doc. web n. 1763071; Garante per la protezione dei dati personali, 4 ottobre 2011, n. 370, doc. web n. 1850581.

[6] In generale, con riferimento al crescente controllo dei lavoratori conseguente al sempre maggior impiego di strumenti informatici nell'ambiente produttivo, cfr., D. Poletti, *Il c.d. diritto alla disconnessione nel contesto dei «diritti digitali»*, in *Responsabilità civile e previdenza*, 2017, I, 8 ss.

2. La recente elaborazione del rischio derivante dall'uso dei dati a livello europeo

L'esigenza di una più ampia interpretazione della nozione di rischio – emersa già da tempo in alcuni contributi dottrinali[7], nonché in diversi progetti H2020 sulla valutazione etica della ricerca e dell'innovazione[8] – sembra aver trovato un primo concreto riconoscimento normativo all'interno del Regolamento (UE) 2016/679.

In proposito, può osservarsi come il profilo del rischio e della sua gestione – senz'altro già elemento essenziale nell'ambito delle diverse normative in materia di protezione dei dati personali – rappresenti un elemento chiave di tutela nel Regolamento, maggiormente incentrato sul principio di *accountability* e di prevenzione del danno[9].

In questo contesto, come confermato dallo stesso Gruppo di Lavoro Articolo 29 per la protezione dei dati, il riferimento ai diritti e alle libertà delle persone, contenuto nel considerando n. 75 e nell'art. 35, nonché in altre disposizioni della nuova disciplina[10], suggerisce una

[7] Cfr., tra gli altri, A.H. Vedder, *Privatization, Information Technology and Privacy: Reconsidering the Social Responsibilities of Private Organizations*, in G. Moore (ed.), *Business Ethics: Principles and Practice*, Sunderland, Business Education Publishers, 1997, 215 ss.; D. Wright-M. Friedewald, *Integrating privacy and ethical impact assessments*, in *Science and Public Policy*, 2013, XL, 755 ss., consultabile all'indirizzo: https://works.depress.com/michael_friedewald/66/; Aa. Vv., *Group Privacy. New Challenges of Data Technologies*, L. Taylor-L. Floridi-B. van der Sloot (eds.), Springer International Publishing AG, 2017; A. Mantelero, *Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection*, cit., 238 ss.

[8] Cfr. Progetto europeo H2020 SATORI "*Stakeholders Acting Together on the Ethical Impact Assessment of Research and Innovation*", consultabile al seguente all'indirizzo: http://satoriproject.eu/; Progetto europeo H2020 Virt-EU "Values and ethics in Innovation for Responsible Technology in Europe", consultabile all'indirizzo: https://virteuproject.eu/

[9] Cfr., G. Finocchiaro, *Introduzione al Regolamento Europeo sulla protezione dei dati*, in *Le nuove leggi civili commentate*, 2017, I, 10; Id., *Il quadro d'insieme sul regolamento europeo sulla protezione dei dati personali*, in G. Finocchiaro (a cura di), *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, Zanichelli, 2017, 12 s.

[10] Cfr., tra gli altri, artt. 24 e 32, Regolamento (UE) 2016/679.

lettura «estensiva» della nozione di rischio, fino a comprendere la dimensione collettiva del potenziale impatto che l'impiego dei dati può comportare[11].

Nello specifico, la nozione di rischio adottata dal nuovo Regolamento sembra consentire di andare oltre il rischio concernente la protezione dei dati e la riservatezza dell'interessato, per ricomprendere ulteriori diritti e libertà fondamentali, quali la libertà di movimento, di pensiero, di coscienza e di religione o, ancora, la libertà da discriminazione[12].

A ciò si aggiunga che, il riferimento a «qualsiasi altro danno economico o sociale», contenuto nel considerando n. 75, assume particolare importanza nell'attuale scenario tecnologico caratterizzato dal largo ricorso all'impiego dei Big Data e dei processi decisionali che sugli stessi si basano, in ragione delle potenziali conseguenze per gli interessati in termini di discriminazione piuttosto che di sicurezza dei dati.

Nonostante il Regolamento (UE) 2016/679 sembri porre le basi per una visione più ampia dei rischi concernenti l'uso dei dati, le previsioni in materia di valutazione e gestione del rischio ivi contenute risultano, tutt'ora, principalmente volte a garantire la sicurezza e la qualità dei dati. In particolare, nel contesto delle disposizioni introdotte dal legislatore europeo, paiono essere carenti strumenti

[11] Cfr., Article 29 Data Protection Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of regulation 2016/679*, adottate il 4 aprile 2017 e da ultimo modificate e adottate il 4 ottobre 2017, consultabili al seguente indirizzo: *http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236* (al riguardo, cfr. le osservazioni di R. Gellert, *The Article 29 Working Party's Provisional Guidelines on Data Protection Impact Assessment*, in *European Data Protection Law Review*, 2017, III, 2, 212 ss.). Per tali osservazioni cfr., altresì, A. Mantelero, *Responsabilità e rischio nel Reg. UE 2016/679*, in *Le nuove leggi civili commentate*, 2017, I, 155; C. Quelle, *The "risk revolution" in EU data protection law: We can't have our cake and eat it, too*, in R. Leenes-R. van Brakel-S. Gutwirth-P. De Hert (eds.), *Data Protection and Privacy: The Age of Intelligent Machines*, Londra, Hart Publishing, 2017, IV, consultabile all'indirizzo *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3000382*

[12] V., Article 29 Data Protection Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of regulation 2016/679*, cit., III.

concreti volti a far fronte alle nuove forme di pregiudizio che possono derivare dall'uso dei dati ovvero al fine di fornire un'efficace risposta sia in termini di tutela dei diversi diritti fondamentali potenzialmente pregiudicati dal trattamento, che di considerazione delle diverse istanze etiche e sociali che possono venire in esame in occasione di particolari trattamenti[13].

Una maggiore e più operativa presa di coscienza di queste istanze è invece emersa sia nelle prime indicazioni del Gruppo di Lavoro Articolo 29 per la protezione dei dati[14] sia, in particolare, a livello di Consiglio d'Europa, laddove un ruolo di sicuro rilievo per una valutazione più ampia del concetto di rischio dev'essere senz'altro riconosciuto alle linee guida sui Big Data recentemente adottate[15].

Preso atto delle nuove questioni sollevate dalle forme di trattamento basate sull'analisi di grandi quantità di dati, le linee guida suggeriscono una valutazione dei rischi che tenga altresì conto del-

[13] Sottolineano i limiti del modello adottato dal legislatore europeo, tra gli altri, A. Mantelero, *Regulating big data. The guidelines of the Council of Europe in the context of the European data protection framework*, in *Computer law & Security Review*, 2017, XXXIII, 588 ss.; V. Mayer-Schönberger-Y. Padova, *Regime Change? Enabling Big Data trough Europe's New Data Protection Regulation*, cit., 331 ss. Le medesime considerazioni riguardano, altresì, i recenti modelli di valutazione di impatto elaborati dall'autorità garante francese: cfr., CNIL, *Privacy Impact Assessment (PIA). Knowledge Bases*, 2018, consultabile all'indirizzo: *https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-en-knowledgebases.pdf*; CNIL, *Privacy Impact Assessment (PIA). Methodology*, 2018, in *https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-1-en-methodology.pdf*; CNIL, *Privacy Impact Assessment (PIA). Templates*, 2018, in *https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-2-en-templates.pdf*

[14] Cfr., Article 29 Data protection Working Party, *Statement on the role of a risk-based approach in data protection legal frameworks*, adottato il 30 maggio 2014, consultabile al seguente indirizzo: *http://194.242.234.211/documents/10160/3815091/WP+218+Statement+risk-based+approach.pdf*

[15] Cfr., Consultative Committee of the Convention for the Protection of Individuals with Regard to automatic Processing of Personal Data, *Guidelines on the Protection of Individuals with Regard to the Processing of Personal Data in a World of Big Data*, Strasburgo, 23 gennaio 2017, consultabili al seguente indirizzo: *https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806ebe7a*, sez. IV, § 2.3. In proposito, cfr., più ampiamente, A. Mantelero, *Regulating Big Data. The guidelines of the Council of Europe in the context of the European data protection framework*, cit., 584 ss.

la dimensione collettiva dell'uso dei dati, nonché delle conseguenze che possono derivare sotto il profilo etico e sociale.

Secondo una simile linea di ragionamento, anche l'*European Data Protection Supervisor* ha sottolineato le diverse questioni etiche che possono venire in considerazione nel contesto, ad esempio, dei *big data*, del *cloud computing*, dell'*Internet of things*, ovvero in occasione dell'impiego della biostampa 3D o delle tecniche di intelligenza artificiale, esortando un generale ripensamento del rapporto tra la tecnologia e i valori umani, al fine di assicurare il più ampio rispetto della dignità individuale[16].

L'ampia riflessione avviata in materia da tale organo ha inoltre condotto l'EDPS alla costituzione di un Comitato consultivo *ad hoc*, con il preciso compito di riconsiderare la dimensione etica dell'uso dei dati[17].

3. L'impatto del trattamento nella giurisprudenza delle autorità garanti italiana e spagnola

Quanto fin qui osservato consente di confermare una generale acquisita consapevolezza dei nuovi e più ampi pregiudizi che possono derivare dall'uso dei dati nell'attuale contesto informatico e tecnologico.

I modelli di valutazione e gestione del rischio risultano, tuttavia, ancora principalmente incentrati sulla tutela della qualità e della sicurezza dei dati, tralasciando, invece, gli aspetti inerenti alla natura degli ulteriori interessi che possono venire in considerazione nel caso concreto e i profili riguardanti la loro specifica tutela.

Se, dunque, sul piano teorico e degli indirizzi di *policies*, si stanno delineando direttrici favorevoli ad una più ampia analisi del rischio, sotto il profilo operativo risulta ancora lacunosa la mappa di quelli che dovrebbero essere in concreto i criteri ispiratori di tale analisi.

[16] Cfr., European Data Protection Supervisor, *Towards a new digital ethics. Data, dignity and technology*, Opinion 4/2015, consultabile al seguente indirizzo: https://edps.europa.eu/sites/edp/files/publication/15-09-11_data_ethics_en.pdf

[17] Al riguardo, cfr., quanto osservato dal Comitato nel suo primo Report: EDPS Ethics Advisory Group, Report 2018, 6 ss., consultabile all'indirizzo: https://edps.europa.eu/sites/edp/files/publication/18-01-25_eag_report_en.pdf

Da qui la necessità di indagare se e come una valutazione maggiormente estesa delle implicazioni del trattamento dei dati, che includa tanto i diritti e le libertà dei singoli quanto le istanze etiche e sociali, abbia già trovato riscontro nella giurisprudenza delle autorità garanti nazionali[18], fornendo così elementi utili all'elaborazione di un più ampio modello di valutazione del rischio[19].

In particolare, la natura relativa dei valori di cui si discute, così come il condizionamento che anche le libertà e i diritti fondamentali ricevono dal contesto sociale, hanno portato a circoscrivere una prima indagine del tema alla giurisprudenza delle autorità preposte alla protezione dei dati personali in Italia e in Spagna, anche in ragione della comunanza e somiglianza che connota gli ordinamenti di tali Paesi, sia sul piano giuridico che dei più ampi valori socio-culturali.

In questo contesto, sono state esaminate oltre 300 decisioni, selezionate mediante il ricorso a parole chiave ritenute maggiormente pertinenti rispetto alla finalità perseguita. Successivamente, sono state individuate le pronunce ritenute più significative, in quanto in grado di rivelare una particolare sensibilità delle autorità garanti verso i diritti e le libertà fondamentali suscettibili di subire un pregiudizio dall'uso dei dati.

Dall'esame delle decisioni considerate è emersa una particolare attenzione da parte delle autorità garanti italiana e spagnola verso la pluralità di valori, diritti e libertà suscettibili di essere coinvolti a fronte di un determinato trattamento di dati personali. Tali autorità, infatti, nel valutare la legittimità di un determinato trattamento, sembrano porre l'accento sui possibili pregiudizi che possono derivare a danno, ad esempio, della libertà di autonomia e di autodeterminazione, dell'identità individuale, dell'integrità

[18] Tale attività rappresenta parte della ricerca svolta nell'ambito del Progetto europeo H2020 Virt-EU, cit., sui valori e l'etica nel contesto delle innovazioni tecnologiche e, in particolare, delle tecnologie IoT.

[19] Al riguardo, cfr., tra gli altri, C. Raab-D. Wright, *Surveillance: Extending the Limits of Privacy Impact Assessment*, in D. Wright D.-P. De Hert (eds.), *Privacy Impact Assessment*, Springer Science+Bussiness Media B. V., 2012, 363 ss.; A. Mantelero, *AI and Big Data: A blueprint for a human rights, social and ethical impact assessment*, in *Computer law & Security Review*, 2018, XXXIV, 754 ss.

fisica, della libertà da discriminazione ovvero della dignità degli interessati[20].

Al riguardo, occorre nondimeno evidenziare che in molte delle decisioni esaminate il riferimento ai diritti e alle libertà fondamentali coinvolti emerge solo implicitamente dalle osservazioni formulate dalle autorità garanti, sebbene non manchino ipotesi in cui tali profili sono espressamente richiamati. Nello specifico, la tutela dei diritti e delle libertà fondamentali è spesso realizzata, da parte delle autorità in esame, mediante il ricorso ai tradizionali principi elaborati nell'ambito della disciplina sulla protezione dei dati personali, senza, dunque, un preciso richiamo al singolo diritto o alla particolare libertà destinati ad assumere rilevanza nel caso concreto. Nelle decisioni delle autorità garanti si rinviene, dunque, il ricorso ai generali principi in materia di trattamento dei dati, quali quello di finalità, di legittimità, di necessità, di trasparenza, di pertinenza e di non eccedenza, onde tutelare, spesso implicitamente, valori diversi da quelli oggetto della disciplina specifica concernente il trattamento dati.

In particolare, è frequente l'impiego del principio di proporzionalità al fine di operare un bilanciamento dei diversi interessi coinvolti nel caso concreto, sebbene tale giudizio si traduca sovente in una enunciazione assiomatica, ove la valutazione di tali interessi non risulta adeguatamente motivata nel contesto delle singole decisioni.

Delineate tali criticità – che complicano la ricostruzione della *ratio* argomentativa delle autorità garanti –, un primo importante interesse che emerge in modo ricorrente nell'ambito delle decisioni esaminate riguarda l'esigenza di tutelare l'autonomia e l'autodeterminazione delle persone soggette al trattamento, presa in considerazione sotto diversi profili. In particolare, nel contesto delle singole decisioni tale libertà è stata declinata come libertà di scelta, di comportamento e di movimento, come libertà di autonomia informativa, come libertà nell'esercizio della professione o, ancora, come libero e armonico sviluppo della persona.

Nello specifico, l'esigenza di tutela dell'autonomia e dell'autodeterminazione del singolo, intesa quale libertà di scelta, di mo-

[20] Cfr. le pronunce delle autorità garanti richiamate *infra*.

vimento e di comportamento, è rinvenibile nell'ambito di quelle decisioni che hanno ad oggetto l'impiego di strumenti in grado di consentire il monitoraggio degli interessati. È il caso, ad esempio, dell'impiego di strumenti di videosorveglianza o di sistemi che consentono la localizzazione (quali, ad esempio, i sistemi GPS ovvero la tecnologia RFID)[21].

In proposito, le autorità garanti hanno evidenziato come tali strumenti siano suscettibili di condizionare i comportamenti e gli spostamenti dell'interessato. In particolare, dalle opinioni espresse al riguardo si evince che, ogniqualvolta gli strumenti impiegati consentano – per loro natura o per le modalità con cui gli stessi vengono utilizzati – di dar luogo a forme di monitoraggio continuo e/o invasivo, gli stessi devono ritenersi suscettibili di limitare le scelte degli interessati; questi ultimi, infatti, in quanto a conoscenza dell'altrui controllo, potrebbero essere portati ad assumere un determinato comportamento solo in quanto ritenuto maggiormente rispondente alle altrui aspettative.

Nel contesto delle decisioni delle autorità garanti in esame, l'ampia nozione di tutela della libertà di autonomia e di autodeterminazione si concretizza, inoltre, anche in termini di autonomia informativa degli interessati.

È il caso, ad esempio, di quei servizi la cui fruibilità da parte degli utenti venga subordinata al previo consenso al trattamento per finalità di marketing. Al riguardo, nel valutare negativamente la legittimità di tali trattamenti, è stato posto in luce, in particolare, come tali pratiche impediscano agli interessati di esprimere liberamente le proprie scelte e le proprie determinazioni in merito all'utilizzo dei dati[22].

[21] Con riferimento all'impiego di strumenti che consentono il controllo dell'attività dei lavoratori cfr., tra le altre, Garante per la protezione dei dati personali, 8 settembre 2016, n. 350, doc. web n. 5497522; Garante per la protezione dei dati personali, 18 aprile 2018, n. 232, doc. web n. 9358266; Agencia Española de Protección de Datos, Expediente n. E/02689/2012. Con riferimento, invece, agli strumenti di videosorveglianza e di localizzazione impiegati al di fuori del contesto lavorativo, cfr., *ex multis*, Garante per la protezione dei dati personali, 7 novembre 2013, n. 499, doc. web n. 2911484; Agencia Española de Protección de Datos, Procedimiento n. A/00109/2017.

[22] Cfr., *ex multis*, Garante per la protezione dei dati personali, 27 ottobre 2016, n. 439, doc. web n. 5687770.

Ancora, la libertà di autonomia e di autodeterminazione è stata intesa, altresì, quale libertà diretta a tutelare l'autonomia delle persone soggette al trattamento nell'esercizio della propria professione.

In questo senso vengono invero in considerazione, ad esempio, i trattamenti effettuati per il tramite dell'installazione di sistemi di videosorveglianza all'interno delle aule didattiche di un asilo nido, in grado di consentire ai genitori un controllo a distanza dei figli durante il loro periodo di permanenza presso la struttura. Con riferimento a tali trattamenti – rispetto ai quali è necessario altresì considerare il grado di autonomia in concreto rimesso al lavoratore nello svolgimento della propria attività – è stata invero evidenziata l'esigenza di tutelare la libertà di scelta dei metodi educativi e d'insegnamento dei docenti coinvolti nel trattamento[23].

La libertà di autonomia e di autodeterminazione è stata infine presa in considerazione rispetto all'esigenza di assicurare adeguata tutela al libero e armonico sviluppo dell'interessato. Questo è emerso, ad esempio, con riferimento al controllo da parte del datore di lavoro delle comunicazioni elettroniche scambiate dai propri dipendenti – effettuate sia nel contesto lavorativo che al di fuori dello stesso – ovvero della navigazione Internet da parte dei medesimi[24]. In questo contesto, nell'ambito delle decisioni esaminate è stato in particolare posto in luce come il controllo delle comunicazioni o del comportamento *online* sia suscettibile di dar luogo a forme di condizionamento, in grado di incidere sui rapporti dell'interessato con gli altri consociati.

Al di fuori del contesto delle comunicazioni, la tutela del libero e armonico sviluppo degli interessati, quale espressione della libertà di autonomia e autodeterminazione ai medesimi riconosciuta, è emersa, invece, nell'ipotesi di diffusione da parte degli organi di informazione di dati riguardanti minori vittime di violenza sessuale[25] ovvero rispetto all'installazione da parte di un hotel di sistemi di

[23] Garante per la protezione dei dati personali, 8 maggio 2013, n. 230, doc. web n. 2433401.

[24] Garante per la protezione dei dati personali, 4 giugno 2015, n. 345, doc. web n. 4211000; Agencia Española de Protección de Datos, Gabinete Jurídico, Informe 0464/2013.

[25] Garante per la protezione dei dati personali, 10 luglio 2008, doc. web n. 1536583.

videosorveglianza diretti a monitorare le aree dedicate al relax dei clienti[26], in quanto attività in grado di incidere negativamente sui rapporti sociali dell'interessato e, in generale, sulla sua vita privata.

L'interesse in esame è stato inoltre preso in considerazione con riferimento all'ipotesi, sopra richiamata, dell'installazione di sistemi di videosorveglianza all'interno di un asilo nido[27], rispetto alla quale, oltre all'esigenza di salvaguardare l'autonomia dell'attività professionale dei docenti, possono venire in considerazione profili inerenti alla tutela del libero e armonico sviluppo dei minori.

Nell'ambito delle decisioni esaminate, le autorità garanti italiana e spagnola hanno posto in luce, altresì, l'esigenza di tutelare l'identità dell'interessato, la quale può subire un pregiudizio, ad esempio, a fronte di trattamenti diretti a raccogliere dati univoci dello stesso. Si tratta, in particolare, di tutti quegli strumenti in grado di individuare e raccogliere informazioni strettamente inerenti all'identità, quali i dati biometrici, che sempre più spesso vengono impiegati – sia nell'ambito del rapporto di lavoro che al di fuori dello stesso – per regolare l'accesso a determinati spazi e servizi.

L'esigenza di porre attenzione al trattamento dei dati relativi all'identità dell'interessato deriva, in particolare, dalla constatazione per la quale tali informazioni sono strettamente inerenti alla persona e, nel caso di dati biometrici o genetici, non facilmente modificabili o immodificabili. Di conseguenza, un eventuale uso abusivo di tali dati è suscettibile di arrecare conseguenze pregiudizievoli a danno dei soggetti coinvolti, come quelle derivanti dall'eventuale furto d'identità[28].

Un ulteriore importante nucleo di interessi e libertà oggetto di particolare attenzione da parte delle autorità nazionali è riconducibile al diritto all'integrità fisica dell'interessato, suscettibile di subire un pregiudizio in occasione di determinati trattamenti. In questo ambito vengono pertanto in considerazione tutti quegli strumenti diretti alla raccolta di informazioni inerenti all'interessato suscettibili di tradursi in forme invasive della sfera fisica dello stesso.

[26] Agencia Española de Protección de Datos, Procedimiento n. A/00109/2017, cit.

[27] Garante per la protezione dei dati personali, 8 maggio 2013, n. 230, cit.

[28] Garante per la protezione dei dati personali, 15 giugno 2006, n. 1306098; Agencia Española de Protección de Datos, Gabinet Juridico, Informe 0392/2011.

Un esempio in tal senso è dato dall'impiego di sistemi RFID mediante l'uso di microchip sottocutanei in grado di incorporare informazioni personali relative ai suoi portatori (quali, ad esempio, i dati necessari per l'identificazione della persona interessata, il numero della carta di credito o le informazioni di carattere sanitario)[29].

In proposito, l'autorità garante spagnola, chiamata a pronunciarsi sulla legittimità di tale trattamento, ha posto l'accento sull'elevato grado di invasività di tali strumenti, capaci di incidere significativamente sulla sfera fisica e personale dell'interessato. Per queste ragioni, l'autorità ne ha limitato l'impiego alle ipotesi in cui non sia possibile il ricorso a strumenti meno invasivi che consentano il raggiungimento delle medesime finalità.

Le decisioni esaminate hanno inoltre consentito di individuare il diritto alla non discriminazione come uno degli elementi che informa le linee argomentative delle autorità garanti.

In proposito, può richiamarsi una pronuncia del Garante italiano avente ad oggetto un trattamento di dati sensibili (in particolare, di quelli idonei a rivelare l'origine etnica o razziale, le convinzioni religiose, lo stato di salute ovvero l'orientamento sessuale) realizzato da parte di un'agenzia di intermediazione immobiliare, al solo scopo di soddisfare determinate esigenze di natura discriminatoria manifestate dai proprietari degli immobili[30].

Infine, un interesse preminente nelle carte dei diritti fondamentali emerso in modo costante nelle decisioni delle autorità garanti è la tutela della dignità dell'interessato.

In questo contesto, possono richiamarsi, ad esempio, i casi dei trattamenti di dati posti in essere mediante l'impiego di strumenti biometrici[31], di quelli in grado di dar luogo a forme di pubblicità della situazione patrimoniale dell'interessato[32] ovvero idonei a rivelare a

[29] Agencia Española de Protección de Datos, Gabinete Jurídico, Informe 0292/2010.

[30] Garante per la protezione dei dati personali, 11 gennaio 2007, doc. web n. 1381620.

[31] Al riguardo, cfr., *ex multis*, Garante per la protezione dei dati personali, 1 agosto 2013, n. 384, doc. web n. 2578547; Agencia Española de Protección de Datos, Gabinet Jurídico, Informe 0065/2015.

[32] Garante per la protezione dei dati personali, 8 giugno 1999, doc. web n. 40369.

terzi l'esistenza di posizioni debitorie[33] o, ancora, l'ipotesi di un trattamento caratterizzato dall'impiego, da parte del datore di lavoro, di tagliandi per consentire l'allontanamento dei dipendenti per necessità fisiologiche[34].

Al riguardo, le autorità garanti hanno in particolare posto in luce come tali trattamenti siano anche suscettibili di dar luogo, a seconda dei casi, a conseguenze di carattere denigratorio o lesive dell'onore personale e/o professionale ovvero della sfera intima dell'interessato.

4. Conclusioni

Sebbene sia possibile rinvenire – sia a livello normativo che dottrinale – numerose istanze in merito alla necessità di guardare ai più ampi rischi inerenti ai diritti fondamentali ed ai profili etico-sociali dell'uso dei dati, i modelli di analisi e gestione del rischio in uso e recentemente elaborati dalle autorità garanti risultano ancora incentrati sulla tutela della qualità e della sicurezza delle informazioni.

In questo contesto, l'esame dell'elaborazione giurisprudenziale delle autorità garanti italiana e spagnola ha invece messo in luce l'emergere di una pluralità di diritti e libertà che vengono in considerazione nel contesto di un determinato trattamento, ben al di là della mera dimensione incentrata su qualità e modalità di trattamento del dato. È inoltre emerso come il frequente ricorso, in sede argomentativa, ai generali principi propri della materia della protezione dei dati personali finisca per mettere in ombra e ad assumere come implicita la tutela di una più vasta gamma di diritti e libertà.

Da quanto sopra emerge, pertanto, la necessità che la tutela dei diritti e delle libertà fondamentali, più volte anche espressamente richiamata nel Regolamento (UE) 2016/679, venga resa maggiormente esplicita e vengano elaborati nuovi modelli operativi volti a rendere il trattamento dei dati personali conforme ad una più ampia

[33] Garante per la protezione dei dati personali, 28 maggio 2015, n. 319, doc. web n. 4131145.

[34] Garante per la protezione dei dati personali, 24 febbraio 2010, doc. web n. 1705070.

gamma di valori ed interessi, sempre più al centro delle aspettative sociali con riferimento all'impiego dei dati personali.

Appare dunque evidente l'esigenza di adottare un approccio più ampio nella valutazione del rischio derivante dall'uso dei dati e l'opportunità di elaborare un modello di analisi e gestione dei rischi che tenga conto, non solo dei tradizionali principi in materia di sicurezza e qualità dei dati, ma, altresì, degli ulteriori valori, diritti e libertà suscettibili di subire un pregiudizio in occasione di un determinato trattamento dei dati personali.

La tutela aggregata dei dati personali nel Regolamento UE 2016/679: una base per l'introduzione di rimedi collettivi?

Federica Casarosa

Sommario: 1. Introduzione – 2. L'attuazione dell'art 80 Reg. 2016/679 in Italia – 3. Valutazioni conclusive

1. Introduzione

Il Regolamento UE 2016/679, recentemente entrato in vigore, è il risultato di un lungo e dibattuto iter di elaborazione a livello europeo che ha portato alla riformulazione della normativa relativa alla tutela dei dati personali alla luce del modificato contesto sociale, tecnico e giuridico che è emerso nei più di venti anni di vigenza della precedente Direttiva 95/46/CE. Durante il periodo di stesura del testo, il legislatore europeo ha fatto proprie numerose istanze di tutela emerse nell'applicazione della direttiva da parte della Corte di Giustizia dell'UE (nel prosieguo CGUE), come per esempio nel caso dell'ambito di applicazione territoriale della normativa, della definizione di dato personale, e del diritto all'oblio. Parallelamente, il Regolamento ha introdotto nuove questioni che la giurisprudenza non ha ancora affrontato, quali per esempio il diritto alla portabilità dei dati, la tutela del consenso del minore, ecc.

Fra i contenuti innovativi del Regolamento vi è anche la norma prevista all'art. 80 in cui si riconosce la possibilità per il titolare dei dati di esercitare i propri diritti anche attraverso un mandato nei confronti di associazioni o organizzazioni senza scopo di lucro che possono rappresentarlo sia nei procedimenti amministrativi

di fronte al Garante, sia nei procedimenti giudiziali di fronte ai tribunali civili.

Questa norma si inserisce all'interno di un più ampio dibattito che ha interessato il tema della tutela collettiva in diversi ambiti giuridici a livello europeo. Recentemente, infatti, non soltanto sono stati pubblicati i risultati della consultazione della Commissione[1] in merito all'applicazione e all'effettività della Raccomandazione 2013/396/UE relativa a principi comuni per i meccanismi di ricorso collettivo di natura inibitoria e risarcitoria negli Stati membri[2], ma proprio su tali risultati la Commissione ha deciso di adottare una nuova direttiva sulle azioni collettive tale da rendere più uniforme ed efficiente il sistema di accesso alla giustizia in caso di violazioni diffuse. Tuttavia, l'ambito di applicazione prescelto dal legislatore in questo caso si è focalizzato nel solo settore della tutela dei consumatori[3].

Dunque, se da un lato, la scelta di promuovere l'adozione di strumenti di tutela aggregata al fine di raggiungere l'effettività della tutela nel caso di interessi diffusi è un approccio già adottato dal legislatore europeo; dall'altro, tale scelta di policy si scontra con un intervento tuttora frammentario, i cui effetti si ripercuotono direttamente sugli strumenti disponibili a livello nazionale[4]. Ciò emerge

[1] Commissione Europea, An evaluation study of the impact of national procedural laws and practices on the equivalence and effectiveness of the procedural protection of consumers under EU law, JUST/2014/RCON/PR/CIVI/0082, reperibile all'indirizzo: *http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=612847*.

[2] Raccomandazione della Commissione dell'11 giugno 2013 relativa a principi comuni per i meccanismi di ricorso collettivo di natura inibitoria e risarcitoria negli Stati membri che riguardano violazioni di diritti conferiti dalle norme dell'Unione, 2013/396/UE, reperibile all'indirizzo: *https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex%3A32013H0396*.

[3] Proposta di Direttiva del Parlamento Europeo e del Consiglio relativa alle azioni rappresentative a tutela degli interessi collettivi dei consumatori e che abroga la direttiva 2009/22/CE, Bruxelles, 11 Aprile 2018, COM/2018/184 final reperibile all'indirizzo: *https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:52018PC0184*.

[4] Relazione della Commissione al Parlamento Europeo, al Consiglio e al Comitato Economico e Sociale Europeo sull'applicazione della raccomandazione della Commissione, dell'11 giugno 2013, relativa a principi comuni per i meccanismi di ricorso collettivo di natura inibitoria e risarcitoria negli Stati membri che riguar-

chiaramente nel caso della protezione dei dati personali, laddove, nonostante vi siano sempre più casi di violazione massiva delle norme di protezione dei dati, la possibilità per i titolari di utilizzare forme di tutela aggregata è disponibile soltanto in alcuni Stati membri[5].

L'approccio adottato dal Regolamento, sfortunatamente, non permette di ridurre tale rischio di frammentazione, poiché la scelta del legislatore non è stata quella di delineare una azione collettiva di matrice europea, quanto piuttosto di definire un diritto europeo all'azione collettiva. In effetti, il Regolamento afferma che il titolare dei dati "ha il diritto di" avviare azioni collettive, senza definire tale strumento, lasciando agli Stati membri la decisione circa le caratteristiche e le norme procedurali da applicarsi.

In assenza di una precisa indicazione normativa nell'attuale quadro previsto dal Regolamento, gli Stati membri hanno ampia discrezionalità. Le opzioni disponibili per i legislatori nazionali sono principalmente due: da un lato, la possibilità di estendere l'applicabilità delle norme preesistenti relative ad azioni collettive anche al settore della protezione dei dati personali; e dall'altro introdurre una nuova normativa che abbia la finalità di qualificare in dettaglio:

- la procedura applicabile, inclusa la legittimazione ad agire;
- gli effetti di tali decisioni;
- il coordinamento fra azioni individuali e 'aggregate', ed infine
- il coordinamento delle azioni di fronte all'autorità garante e ai tribunali.

dano violazioni di diritti conferiti dalle norme dell'Unione (2013/396/UE) Bruxelles, 25.1.2018 COM (2018) 40 final, reperibile all'indirizzo: *https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=COM%3A2018%3A40%3AFIN*.

Agenzia europea per i diritti fondamentali, *Access to data protection remedies in EU Member States*, 2013, reperibile all'indirizzo *http://fra.europa.eu/en/publication/2014/access-data-protection-remedies-eu-member-states*.

[5] In tali casi, peraltro, la normativa applicata è quella dedicata alla tutela del consumatore estesa anche alla tutela dei dati personali, come per esempio nel caso della Francia, dove la cosiddetta *actione de groupe* consente di presentare una azione inibitoria senza tuttavia avere la possibilità di richiedere il risarcimento del danno, si veda A. Biard-R. Amaro, *Resolving Mass Claims in France - Toolbox & Experience*, 2016, reperibile all'indirizzo: *https://www.law.ox.ac.uk/sites/files/oxlaw/france_0.pdf*

Alcuni elementi utili per delineare tali caratteristiche più specifiche possono individuarsi nella giurisprudenza della CGUE, ed in particolare il caso *Schrems II* (C-498/16)[6], laddove la corte non esclude la possibilità per un titolare dei dati, in quanto anche consumatore, di utilizzare gli strumenti della tutela collettiva disponibile a livello nazionale nel caso di azioni di classe (laddove la classe di titolari dei dati hanno la comune caratteristica di essere residente nel medesimo Stato membro).

Il presente contributo sarò dunque dedicato all'analisi degli aspetti procedurali che devono caratterizzare la tutela aggregata alla luce delle indicazioni offerte dalla giurisprudenza europea così da verificare se e come l'attuazione del Regolamento in Italia possa essere il più possibile conforme al più ampio quadro di interventi del legislatore europeo.

2. L'attuazione dell'art 80 Reg. 2016/679 in Italia

L'art 80 Reg. 2016/679 individua tre diverse tipologie di azione:

- un'azione collettiva a base opt-in, in cui gli interessati hanno il diritto di incaricare un ente autorizzato di presentare un reclamo a loro nome, di esercitare le azioni definite negli articoli 77, 78 e 79 del Regolamento;
- un'azione collettiva a base opt-in, in cui gli interessati hanno il diritto di incaricare un ente autorizzato di esercitare il diritto a ricevere un risarcimento solo se la legislazione dello Stato membro lo consente;
- un'azione collettiva a base opt-out, in cui le entità autorizzate sono autorizzate ad agire per conto degli interessati senza aver ottenuto un mandato da tali soggetti in caso di violazione dei diritti di una persona interessata ai sensi del regolamento, a condizione che lo Stato membro abbia previsto tale possibilità. Le richieste di risarcimento sono, tuttavia, escluse da questo meccanismo.

[6] Sentenza della Corte (Grande Sezione) del 6 ottobre 2015 (domanda di pronuncia pregiudiziale proposta dalla High Court (Irlanda) – Maximillian Schrems / Data Protection Commissioner, (Causa C-362/14), GU C 351 del 06/10/2015.

Secondo il decreto legislativo n. 101/2018 recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 approvato dal Consiglio dei Ministri il 10 agosto 2018, il legislatore italiano ha introdotto nell'art. 142 cod. privacy e nell'art. 10 del d.lgs. 150/2011, la possibilità per il soggetto titolare dei dati di dare mandato ad enti del terzo settore per perseguire rispettivamente il reclamo di fronte all'Autorità Garante dei dati personali e il ricorso di fronte al tribunale civile.

Il legislatore italiano, tuttavia, non ha individuato in modo dettagliato le questioni precedentemente elencate, piuttosto ne ha lasciato all'interprete e al giudice la successiva qualificazione. Tuttavia, tale qualificazione non è di agevole soluzione, tanto che potrebbero porsi numerosi dubbi sia di natura sistematica che di natura processuale. Il presente contributo cercherà dunque di evidenziare le questioni ancora aperte, offrendo laddove possibile spunti interpretativi.

2.1. La legittimazione ad agire

L'art. 80 Reg. 2016/679 individua come legittimati ad agire in nome e per conto dei titolari dei dati personali le associazioni e organismi no profit. Al fine di garantire che il soggetto rappresentativo agisca nell'interesse del gruppo tutelato e non per scopi personali, la normativa europea ha imposto criteri reputazionali minimi:

- l'associazione o organizzazione deve essere senza scopo di lucro;
- deve essere regolarmente costituita, secondo le norme nazionali applicabili;
- deve essere attivo nel settore della protezione dei diritti e delle libertà degli interessati con riguardo alla protezione dei dati personali.

Il legislatore italiano ha seguito la medesima definizione riconoscendo legittimazione attiva, secondo il novellato art. 142 cod. privacy e art. 10 del d.lgs. 150/2011, agli enti del terzo settore costituiti ai sensi del d.lgs. 117/2017[7]. Nello specifico, anche il legislatore italiano ha incluso la necessità che tali enti siano attivi nel settore della protezione dei dati personali.

[7] Cfr. art. 16, c. 1 lett. e) e art. 17 c. 1 del decreto legislativo n. 101/2018.

Per quanto affine ad altre norme relative alla rappresentanza di interessi collettivi[8], il terzo requisito incluso nell'art. 80 può essere interpretato in modo restrittivo, poiché in pratica impone all'associazione o organizzazione no profit non soltanto di avere nel suo statuto l'obiettivo di tutela dei dati personali, ma di avere già svolto attività che si riferiscano a tale obiettivo. Da un lato, la scelta del legislatore europeo si muove verso una maggiore garanzia di competenza e di affidabilità dei soggetti legittimati ad agire; tuttavia, tale limitazione può essere problematica laddove, per esempio, l'organizzazione sia stata costituita a tutela degli interessi di altre categorie di soggetti, come per esempio i consumatori o i lavoratori. In questi casi, la protezione dei dati personali dei consumatori o dei lavoratori potrebbe non essere né esplicitamente definita negli obiettivi statutari, né essere stata oggetto di precedente attività. Dunque, potrebbe limitarsi la legittimazione attiva nei confronti di soggetti che possono d'altronde garantire sia la competenza sia la finalità di tutela dei diritti e delle libertà degli interessati.

Sperabilmente, ulteriori elementi saranno offerti dalla decisione della CGUE nel caso *Fashion Id.* (C-40/17)[9] in cui il rinvio della corte tedesca di Düsseldorf include una questione relativa alla legittimazione attiva delle associazioni senza scopo di lucro che si occupino della tutela degli interessi dei consumatori in caso di violazione della normativa sulla protezione dei dati personali.

2.2. La competenza territoriale

Il Regolamento tace sulle norme procedurali da applicarsi in caso di azioni collettive, lasciando al legislatore nazionale piena discrezionalità. Per quanto riguarda il foro applicabile, un'esplicita indicazione proviene dall'art. 79 (2) del Regolamento, dove si prevede espressamente che i ricorsi (individuali) dinanzi alle autorità giurisdizionali

[8] Si veda per esempio l'art. 7 (2) della Direttiva 2000/43/CE del Consiglio, del 29 giugno 2000, che attua il principio della parità di trattamento fra le persone indipendentemente dalla razza e dall'origine etnica, nonché l'art. 4 della Proposta di direttiva relativa alle azioni rappresentative a tutela degli interessi collettivi dei consumatori.

[9] Domanda di pronuncia pregiudiziale proposta dall'Oberlandesgericht Düsseldorf (Germania) il 26 gennaio 2017 – Fashion ID GmbH & Co. KG / Verbraucherzentrale NRW eV, (Causa C-40/17), GU L 281, 31.

debbano essere promossi nello Stato membro in cui il titolare del trattamento o il responsabile del trattamento ha uno stabilimento. In alternativa, tali azioni possono essere promosse dinanzi alle autorità giurisdizionali dello Stato membro in cui l'interessato risiede abitualmente.

Il legislatore italiano ha riprodotto la norma del Regolamento relativa alle azioni individuali applicandola alle norme relative alla competenza territoriale, definendo al novellato art. 10 del d.lgs. 150/2011 che «Sono competenti, in via alternativa, il tribunale del luogo in cui il titolare del trattamento risiede o ha sede ovvero il tribunale del luogo di residenza dell'interessato». Tuttavia, nel prosieguo della norma, il legislatore ha omesso di specificare se e come la stessa debba adattarsi al caso di azioni collettive. Infatti, in caso di plurimi soggetti mandatari rispetto all'ente del terzo settore, potrebbe essere difficilmente applicabile l'alternativa fra competenza del tribunale del luogo di residenza o stabilimento del titolare del trattamento e quella del tribunale del luogo in cui ha residenza l'interessato, poiché per esempio all'azione potrebbero partecipare soggetti aventi residenza in luoghi diversi. Dunque, salvo lasciare all'associazione libera scelta circa il tribunale di residenza di uno o più dei mandatari, potrebbe essere ragionevole interpretare la norma individuando la competenza nel tribunale del luogo di residenza o stabilimento del titolare del trattamento[10].

2.3. Effetti delle decisioni

L'azione collettiva potrà dunque portare ad una decisione che affermi la violazione delle norme relative ai dati personali tale da permettere l'irrogazione di una sanzione amministrativa pecuniaria ovvero il risarcimento del danno nei confronti dei soggetti interessati.

Laddove la condotta del titolare del trattamento sia dunque qualificata come lesiva dei diritti degli interessati mandatari dell'azione collettiva, quali effetti potrà avere tale declaratoria nei confronti dei soggetti che non hanno partecipato all'azione? Alla luce della lette-

[10] Ciò risponde anche ad una analogia rispetto alle norme previste per le azioni collettive a tutela dei consumatori, laddove l'art 140 cod. cons. prevede la competenza territoriale del tribunale del luogo ove è stabilito il professionista.

ra dell'art 80 (2) del Regolamento, appare evidente che il legislatore europeo ha riconosciuto la possibilità che gli Stati membri possano adottare norme che permettano la rappresentanza degli interessi indipendentemente da forme di mandato. Questo permetterebbe, dunque, alle associazioni e organismi no profit di presentare azioni declaratorie della violazione delle norme sulla protezione dei dati personali cui possano seguire azioni c.d. *follow-on* da parte dei singoli consumatori al fine di ottenere eventuale risarcimento circa i danni sofferti in ragione della violazione. Purtroppo, il legislatore italiano ha escluso tale ipotesi consentendo esclusivamente l'opzione di azioni collettive basate sul sistema *opt-in*. In tali casi, la decisione del Garante così come quella del tribunale potrà avere effetto giuridico nei confronti dei soli interessati mandatari dell'azione.

È interessante osservare che nel quadro degli interventi europei relativi alle azioni collettive, un approccio ben più efficace è stato adottato nella proposta di direttiva relativa alle azioni rappresentative a tutela degli interessi collettivi dei consumatori. In questo caso, infatti, l'art. 10 della proposta di direttiva afferma che, in caso di decisione definitiva di un organo giurisdizionale o amministrativo declaratoria, in sede di azione collettiva, della violazione da parte di un operatore commerciale delle norme relative alla protezione dei consumatori, tale decisione costituirà «prova inconfutabile nelle azioni di natura risarcitoria (all'interno dello stesso Stato membro) o una presunzione relativa dell'avvenuta violazione (per le cause intentate in un altro Stato membro)». Appare evidente che in questo caso, il legislatore ha recepito le problematiche sorte a seguito dei casi di violazione occorsi negli Stati membri, primo fra tutti il caso *Dieselgate*, laddove infatti la tutela collettiva degli utenti si è scontrata con la difficoltà di riconoscere degli effetti alle decisioni delle autorità garanti della concorrenza dei singoli stati rispetto alle azioni collettive relative alle medesime violazioni[11].

Tale diverso approccio non è però scevro di conseguenze nell'applicazione pratica, poiché possono ben presentarsi casi in cui vi sia una sovrapposizione fra lo status di consumatore e quello di titolare dei dati personali, così come ha chiaramente dimostrato il caso

[11] Si veda la Proposta di Direttiva relativa alle azioni rappresentative a tutela degli interessi collettivi dei consumatori, in part. p. 7.

Schrems II (C-498/16) di fronte alla CGUE. Per esempio, una azione collettiva focalizzata sulla vessatorietà di clausole contrattuali, quali la c.d. privacy policy annessa come contenuto contrattuale in numerosi termini di servizio per i servizi della società dell'informazione, potrebbe avere la possibilità di garantire sia ai partecipanti all'azione di ottenere il riconoscimento della condotta lesiva dell'operatore commerciale (e in questo caso titolare del trattamento) e conseguentemente il risarcimento per i danni provocati dalla stessa condotta, ma anche permettere ai consumatori che si trovino nelle stesse condizioni contrattuali di utilizzare la decisione quale prova inconfutabile per presentare equivalenti azioni di risarcimento dei danni sofferti[12]. Lo stesso non potrebbe accadere invece nel caso di azioni collettive nei confronti dello stesso operatore commerciale laddove venga contestata la violazione delle norme a tutela della protezione dei dati personali. Dunque, potrebbe emergere una situazione di disparità di tutela giurisdizionale non giustificata da differenze di natura sostanziale rilevanti.

2.4. Coordinamento in caso di azioni paneuropee

Un aspetto specifico sollevato dall'art. 81 del Regolamento è la possibilità che vi sia un coordinamento fra azioni relative alla medesima violazione in più di uno Stato membro. In questo caso il Regolamento prevede una ipotesi speciale di litispendenza[13] secondo la quale in caso di coincidenza della medesima parte processuale (titolare del trattamento o responsabile del trattamento) l'autorità giurisdizionale successivamente adita sulla medesima violazione

[12] N. Helberger-F. Zuiderveen Borgesius-A. Reyna, *The Perfect Match? A Closer Look At The Relationship Between Eu Consumer Law And Data Protection Law*, in *Common Market Law Review*, vol. 54, 2017, 1427-1466.

[13] Si veda l'art. 29 del Reg. 1215/2012 concernente la competenza giurisdizionale, il riconoscimento e l'esecuzione delle decisioni in materia civile e commerciale in cui si afferma in modo analogo che «qualora davanti alle autorità giurisdizionali di Stati membri differenti e tra le medesime parti siano state proposte domande aventi il medesimo oggetto e il medesimo titolo, l'autorità giurisdizionale successivamente adita sospende d'ufficio il procedimento finché sia stata accertata la competenza dell'autorità giurisdizionale adita in precedenza». Tuttavia in questo caso si prevede che vi sia una completa sovrapposizione di entrambe le parti processuali per poter applicare la norma. Si veda T. Bosters, *Collective Redress and Private International Law in the EU*, The Hague, Asser Press, 2017, 145 e ss.

possa sospendere l'azione per poter attendere il risultato del procedimento di fronte all'autorità straniera[14]. Inoltre, il Regolamento riconosce la possibilità alle autorità giurisdizionali di dichiararsi incompetenti, su richiesta di parte, nel caso in cui «l'autorità giurisdizionale adita per prima sia competente a conoscere delle domande proposte e la sua legge consenta la riunione dei procedimenti» (art 81 (3)).

In assenza di una specifica esclusione, tale norma potrebbe avere effetto anche nei confronti di azioni collettive che siano presentate in Stati membri diversi. Tuttavia, in tal caso ancora più ampi diventano i problemi di coordinamento fra i procedimenti, in particolare le questioni dubbie riguardano sia il caso in cui il giudice nazionale decida di sospendere il procedimento, sia il caso in cui il giudice nazionale decida di proseguire nel procedimento. Nel primo caso, dovrebbe valutarsi quali effetti potrebbe avere la decisione transfrontaliera nel procedimento italiano. Nel secondo caso, emergono altrettanti dubbi circa le modalità secondo le quali tali procedimenti simultanei possano proseguire a livello nazionale, tenendo conto di quale influenza potrebbe avere la decisione straniera sul procedimento nazionale.

3. Valutazioni conclusive

Come emerge dalla precedente trattazione, il Regolamento (UE) 2016/679 ha avuto il merito di innovare il settore della tutela giurisdizionale relativa alla protezione dei dati personali con uno nuovo strumento che offre ai titolari dei dati personali la possibilità di coordinare le proprie istanze per ottenere maggiore e migliore accesso alla giustizia attraverso un procedimento unitario per la soluzione di controversie fra loro uniformi. Tuttavia, l'intervento apre squarci problematici sotto diversi punti di vista.

In primo luogo, l'approccio adottato non si discosta dal trend legislativo e giurisprudenziale che caratterizza i recenti interventi del legislatore europeo, che, pur affermando la necessità di tutela effettiva dei diritti di matrice europea, riconosce una gerarchia fra azioni

[14] Si veda anche quanto previsto nel Considerando 144 del Regolamento 2016/679.

di natura individuale e azioni di natura collettiva, riconoscendo un evidente primato alla prima rispetto alla seconda[15].

Inoltre, la completa delega operata dal legislatore europeo nei confronti degli Stati membri rischia di minare gli obiettivi di armonizzazione cui ambiva la riforma operata appunto attraverso la scelta legislativa del regolamento, questo poiché numerosi sono gli aspetti procedurali che possono portare a differenze di protezione sostanziali fra paese e paese.

Infine, come precedentemente descritto, l'assenza di indicazioni in merito a legittimazione attiva, competenza territoriale e soprattutto effetti delle decisioni potrebbe portare a disparità di trattamento fra interessi (collettivi) tutelati laddove si verifichi una sovrapposizione fra soggetti qualificabili come titolare di dati personali e consumatori.

Il legislatore italiano, anche a causa del tempo limitato che è stato dedicato alla definizione dello strumento di attuazione del Regolamento europeo, ha operato una integrazione minimale, consentendo l'ingresso dell'azione collettiva a tutela dei titolari dei dati personali nel nostro ordinamento, senza però predisporre norme di dettaglio che potessero rendere più chiaro all'interprete (e nel caso concreto al giudice) quali norme processuali possano essere applicabili. Sarà dunque probabile che nel prossimo futuro numerosi saranno i rinvii pregiudiziali dei giudici italiani che cercheranno di rendere la disciplina sulle azioni collettive in questo settore più chiara e conforme a criteri uniformi a livello europeo.

[15] F. Cafaggi-F. Casarosa, *L'effettività dei rimedi nelle interazioni giudiziali fra corti nazionali e corti europee*, in P. Gallo-G. Magri-M. Salvadori, *L'armonizzazione del Diritto europeo: Il ruolo delle Corti*, Milano, Ledizioni, 2017, 55-86, part. 76.

GDPR e forme di autoregolamentazione privata: continuità e discontinuità nella disciplina dei codici di condotta

Maria Concetta Causarano

Sommario: 1. Introduzione – 2. GDPR e codici di condotta: quali novità? – 3. Le indicazioni ermeneutiche del Wp29 sui codici di condotta – 4. Il ruolo dei codici di condotta nell'applicazione ultraventennale della direttiva 95/46/CE – 5. Quali c*hecks and balances* per i codici di condotta? Il ruolo della *data protection community* – 6. Codici di condotta e *data consumer law*. La necessità di una prospettiva armonizzata di tutela

1. Introduzione

La disciplina prevista dal regolamento 679/2016/UE costituisce un inedito intreccio tra vecchi e nuovi elementi[1]. Consapevole delle inefficienze applicative e del livello di inadeguatezza della direttiva 95/46/CE rispetto alle sfide tecnologiche attuali[2], il legislatore europeo abbandona il paradigma normativo gerarchico e accentrato (*command-and-control approach*) a questa sotteso per affermare un modello decentralizzato di tutela. Tale mutamento di prospettiva nel GDPR ha portato, di conseguenza, gli strumenti di autoregolamenta-

[1] V. Mayer-Schönberger-Y. Padova, *Regime change? Enabling big data through Europe's new data protection regulation*, in *Columbia Science & Technology Law Review*, 2016, 324.

[2] Considerando 9, reg. UE 2016/679 del 27 aprile 2016.

zione privata sotto i riflettori[3]. Nel tentativo di condensare i risultati raggiunti nell'ultimo ventennio in termini di *self-* e co-*regulation*, il regolamento prevede insieme codici di condotta (art. 40), organismi di controllo (art. 41), certificazioni, sigilli e marchi (artt. 42-43). Si tratta di una scelta giustificata dall'esigenza di restituire un certo grado di flessibilità e semplificazione nella gestione dei rischi e nell'adempimento degli obblighi che il GDPR pone sul titolare del trattamento. Tuttavia, si dubita che l'approccio fiducioso nelle capacità regolative degli attori privati e "sbilanciato" sulla loro autonoma competenza decisionale[4] sia quello più idoneo ad essere impiegato in un contesto normativo che ha per obiettivo la tutela di un diritto fondamentale. Volendo soffermare l'attenzione sui codici di condotta, tale assunto emerge in tutta la sua evidenza. Dietro lo scopo di precisare l'applicazione del regolamento, con l'adozione di un codice *ex* art. 40 GDPR i privati finiscono per co-determinare il contenuto e le modalità di esercizio dei diritti degli interessati riconosciuti dalla nuova regolamentazione europea.

Con il presente contributo si intende approfondire se e in che modo il ruolo riconosciuto ai codici di condotta dal GDPR possa contribuire a tutelare effettivamente il diritto alla protezione dei dati personali. L'analisi sarà articolata in tre parti. Nella prima parte, verranno esaminati, anche tramite le recenti indicazioni ermeneutiche del Wp29 sui codici di condotta, gli elementi di novità contenuti nel regolamento. Nella seconda parte, invece, verrà considerato il ruolo concreto che i codici di condotta hanno avuto sia nella prassi applicativa che nei provvedimenti del Garante e nella giurisprudenza *ante* GDPR. Infine, verranno presentate alcune criticità legate al profilo della *public accountability* dei codici di condotta e verrà proposta una ricostruzione dell'istituto che tenga conto delle possibili sovrapposizioni con altre discipline europee che regolano il mercato.

[3] I. Kamara, *Co-regulation in EU personal data protection: the case of technical standards and the privacy by design standardisation 'mandate'*, in *European Journal of Law and Technology*, 2017, 8.1, 2.

[4] Sulla redistribuzione di competenze decisionali sul diritto alla protezione dei dati nel GDPR, si veda C. Quelle, *Privacy, Proceduralism and Self-Regulation in Data Protection Law*, in *Teoria Critica della Regolazione Sociale*, 2017, 1, 102.

2. GDPR e codici di condotta: quali novità?

Il legislatore europeo fa dei codici di condotta un elemento centrale della nuova *data protection toolbox* contenuta nel GDPR e introduce, rispetto al sistema previsto nella direttiva, una disciplina densa di indicazioni. Innanzitutto, è mutato il modello di regolazione prescelto: i codici di condotta, infatti, divengono propriamente degli strumenti di co-regolamentazione[5]. A dire il vero, la scelta effettuata più di un ventennio fa con l'art. 27 della direttiva era già espressione di un principio di sussidiarietà in senso orizzontale. Tuttavia, se quest'ultimo lasciava spazio eventualmente per un'ipotesi di *self-regulation* pura, adesso – eliminato ogni margine discrezionale circa la possibilità di sottoporre il codice di condotta all'Autorità – l'adozione dei codici viene procedimentalizzata secondo fasi ben scandite.

In secondo luogo, viene mantenuta la funzione di concretizzazione e integrazione dei principi e clausole generali contenuti nella regolamentazione di matrice europea. Tuttavia, i codici diventano per il titolare del trattamento dei dati, nell'ottica del principio di *accountability* di cui all'art. 5.2 GDPR, strumenti di agevolazione della dimostrazione del rispetto del regolamento[6]. Ancora, l'art. 40 GDPR, oltre a contenere al paragrafo 3 un'elencazione non tassativa degli eventuali contenuti, amplia le tipologie di codice che possono essere adottate. Se nella direttiva i codici potevano essere o nazionali o comunitari, nel GDPR si prevede la possibilità di adottare anche codici di condotta aventi efficacia generale all'interno dell'Unione (art. 40.9)[7]. L'adozione di tale ultima tipologia di codici, riconosce un ruolo preminente alla Commissione la quale «può decidere» in modo discrezionale che,

[5] A.R. Popoli, *Codici di condotta e Certificazioni*, in G. Finocchiaro (a cura di), *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, Zanichelli, 2017, 395.

[6] I codici di condotta vengono a tal proposito richiamati in più luoghi del reg. UE 679/2016, in particolare dagli artt. 24.3, 32.5, 35.8, 28.5, 46.2 lett. e), 83.2 lett. i). Per un approfondimento, A.R. Popoli, *Codici di condotta*, cit., 403-404; L. Bolognini, *Codici di condotta*, in L. Bolognini-E. Pelino-C. Bistolfi, *Il Regolamento Privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, Milano, Giuffré, 2016, 430-432.

[7] Sebbene non configurino una categoria autonoma, tale tipologia può rilevare anche in caso di trasferimenti transfrontalieri dei dati ai sensi dell'art. 40.3 GDPR.

tramite l'adozione di atti di esecuzione, i codici ritenuti conformi al GDPR da parte del Comitato europeo per la protezione dei dati possano avere una validità generalizzata in tutti gli Stati membri[8]. Infine, è stata istituzionalizzata la funzione di monitoraggio ed *enforcement* dei codici adottati, funzione che il testo della direttiva formalmente non considerava. Fermi i poteri delle Autorità nazionali, il GDPR assegna tale funzione anche ad organismi di controllo privati che devono essere accreditati secondo i parametri individuati dall'art. 41.2 e specificati dalle Autorità in dialogo con il Comitato europeo, nelle forme del meccanismo di coerenza *ex* art. 63 GDPR.

In sintesi, i codici di condotta dovrebbero configurarsi come un microsistema di regole che si spinge oltre i requisiti normativi di base[9] e la cui adozione deve essere giustificata dalle specifiche caratteristiche del trattamento dei dati nei settori interessati. In tale direzione, è stato sostenuto che sia il codice di condotta sia l'organismo di controllo possono costituire «una sorta di GDPR "parallelo" o, se si preferisce, una forma di applicazione "parallela e a tutela crescente" della normativa generale»[10].

3. Le indicazioni ermeneutiche del Wp29 sui codici di condotta

A differenza di quanto è avvenuto per altri istituti del GDPR[11], l'EDPB non ha ancora pubblicato nessun documento relativo agli artt. 40 e 41

[8] Il ruolo rafforzato della Commissione comporta che il controllo e la misura della partecipazione pubblica alla scelta di estendere l'ambito di applicazione dei codici di condotta adottati, si realizzi nelle forme della procedura di "comitatologia" di cui all'art. 5 reg. (UE) 182/2011 del 16 febbraio 2011, richiamato espressamente dall'art. 40.9 GDPR.

[9] In tal senso i codici di condotta andrebbero inquadrati tra i «voluntary accountability systems that go above and beyond the minimum legal requirements» a cui si riferisce il Wp29 nel descrivere uno dei due livelli dell'architettura normativa dei meccanismi di *accountability*, cfr. Wp29, *Opinion 3/2010 on the principle of accountability* [adottata il 13.7.2010] 00062/10/EN WP 173, 6.

[10] F. Pizzetti, *La protezione dei dati personali e la sfida dell'Intelligenza Artificiale*, in F. Pizzetti (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Torino, Giappichelli, 2018, 154.

[11] In data 30.5.2018 il neoistituito Comitato europeo per la protezione dei dati personali ha pubblicato le *Guidelines 1/2018 on certification and identifying*

del regolamento. Allo stato i titolari e responsabili del trattamento non dispongono di nessuna indicazione ermeneutica ufficiale che possa guidarli nell'interpretazione della nuova disciplina dei codici di condotta. Tuttavia, alcune utili indicazioni possono essere rinvenute nel parere del Gruppo art. 29 sui codici di condotta per il *cloud computing* e nella nota sul progetto di codice di condotta per le applicazioni relative alla salute per telefoni cellulari (cd. *mHealth apps*)[12].

Ai fini del nostro discorso, preme sottolineare in particolare due elementi: la valutazione del "sufficiente valore aggiunto" del codice in sede di redazione e la funzione di monitoraggio e controllo dei codici adottati. Quanto al primo, secondo il Wp29, il codice di condotta, oltre ad essere conforme alle disposizioni di diritto europeo e alle rispettive norme nazionali di adeguamento, deve possedere un «sufficient added value»[13] rispetto a quest'ultime. In altri termini, il codice deve concentrarsi sulle problematiche specifiche legate alla protezione dei dati personali nel settore di riferimento, inserendo in modo chiaro esempi, soluzioni pratiche o raccomandazioni, come emerse anche nel dialogo con gli *stakeholders*. Nessuna indicazione viene fornita sui criteri in base ai quali condurre tale sindacato di "sufficienza", né si prevede la possibilità per i terzi interessati del settore di riferimento di intervenire per manifestare il proprio punto di vista. Tale giudizio resta in definitiva affidato al prudente apprezzamento delle Autorità nazionali e del Comitato europeo, nella fase di negoziazione e revisione dei contenuti del codice con i soggetti promotori.

In particolare, nella nota sulle *mHealth apps*, il Gruppo art. 29 si sofferma poi sulla funzione di monitoraggio ed *enforcement* dei codici di condotta. Si sottolinea la necessità ai sensi dell'art. 40.4 GDPR: di definire in modo chiaro sanzioni concrete e meccanismi di

certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679.

[12] Wp29, Opinion 2/2015 on *C-SIG Code of Conduct on Cloud Computing*, 2588/15/EN WP 232, 2015; *Letter of the Chair of the ART 29 WP re mHealth* del 10.4.2017, consultabile qui: *http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610145* (7 dicembre 2018).

[13] Il criterio del *sufficient added value* per i codici di condotta era già stato indicato dal Wp29 in *Future work on codes of conduct: Working document on the procedure for the consideration by the Working Party of Community codes of conduct*, DG XV D/5004/98, WP 13, adottato il 10.9.1998.

risoluzione alternativa delle controversie; di incrementare l'*information transparency*, rendendo pubbliche le informazioni relative alla violazione del codice e chiarendo le modalità in cui le Autorità nazionali competenti saranno informate delle violazioni; di fornire informazioni sui criteri utilizzati per il monitoraggio periodico.

Sembrerebbe implicita l'idea di creare un sistema autosufficiente di *governance* interna per garantire il rispetto delle regole contenute nel codice e nel regolamento nell'ottica di una *enforced self-regulation*[14]. Si tratta di un sistema in cui l'Autorità pubblica, approvato inizialmente il codice, si limita a svolgere il ruolo di *auditor*, ossia una funzione di monitoraggio e promozione dell'attività di regolamentazione privata[15]. Tuttavia, come si dirà nel prosieguo della trattazione, è il bene della vita che con il GDPR si intende tutelare a rendere inadatta una struttura decentralizzata di tutela, che continua a fare affidamento sull'uso dei codici di condotta.

4. Il ruolo dei codici di condotta nell'applicazione ultraventennale della direttiva 95/46/CE

Nella prassi sviluppatasi nel vigore della precedente disciplina, sia a livello italiano che europeo, i codici di condotta hanno registrato uno scarso successo applicativo. Tralasciando il dato formale inerente all'adozione di un numero esiguo di codici[16], appare utile analizzare

[14] L'espressione è di Ayres e Braithwaite (I. Ayres-J. Braithwaite, *Responsive Regulation*, New York, Oxford University Press, 1992, 102-103) che definivano l'*enforced self-regulation* come «a form of subcontracting regulatory functions to private actors». Tuttavia, nel modello da loro proposto l'interlocutore dell'Autorità pubblica era la singola impresa e non settori o livelli di impresa, come avviene nel modello accolto dal GDPR.

[15] A. Spina, *Alla ricerca di un modello di regolazione per l'economia dei dati. Commento al Regolamento (UE) 2016/679*, in *Rivista della Regolazione dei mercati*, 2016, 1, 149, il quale compie un confronto con alcune discipline in cui la gestione dei rischi è affidata alle imprese.

[16] In ambito europeo, soltanto il cd. codice "FEDMA" nel settore del marketing diretto ha passato positivamente il vaglio del Wp29. In Italia, invece, sono stati adottati ad oggi soltanto sette codici di condotta ai sensi dell'art. 12 d.lgs. 196/2003. Si tratta per di più di "codici di seconda generazione", ossia codici la cui adozione era già stata ritenuta meritevole dal legislatore tramite la previ-

le modalità in cui tali codici sono stati richiamati a livello argomentativo nelle decisioni del Garante per la protezione dei dati personali e nella giurisprudenza.

Limitando l'indagine all'ordinamento interno, com'è noto, il preciso significato giuridico delle regole contenute nei codici di deontologia è sancito dall'art. 12 c. 3 (ora trasfuso nell'art. 2-*quater* c. 4[17]) d.lgs. 196/2003, laddove prescrive che il rispetto dei codici approvati costituisce «condizione essenziale per la liceità e correttezza del trattamento dei dati personali»[18].

Tuttavia, nei provvedimenti del Garante e nelle sentenze più recenti, i codici di condotta non sembrano aver rivestito un ruolo centrale nella tutela dei dati personali. Si riscontra un utilizzo prevalente dei codici, *in primis* quello dei giornalisti e quello per scopi storici, come parametro valutativo non esclusivo, ossia ad integrazione dei principi contenuti nella disciplina generale di riferimento. In tal senso, la giurisprudenza di legittimità, è consolidata nel qualificare i codici come «fonte normativa integrativa dell'ordinamento»[19].

sione di un'autonoma base legale (artt. 102, 106, 139, 117, 118, 135 d.lgs. 196/2003). Per un quadro d'insieme dei codici sino ad ora adottati, cfr. A.R. Popoli, *Codici di condotta*, cit., 377 ss.

La disciplina di riferimento citata contenuta nel d.lgs. 196/2003 è stata, da ultimo, modificata dal decreto legislativo 10 agosto 2018 n. 101 e recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679. A differenza di quanto disposto dal previgente art. 12 d.lgs. 196/2003, il nuovo art. 2- *quater* d.lgs. 196/2003 oltre ad introdurre la nuova terminologia "regole deontologiche", delimita le tipologie di trattamento dei dati per cui il Garante promuove l'adozione concertata di tali regole, richiamando gli artt. 6.1 c) ed e), 9.4, e il Capo IX del GDPR. Si segnala, peraltro, che i codici di deontologia e di buona condotta vigenti al momento in cui si scrive continueranno a produrre effetti ai sensi e nei limiti previsti dall'art. 20 del d.lgs. 101/2018.

17 Così come introdotto dall'art. 2 c. 1 lett. 4) del d.lgs. 101/2018.

18 Per un'attenta analisi della portata giuridica e delle differenze tra tali principi, cfr. E. Navarretta, Sub. *Art. 11*, in C.M. Bianca-F.D. Busnelli (a cura di), *La protezione dei dati personali: commentario al D.lgs. 30 giugno 2003, n. 196*, Padova, Cedam, 2007, I, 251 ss; F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, Torino, Giappichelli, 2016, 266-267.

19 Cass., sez. I civ., sent. 25 giugno 2004, 11864; Cass., sez. III civ., 24 aprile 2008, 10690; Cass., sez. III pen., 16 luglio 2013, 7504 e giurisprudenza cit., in particolare Cass., sez. III pen., 5 marzo 2008,16145: «La fonte necessaria cui attingere la regola

Più rari i casi, invece, in cui i criteri in base ai quali effettuare il sindacato di liceità del trattamento sono stati desunti direttamente dai codici di condotta. A questo proposito, possono menzionarsi una serie di decisioni del Garante in cui è contenuto un esplicito ed esclusivo riferimento alle disposizioni dell'ultimo codice di condotta adottato, quello sull'informazione commerciale, sotto il profilo della liceità e correttezza nella raccolta e conservazione dei dati[20].

Diversi fattori sono stati indicati come determinanti per la scarsa diffusione e utilizzo dei codici di condotta in ambito nazionale ed europeo[21]. Sicuramente, dal punto di vista delle imprese, un ruolo importante ha giocato la circostanza che l'adozione di un codice e dunque l'assunzione di una serie di obblighi ulteriori (il cd. *added value* già richiamato), non era in nessun modo incentivata dall'ottenimento di una qualche forma di vantaggio (*rectius* immunità) nei confronti dell'Autorità competente. Sotto questo profilo, il fatto che il GDPR abbia strettamente legato i codici di condotta al principio di *accountability*, dovrebbe astrattamente funzionare da *efficient nudging element*, ossia alla maniera di una spinta gentile per le imprese verso la loro adozione. L'elaborazione del codice consente, infatti, ai titolari e ai responsabili del trattamento di identificare e delimitare l'area di rischio, specificando le *meta-regulatory obligations*[22] che il regolamento fonda su clausole di ampia formulazione. Al contempo, però, non può escludersi che il codice venga considerato dagli attori privati soltanto un ulteriore adempimento formale del GDPR su base volontaria, che abbia il

di condotta è il codice deontologico, fonte normativa, vincolante, la cui violazione è deducibile nel giudizio di legittimità».

[20] Tra i più recenti, v. provvedimenti del Garante per la protezione dei dati personali del 18 gennaio 2018, 19 ottobre 2017, 12 ottobre 2017. Nel provvedimento del 26 luglio 2017 emblematicamente si legge: «Rilevato che la liceità del trattamento posto in essere dalla resistente deve essere valutato alla luce delle disposizioni contenute nel codice di deontologia e di buona condotta [...] Ritenuto, alla luce di quanto sopra esposto, che appaiano rispettati i presupposti di liceità del trattamento richiesti dal codice deontologico».

[21] A.R. Popoli, *Codici di condotta*, cit., 393-395.

[22] In tal senso si pone il Considerando 98 GDPR. Per un'analisi si veda C. Quelle, *Privacy, Proceduralism,* cit., 101.

vantaggio di creare una sorta di *safe harbour* per il trattamento dei dati effettuato[23]. In sintesi, come si approfondirà nel prossimo paragrafo, suscita non poche perplessità la scelta operata dal legislatore europeo riguardo ai codici di condotta per raggiungere il primo dei due obiettivi indicati dall'art. 1 GDPR: la protezione delle persone fisiche con riguardo al trattamento dei dati personali. E ciò non solo per lo scarso successo di tale strumento già durante il vigore della direttiva ma soprattutto per le caratteristiche legate al modello regolativo sotteso a tale istituto.

5. Quali *checks and balances* per i codici di condotta? Il ruolo della *data protection community*

Secondo una recente lettura, le regole del GDPR sembrano seguire due direttrici: da un lato, il rafforzamento dei diritti dell'interessato, dall'altro, la costruzione di un complesso sistema di *governance* collaborativa tra Autorità pubblica e soggetti privati[24]. A quest'ultima linea di sviluppo devono essere ricondotti i meccanismi formali di co-regolamentazione previsti dal regolamento, di cui i codici di condotta rappresentano l'esempio per eccellenza. Con l'adozione di tali codici, le imprese sono incaricate di co-determinare il contenuto e l'esercizio dei diritti[25] che il regolamento riconosce in capo agli interessati, adattandoli alle specificità dei settori e dei livelli di impresa considerati.

[23] Si dubita, peraltro, che la scelta effettuata dal legislatore italiano *ex* art. 166 d.lgs. 196/2003 (come modificato dal d.lgs. 101/2018), con cui si prevede espressamente l'applicabilità della sanzione amministrativa pecuniaria di cui all'art. 83.5 GDPR anche nel caso di violazione delle regole deontologiche di cui all'art. 2-*quater* d.lgs. 196/2003, possa servire da efficace fattore deterrente volto a favorire una condotta conforme ai codici di condotta approvati. Vedi *infra*.

[24] M.E. Kaminski, *Binary governance: a two-part approach to accountable algorithms*, 2018, 49. Inedito, le bozze sono state consultate per gentilezza dell'Autrice.

[25] Sotto il profilo dell'esercizio dei diritti, cfr. l'art. 40.2 lett. f) e k) reg. UE 2016/679. In tal senso, in ambito nazionale, può citarsi a titolo esemplificativo il c. 4-*bis* aggiunto all'art. 100 d.lgs. 196/2003 dal d.lgs. 101/2018, laddove *expressis verbis* prescrive che: «I diritti di cui al comma 2 (ossia il diritto dell'interessato di rettifica, cancellazione, limitazione e opposizione *ex* artt. 16,17,18 e 21 GDPR) si esercitano con le modalità previste dalle regole deontologiche».

Occorre, tuttavia, interrogarsi sull'opportunità di utilizzare tali strumenti quando l'obiettivo che si intende perseguire sia la protezione di un diritto fondamentale. Il carattere di effettività della regolamentazione privata dal punto di vista pubblico, inteso come capacità di raggiungere risultati socialmente ottimali e accettabili, può divergere notevolmente dalle logiche sottese agli schemi normativi privati[26]. È significativo, in tal senso, che già nel 2001, il Libro bianco sulla *governance* europea conteneva un *caveat* importante riguardo l'utilizzo dello schema regolativo di natura co-regolamentare in presenza di diritti fondamentali, escludendone in modo assoluto qualsiasi utilizzo[27].

In senso critico rispetto a tale deroga assoluta, è stato rilevato, tuttavia, che il sindacato di compatibilità tra gli schemi normativi privati e i diritti fondamentali deve essere effettuato in concreto in relazione al disegno istituzionale che ruota intorno a tali strumenti[28]. In altri termini, la costruzione di un oculato sistema di *checks and balances*, in termini di partecipazione degli *stakeholders* e accesso alla giustizia, renderebbe possibile impiegare i meccanismi di co-regolamentazione anche nei settori in cui viene in rilievo la protezione dei diritti fondamentali[29].

Anche a voler aderire a tale ultima ricostruzione, le nuove regole inserite nell'architettura del GDPR non risultano efficacemente controbilanciate da adeguate forme di partecipazione e controllo pubblico[30]. La responsabilità per il monitoraggio ed *enforcement* delle regole inserite nei codici di condotta non dovrebbe ricadere unicamente

[26] F. Cafaggi-A. Renda, *Public and Private Regulation: Mapping the Labyrinth*, in CEPS *Working Document* n. 370, settembre 2012, 15.

[27] Commissione EU, *La governance europea. Un libro bianco*, 25.7.2001, COM 2001 (428) *final*, 22.

[28] F. Cafaggi, *Prefazione*, in F. Cafaggi (a cura di), *Reframing self-regulation in European private law*, Kluwer Law International, The Hague 2006, xviii.

[29] È significativo che I. Ayres-J. Braithwaite, (in *Responsive Regulation*, cit., p.102) definiscano la *co-regulation* come una procedura tripartita, in cui le associazioni rappresentative dei consumatori o utenti hanno un ruolo paritario in sede di redazione delle regole.

[30] È proprio l'aspetto della cd. *public-facing accountability* che è stato definito uno dei punti più deboli del nuovo Regolamento, cfr. M.E. Kaminski, *Binary governance*, cit., 75.

sulle Autorità di controllo competenti. Quest'ultime, sebbene adesso coadiuvate dall'azione degli istituendi organismi di controllo privati, rimangono dotate di risorse insufficienti per un'azione incisiva a livello generalizzato[31]. Per tale ragione, sarebbe opportuno decentralizzare il più possibile il controllo secondo un modello diffuso, riconoscendo un ruolo attivo alla *data protection community* sia *ex ante* che *ex post* rispetto all'adozione del codice di condotta.

Sotto il primo profilo, occorre considerare che se l'art. 27.2 ultima parte della direttiva poneva sulle Autorità competenti l'onere di raccogliere le osservazioni delle persone interessate o dei loro rappresentanti, tale disposizione non si rinviene più nel testo dell'art. 40 GDPR. L'onere di consultare gli *stakeholders* è, invece, adesso contenuto nel Considerando 99 GDPR, con una modifica però rilevante: la consultazione delle parti interessate rimane affidata alla scelta discrezionale dei soggetti privati impegnati nella redazione del codice[32].

[31] Se si prende in considerazione, per esempio, la dotazione organica del Garante italiano per la protezione dei dati personali e si opera un confronto tra i dati aggiornati al 18 dicembre 2017 e quelli al 1 luglio 2018 (disponibili online sul sito ufficiale del Garante), si osserva un incremento della dotazione organica per l'anno 2018 di 25 unità (da 145 a 170 unità), ma il numero totale del personale è addirittura diminuito (da 127 a 124 unità). In ogni caso, le previsioni mostrano una carenza di visione rispetto alle funzioni che in concreto l'Autorità sarà chiamata a svolgere alla luce delle disposizioni del nuovo GDPR.

[32] Per quanto riguarda l'ordinamento italiano, il neo-introdotto art. 2-*quater* d.lgs. 196/2003, prevede adesso al c.2 che: «Lo schema di regole deontologiche è sottoposto a consultazione pubblica per almeno sessanta giorni», a differenza del previgente art. 12 del medesimo decreto che nulla disponeva a riguardo.
Si tratta di una scelta apprezzabile del legislatore, sebbene occorra coordinare tale disposizione con le regole contenute nell'ancora vigente regolamento n. 2/2006, *Procedura per la sottoscrizione dei codici di deontologia e di buona condotta*, adottato dal Garante per la protezione dei dati personali il 20.7.2006 (G.U. n.183 dell'8.8.2006). Gli articoli 6 e 7 del predetto regolamento prevedono, infatti, che le osservazioni pervenute nella fase di consultazione pubblica devono essere esaminate e trasmesse ai soggetti rappresentativi o interessati per le valutazioni del caso e sulla base di queste deve essere redatto lo schema finale di codice da trasmettere al Garante. Di conseguenza, per il momento, non esiste alcuna garanzia che i rilievi emersi durante la fase di consultazione pubblica siano poi trasfusi nello schema finale di codice sottoposto al Garante unicamente per l'approvazione.

Quanto alle forme di controllo successivo, invece, il GDPR introduce all'art. 80 dei meccanismi di esercizio del diritto degli interessati di proporre reclamo all'Autorità di controllo o di presentare un ricorso giurisdizionale da parte di associazioni senza scopo di lucro, che siano attive nel settore della protezione dei dati personali. Tuttavia, l'art. 80.2 lascia alla discrezionalità degli Stati membri la scelta di riconoscere a tali enti esponenziali un'autonoma legittimazione ad agire nel caso cui si ritenga che i diritti di cui l'interessato goda a norma del regolamento siano stati violati. In modo poco prudente, si fa dipendere dalla sensibilità dei singoli ordinamenti la possibilità di ampliare le modalità di tutela effettiva dei diritti dell'interessato[33]. Non vi è dubbio, infatti, che qualsiasi scelta in senso negativo costituirà un'occasione mancata verso la possibilità di estendere il dialogo sul sistema di *governance* collaborativa sotteso al GDPR anche ad altri soggetti rispetto allo Stato e al mercato, ossia alla società civile e alle corti.

6. Codici di condotta e *data consumer law*. La necessità di una prospettiva armonizzata di tutela

Occorre accantonare per un momento il binomio codici di condotta-protezione dei dati personali e considerare tali strumenti alla luce dell'altra finalità di cui all'art. 1 GDPR, ossia quella della libera circolazione dei dati. Si può osservare, a tal proposito, come la logica di *market regulation* sottesa al regolamento si identifichi con la promozione della fiducia degli utenti nel mercato digitale[34]. Ma lo

[33] L'EDPS, di recente, ha invitato gli Stati membri ad attuare efficacemente tale disposizione, sottolineandone l'assoluta rilevanza, cfr. EDPS, Opinion 3/2018 *on online manipulation and personal data*, adottata il 19 marzo 2018, 22.
La scelta del legislatore italiano (art. 17 del d.lgs. 101/2018 che ha modificato l'art. 10 del d.lgs. 150/2011), tuttavia, è stata quella di recepire soltanto quanto previsto dall'art. 80.1 GDPR.

[34] Si leggano in tal senso, il Considerando 7, reg. UE 2016/679, ma anche la Comunicazione *Strategia per un mercato digitale in Europa*, COM (2015) 192 *final*, 16; la Comunicazione *Costruire un'economia dei dati europea*, COM (2017) 9 *final*, 3; la Comunicazione *Verso uno spazio comune europeo dei dati*, COM (2018) 232 *final*, 1. Sulla rilevanza del principio di fiducia, F. Pizzetti, *La protezione dei dati personali*, cit., 170.

strumento ritenuto congruo dal legislatore europeo per la realizzazione di tale obiettivo è quello di avere a sua volta fiducia negli attori del mercato stesso.

D'altronde è proprio quanto avviene con i codici di condotta. Se da una parte, come si è visto, il giudizio di compatibilità di quest'ultimi rispetto al diritto alla protezione dei dati si risolverebbe in senso negativo, altrettanto non può dirsi se si considerano i codici nell'ottica dello sviluppo del mercato digitale e della fiducia degli utenti. Tradizionalmente, infatti, i codici di condotta hanno rappresentato uno strumento regolativo ricorrente nelle discipline di derivazione europea che sono intervenute sul mercato. In particolare, il codice è stato configurato quale mezzo d'informazione e di agevolazione delle scelte commerciali dei consumatori al fine di accrescere la fiducia negli *standard* di correttezza e diligenza professionale[35]. L'inserimento dei codici di condotta all'interno del GDPR sembrerebbe porsi in linea di continuità con tale obiettivo. D'altronde, deve rilevarsi come in tempi recenti, nel dibattito sull'economia digitale e specialmente sulla creazione di un mercato europeo dei dati, si sta affermando tra gli studiosi la necessità di approfondire la relazione tra diritto del consumatore e diritto della protezione dei dati personali. Complice il dibattito sui cd. *free online services*[36], si è preso atto che la raccolta e il trattamento dei dati non incide soltanto sui diritti dell'interessato, titolare del diritto alla protezione dei dati personali, ma anche sui diritti del consumatore[37]. La comunanza dei rischi per i diritti tutelati da tali discipline sul piano fattuale dovrebbe ragionevolmente trovare una certa omogeneità in termini di tutela sul piano normativo.

[35] Si pensi, in tal senso, alla dir. 2000/31/CE e dir. 29/2005/CE. Per un approfondimento, cfr. G.L. Fusco, *Codici di autoregolamentazione, uso della rete e informazione dell'utente*, in M. Nuzzo (a cura di), *Il Principio di sussidiarietà nel diritto privato*, Torino, Giappichelli, 2014, 218 ss.

[36] Dibattito culminato da ultimo con la proposta di Direttiva *per una migliore applicazione e modernizzazione del diritto del consumo*, COM (2018) 185 *final*, pubblicata insieme alla Comunicazione *Un new Deal per i consumatori*, COM (2018) 183 *final*, dell'11 aprile 2018.

[37] Per una lucida ricostruzione delle sovrapposizioni tra le due discipline, cfr. N. Helberger-F.Z. Borgesius-A. Reyna, *The perfect match? A closer look at the relationship between EU consumer law and data protection law*, in *Common Market Law Review*, 54, 2017, issue 5.

In tal senso, per esempio, l'adesione da parte di un'impresa – che offre un servizio online connesso al trattamento di dati personali degli utenti – ad un codice di condotta, rileva per l'applicazione sia della disciplina posta a tutela del consumatore sia delle regole del GDPR. Di conseguenza, l'eventuale violazione delle regole del codice, sussistendone i rispettivi presupposti, potrebbe al contempo qualificarsi quale pratica commerciale ingannevole ai sensi dell'art. 6.2 lett. b) della direttiva 2005/29/CE[38] e quale indice dell'inottemperanza agli obblighi di cui agli artt. 5.2. e 24.3 GDPR. Privilegiando un approccio che mira alla pluriqualificazione della condotta dell'impresa responsabile, si favorisce un processo osmotico di armonizzazione del quadro di tutela previsto dalle discipline interessate. Si realizzerebbe, in definitiva, un ampliamento delle modalità di accesso ai rimedi da parte del consumatore-soggetto interessato dal trattamento, contribuendo all'effettività degli interessi che si intendono proteggere[39]. È significativo, peraltro, come l'opportunità di adottare una prospettiva coordinata d'azione venga sollecitata da più parti e primariamente da quelle Autorità che svolgono il ruolo di *whatchdog* della protezione dei dati a livello europeo. Nei documenti più recenti, il Wp29 e il Garante europeo dei dati personali invitano, infatti, ad un maggiore coordinamento tra discipline[40] nell'ambito della *data consumer law*.

In conclusione, la scelta di dare continuità nel nuovo GDPR all'impiego dei codici di condotta può considerarsi un *regulatory paradox*[41].

[38] E ciò per l'ampiezza della definizione di codice di condotta di cui all'art. 2.1 lett. f) dir. 29/2005/CE. Più complessa, invece, la sovrapposizione con i codici di condotta previsti dall'art. 16 dir. 2000/31/CE, dato che la regolamentazione sul commercio elettronico indica, in modo simile al GDPR, i possibili contenuti di tali codici, mentre dall'altro lato non prende espressamente alcuna posizione sull'eventuale violazione delle regole contenute nel codice.

[39] Peraltro, anche l'efficacia dei codici previsti dalla disciplina sulle pratiche commerciali sleali potrebbe trarre beneficio da tale prospettiva metodologica integrata dato che, anche in tale settore, i codici di condotta non hanno sortito gli effetti sperati per la tutela dei consumatori. Sul punto si veda C.M.D.S. Pavillon, *The interplay beetween the unfair commercial practices directive and codes of conduct*, in *Erasmus Law Review*, 2012, 5, issue 4.

[40] Cfr. Wp29, *Letter of the Chair*, cit., 2.; EDPS, Opinion 3/2018, cit., 20.

[41] M.E. Kaminski, *Binary governance*, cit., 44.

Da un lato, le caratteristiche intrinseche dei codici, li rendono forse tra i mezzi regolativi più adeguati ad intervenire in ambiti legati allo sviluppo delle nuove tecnologie e del mercato digitale; dall'altro, però, questi strumenti si rivelano tra i meno adatti, nella prospettiva di tutela di un diritto fondamentale, qual è la protezione dei dati personali.

De jure condito, l'effettività di tale diritto rispetto ai codici di condotta dipenderà in gran parte dalla ricostruzione in via ermeneutica, all'interno della cornice del GDPR, di un sistema di *checks and balances* volto all'ampliamento degli spazi di partecipazione e controllo dei soggetti interessati e dal coordinamento con le altre discipline poste a tutela del mercato e dei consumatori.

L'impatto del Regolamento generale sulla protezione dei dati sul sistema punitivo a livello eurounitario e sovranazionale

Enrico Cottu

Sommario: 1. Il Regolamento come strumento di armonizzazione sanzionatoria. La sanzioni amministrative pecuniarie – 2. I restanti poteri correttivi: misure o sanzioni non pecuniarie dissimulate? – 3. Il possibile concorso di ulteriori sanzioni a livello nazionale e il problema del *ne bis in idem* – 4. La tormentata riforma delle fattispecie penali speciali a protezione dei dati personali

1. Il Regolamento come strumento di armonizzazione sanzionatoria. La sanzioni amministrative pecuniarie

Con l'approvazione del regolamento 2016/679, la disciplina europea della protezione dei dati ha finalmente conosciuto, anche sotto il profilo dell'apparato sanzionatorio, un'evoluzione parallela a quella propria dell'ambito sostanziale del trattamento.

In precedenza, un orizzonte di armonizzazione in materia di sanzioni era rimasto escluso dalla prospettiva comunitaria. La precedente direttiva 95/46/CE, infatti, si limitava a indicare agli Stati il dovere di stabilire e adottare, tra le «misure appropriate per garantire la piena applicazione delle disposizioni della presente direttiva»

altresì «le sanzioni da applicare in caso di violazione delle disposizioni di attuazione» (art. 24)[1].

L'inadeguatezza del conseguente assetto, tuttavia, è risultata particolarmente evidente, messa alla prova di aggressioni "di massa" ai dati personali, realizzate su scala internazionale e attraverso standard unilateralmente definiti, ma affrontate in maniera fortemente differenziata da parte delle Autorità dei vari Stati membri. Paradigmatici, sotto questo profilo, i casi che hanno interessato *Google LLC*: dapprima, in relazione alle intrusioni verso terzi nell'ambito della banca dati del servizio *street view*[2]; successivamente, per l'inadeguatezza della *privacy policy*, in rapporto alle ampie facoltà di conservazione e utilizzo riservatesi dalla multinazionale sulle informazioni raccolte dagli utenti dei propri numerosi servizi[3]. In entrambi i casi, si è registrata entro i confini dell'Unione una notevole frammenta-

[1] Cfr. P. Church-C. Millard, *Comments to Directive 95/46/EC*, *sub* art. 24, in A. Bullesbach-Y. Poullet-C. Prins (a cura di), *Concise European IT Law*, Alphen a/d Rijn, 2010, 110 e ss.

[2] Per realizzare questo servizio (che «fornisce viste panoramiche a 360° in orizzontale e a 160° in verticale lungo le strade (a distanza di 10-20 metri l'una dall'altra) e permette agli utenti di vedere parti di varie città del mondo a livello del terreno»; così l'omonima voce su *wikipedia.org*) sono state impiegate apposite vetture (*Google car*) attrezzate per ottenere la copertura fotografica del percorso, non esclusi i soggetti eventualmente presenti al momento della ripresa, ritratti in immagini universalmente diffuse. Con provvedimento del 15 ottobre 2010 il Garante italiano ha imposto di adottare le misure necessarie per rendere le vetture riconoscibili e comunque informare del loro passaggio (doc. web n. 1759972, in *www.garanteprivacy.it*). Inoltre, è emerso come durante il percorso le *Google car* raccogliessero, accidentalmente, dati relativi alla presenza di reti Wi-Fi e frammenti di comunicazioni elettroniche trasmesse dagli utenti su reti Wi-Fi non protette (c.d. *payload data*). Per ulteriori riferimenti, v. M. Burdon-A. McKillop, *The Google Street View Wi-Fi Scandal and its Repercussions for Privacy Regulation*, in *Monash University Law Review*, 2013, 702-738. In Italia, il Garante (a seguito di segnalazione provenuta dalla stessa Google) ha ingiunto il blocco del trattamento dei dati così raccolti con provvedimento del 9 settembre 2010 (cfr. doc. web n. 1750529).

[3] In questo caso, l'inadeguatezza della *policy* era stata stigmatizzata una lettera del 10 ottobre 2012 indirizzata a Google dal Gruppo di lavoro comune istituito sulla base dell'art. 29 della direttiva (WP 29) composto dall'insieme della autorità nazionali di protezione dei dati, accompagnata da una specifica appendice di raccomandazioni per conformare la *policy* alla normativa europea.

rietà e disomogeneità, in relazione sia alla tipologia dei fatti sanzionati che alla natura ed entità delle sanzioni adottate[4].

Con netta soluzione di continuità, il regolamento si occupa ora (dedicandovi un apposito Capo) di delineare più compiutamente la reazione punitiva alle violazioni dei propri precetti, anzitutto predisponendo uno strumento sanzionatorio comune per le Autorità di controllo e protezione dei dati personali degli Stati membri[5].

Essendo assistite dalla diretta applicabilità propria di tale fonte del diritto, le relative disposizioni appaiono di per sé idonee, dal momento della presa di efficacia del regolamento, a fondare una piena pretesa punitiva nei confronti dei singoli. Tuttavia, nonostante il carattere apparentemente autosufficiente di tale microsistema normativo, è necessario evitare la "illusione ottica" di una

[4] La sanzione comparativamente più elevata nei confronti *corporation* (un milione di euro) è stata irrogata dal Garante italiano per la sola lesione della privacy dei soggetti ritratti nell'ambito di *street view* (cfr. il provvedimento di ordinanza ingiunzione n. 583 del 18 dicembre 2013, in www.garanteprivacy.it [doc. web n. 2954309]); non risultano invece sanzionate, in Italia, le criticità riscontrate nella *privacy policy* aziendale (v. nota precedente), oggetto invece di repressione in altri paesi, per somme nettamente più contenute (v. F. Laugée, *Protection des données personnelles: Google à l'amende en Espagne et en France*, in *La Revue Européenne des Médias*, hiver 2013-2014, n. 29, 20 ss.). In Germania, la sanzione di 145.000 euro per la raccolta illegale di dati tramite Wi-Fi realizzata dalle *Google car* (pur quasi corrispondente al massimo di legge) è immediatamente parsa del tutto inadeguata alla gravità del caso (v. C.C. Miller, *Stern Words, and a Pea-Size Punishment, for Google*, in *New York Times*, 22 aprile 2013); in Regno Unito, sulle medesime condotte, una discussa decisione dell'*Information Commissioner's Office* ha invece evitato di fare uso dei propri consistenti poteri sanzionatori (sino a 500.000 £) limitandosi a ingiungere la distruzione dei dati raccolti. Cfr. C. Williams, *Google escapes fine over Street View Wi-Fi snooping*, in *The Telegraph*, 21 giugno 2013.

[5] La portata armonizzatrice sanzionatoria dell'atto è connessa alla acquisizione di un rilievo ultraindividuale della protezione dei dati personali da A.G. Parisi, *Responsabilità e sanzioni*, in S. Sica-V. D'Antonio-G.M. Riccio (a cura di), *La nuova disciplina europea della privacy*, Milano, 2016, 310, per la quale «Dal quadro sanzionatorio appena delineato emerge ancora una volta la prospettiva diversa della disciplina regolamentare al paragone di quella predisposta dalla direttiva 95/46: quest'ultima è diretta a tutelare, di volta in volta, il singolo nei confronti del titolare del trattamento; il Regolamento mira invece a sanzionare severamente i trattamenti illeciti, in una prospettiva ben più ampia della visione centrata sulla tutela dell'interessato, in quanto rivolta alla salvaguardia dell'intera collettività [...]».

disciplina sanzionatoria unificata; questa, invero, si sarebbe potuta raggiungere se l'Unione avesse optato di esercitare la propria competenza, oltre che con la previsione di norme comuni, riservandosi le fasi di istruttoria e irrogazione delle sanzioni e lasciando agli Stati membri unicamente la fase esecutiva[6]. L'opzione per un modello "decentrato" implica per contro, che ogni Autorità di controllo debba naturalmente fare riferimento, in sede applicativa, alla disciplina generale sull'illecito amministrativo del rispettivo ordinamento nazionale[7].

Nella nuova disciplina comune, assumono rilievo primario le sanzioni amministrative pecuniarie di cui all'art. 83 (*amendes*, *fines* nelle versioni francese e inglese del testo), corredate da una ricca serie di parametri applicativi. Appare opportuno, al riguardo, procedere a una sintetica disamina dei profili contenutistici maggiormente peculiari[8].

Le suddette sanzioni risultano applicabili a un ampio novero di infrazioni delineato, nei paragrafi da 4 a 6 dell'art. 83, mediante la tecnica del rinvio interno, con copertura virtualmente completa de-

[6] Cfr. *amplius* A. Bernardi, *Politiche di armonizzazione e sistema sanzionatorio penale*, in T. Rafaraci (a cura di), *L'area di libertà sicurezza e giustizia*, Milano, 2007, 227-228.

[7] Per l'ordinamento italiano, questo aspetto è reso palese dall'art. 166, comma 8 del d.lgs. n. 196/2003 (come da ultimo novellato dal d.lgs. n. 10 agosto 2018, n. 101) per cui «Nell'adozione dei provvedimenti sanzionatori nei casi di cui al comma 4 si osservano, in quanto applicabili, gli articoli da 1 a 9, da 18 a 22 e da 24 a 28 della legge 24 novembre 1981, n. 689». Nella precedente versione, lo stesso art. 166 operava un rinvio globale (pur sempre «in quanto applicabili») alle disposizioni della l. 689/1981. Tale disciplina peraltro può anche mancare del tutto, senza che dal regolamento subentri obbligo di introdurre tale strumento, come conferma la lettura del considerando 151 relativo a Estonia e Danimarca.

[8] In argomento: A.G. Parisi, *op. cit*., 289 ss.; I. Bistolfi-L. Bolognini, *Le sanzioni*, in I. Bistolfi-L. Bolognini-E. Pelino, *Il Regolamento Privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, Milano, 2016, 685 ss.; M. Ratti, *Il regime sanzionatorio previsto dal Regolamento per l'illecito trattamento dei dati personali*, in G. Finocchiaro (dir. da), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, 2017, 595 ss.; R. Schwartmann *et al*., *Rechtsbehelfe*, *Haftung und Sanktionen*, in R. Schwartmann-A. Jaspers-G. Thüsing-D. Kugelmann (a cura di), *Heidelberger Kommentar - Datenschutz-Grundverordnung mit Bundesdatenschutzgesetz*, München, 2018, spec. 1363 ss.

gli obblighi sorgenti dal regolamento. A fronte di questa variegata tipologia di comportamenti illeciti, vengono previsti due scaglioni di importo massimo di sanzione pecuniaria (10 milioni e 20 milioni di euro)[9]; il che pare sottendere una differenziazione per grado di disvalore operata già in astratto dal Legislatore europeo. L'entità davvero minimale di questa suddivisione, peraltro, suscita qualche perplessità. Una maggiore articolazione interna degli scaglioni suddetti, unita a uno sforzo di più analitica enucleazione e descrizione delle rispettive categorie di condotte, avrebbe verosimilmente consentito una maggiore gradualità e determinatezza della risposta repressiva, apprezzabili sia in termini di rispetto del principio di proporzionalità sia di prevedibilità delle conseguenze della condotta illecita (e, quindi, di orientamento normativo delle regole presidiate)[10].

Dal punto di vista soggettivo, le sanzioni introdotte dal regolamento puniscono "illeciti amministrativi propri" e, pertanto, possono riferirsi tanto a persone fisiche che ad enti pubblici o privati che rivestano, ai sensi del regolamento, il ruolo di titolari e/o responsabili del trattamento dei dati personali. Il regolamento, tuttavia, se non impone, nemmeno appare incompatibile con un ampliamento della responsabilità a collaboratori "esterni" del soggetto qualificato[11].

La natura del soggetto sanzionato, peraltro, è suscettibile di influire significativamente sulla dosimetria sanzionatoria. Nei confronti delle sole imprese, infatti, è previsto che l'importo della sanzione

[9] A. Ciccia Messina, *GDPR: un sistema sanzionatorio a due livelli*, in *IPSOA Quotidiano*, 28 maggio 2018, 13 ss.

[10] Difatti, se è tendenzialmente vero che «sanzioni sono più gravi nelle ipotesi di violazione dei diritti dell'interessato» (F. Costantini, *Il Regolamento (UE) 679/2016 sulla protezione dei dati personali*, in *Il lavoro nella giurisprudenza* n. 6/2018, 552) è anche vero che la medesima soglia di gravita massima è prevista nel caso di violazione a «qualsiasi obbligo ai sensi delle legislazioni degli Stati membri adottate a norma del capo IX» (lett. d) o «l'inosservanza di un ordine, di una limitazione provvisoria o definitiva di trattamento o di un ordine di sospensione dei flussi di dati dell'autorità di controllo ai sensi dell'articolo 58, paragrafo 2, o il negato accesso in violazione dell'articolo 58, paragrafo 1» (lett. e).

[11] Nell'ordinamento italiano potrebbe quindi trovare applicazione la disciplina sul concorso di persone nell'illecito amministrativo dettata all'art. 5 l. 689 del 1981 (cfr. *supra*, nota 6).

irrogata possa arrivare sino a una percentuale del «fatturato mondiale annuo dell'esercizio precedente» (due per cento per le violazioni meno gravi, quattro per cento per le altre)[12]. Rispetto agli operatori economici, pertanto, a ben vedere non sussiste un massimo edittale prefissato, essendo l'importo massimo ricavabile unicamente in forma proporzionale (e a posteriori) rispetto ai ricavi societari[13].

D'altro canto, le nuove sanzioni pecuniarie, sebbene dotate di "tetto massimo", non incontrano alcun limite verso il basso. Difatti per nessuna infrazione, indipendentemente dalla categoria di appartenenza, esiste una soglia minima di importo della sanzione pecuniaria irrogata[14]. Ciò determina la possibilità per le sanzioni di oscillare, in concreto, tra valori diversissimi lungo lo spettro consentito dagli elevati massimali.

A guidare una fase commisurativa, conseguentemente, assai pregnante, viene allegata una fitta serie di "circostanze" attenuanti o aggravanti la responsabilità e, quindi, la sanzione inflitta[15]. Rima-

[12] Sotto questo profilo il regolamento sembra aver preso a modello la «dissuasività delle efficaci sanzioni *antitrust*» (A. Pisapia, *La tutela per il trattamento e la protezione dei dati personali*, Torino, 2018, 122). Il modello seguito sarebbe in particolare quello dei poteri sanzionatori della statunitense *Federal Trade Commission* (I.L. Nicolaidou-C. Georgiades, *The GDPR. New Horizons*, in T.-E-. Synodinou-P. Jougleux-C. Markou-T. Prastitou (a cura di), *EU Internet Law. Regulation and enforcement*, Cham, 2017, 14-15).

[13] Tale approccio, come si è osservato mira ad assicurare l'effetto deterrente nei confronti di grandi società o piattaforme, rispetto alle quali sanzioni con massimale fisso, seppure elevato, si paleserebbero insufficienti. Inoltre, la riferibilità al fatturato mondiale consente di "responsabilizzare" anche le sedi operative locali di grandi multinazionali, dato che «Una violazione del GDPR perpetrata da una di queste sedi, anche se piccola, inciderà infatti, in punto di sanzioni, sul bilancio di tutta la società». Cfr. G. Ziccardi, *GDPR: sanzioni pecuniarie fisse e proporzionali al fatturato*, in *IPSOA Quotidiano*, 21 marzo 2018; Id., *GDPR, multinazionali: sanzioni "pesanti", ma evitabili*, *ivi*, 2 maggio 2018.

[14] In punto cfr. F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali*, II, *Il Regolamento europeo 2016/679*, Torino, 2016, 22-23.

[15] Vengono nominati: la natura, la gravità e la durata della violazione tenendo in considerazione la natura, l'oggetto o a finalità del trattamento in questione nonché il numero di interessati lesi dal danno e il livello del danno da essi subito; il carattere doloso o colposo della violazione; le misure adottate dal titolare del trattamento o dal responsabile del trattamento per attenuare il danno subito dagli interessati; il grado di responsabilità del titolare del trattamento o del re-

ne, tuttavia, del tutto indeterminato quale sia il peso sulla sanzione irrogabile di ogni singolo fattore e risalta altresì l'assenza di alcun criterio di priorità o di contemperamento tra i vari profili rilevanti ai fini della regolazione di ipotesi di infrazione pluricircostanziate. La nutrita elencazione dei fattori rilevanti, inoltre, non riveste carattere tassativo, dal momento che la clausola conclusiva consente alla Autorità emanante di considerare altresì «eventuali altri fattori aggravanti o attenuanti applicabili alle circostanze del caso, ad esempio i benefici finanziari conseguiti o le perdite evitate, direttamente o indirettamente, quale conseguenza della violazione» (lett. k)[16].

Il profilo più delicato della valutazione complessiva demandata all'Autorità competente concerne, peraltro, la stessa scelta di procedere o meno alla irrogazione. La sanzione amministrativa di cui all'art. 83 risulta pertanto connotata dalla non indefettibilità, rappresentando solo una delle possibili conseguenze dell'accertamento dell'illecito[17].

sponsabile del trattamento tenendo conto delle misure tecniche e organizzative da essi messe in atto ai sensi degli articoli 25 e 32; eventuali precedenti violazioni pertinenti commesse dal titolare del trattamento o dal responsabile del trattamento; il grado di cooperazione con l'autorità di controllo al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi; le categorie di dati personali interessate dalla violazione; la maniera in cui l'autorità di controllo ha preso conoscenza della violazione, in particolare se e in che misura il titolare del trattamento o il responsabile del trattamento ha notificato la violazione; il rispetto dei provvedimenti che siano stati precedentemente disposti dell'articolo 58, paragrafo 2, nei confronti del titolare del trattamento o del responsabile del trattamento in questione relativamente allo stesso oggetto; l'adesione ai codici di condotta approvati ai sensi dell'articolo 40 o ai meccanismi di certificazione approvati ai sensi dell'articolo 42.

[16] In senso critico verso «una scelta che punta chiaramente ad una personalizzazione della sanzione», sino a ravvisarvi profili di contrasto con l'uguaglianza formale, P. Marini, *Regolamento Privacy UE e violazioni: le novità dell'apparato sanzionatorio*, in *Quotid. giuridico*, 12 luglio 2017.

[17] Peraltro, il regolamento omette di intervenire su un profilo evidentemente assai delicato per la effettività e dissuasività delle sanzioni, ossia l'assicurabilità del relativo "danno economico", rimessa quindi alle discipline nazionali (sul punto non omogenee e sovente non chiare; Cfr. DLA Piper-AON, *The price of data security – A guide to the insurability of GDPR finesacross Europe*, may 2018). L'assicurazione da sanzioni amministrative, come noto, è espressamente vietata in Italia dall'art. 167, co. 2, d.lgs. n. 209/2005 (Codice delle assicurazioni private).

2. I restanti poteri correttivi: misure o sanzioni non pecuniarie dissimulate?

Il regolamento, infatti, prevede che le sanzioni pecuniarie possano essere applicate dall'Autorità in aggiunta o in alternativa alla adozione di «misure» nell'esercizio dei «poteri correttivi» previsti dall'art. 58 par. 2[18].

La diversa denominazione pare indicare una inequivoca differenza ontologica rispetto alle sanzioni irrogabili in forza dell'art. 83 (che si potrebbe quindi definire, *a contrario*, come base di un potere "repressivo"). Le misure, infatti, in quanto tali non parteciperebbero della natura sanzionatoria[19]. Pare però possibile chiedersi se tale classificazione possa, nel caso di specie, ritenersi appagante, e se nelle suddette misure non possano invece ravvisarsi (almeno in certe ipotesi) autentiche forme di sanzioni amministrative non pecuniarie[20].

La questione non sembra meramente teorica, ove si consideri che in accordo al considerando 148, «l'imposizione di sanzioni, comprese sanzioni amministrative pecuniarie dovrebbe essere soggetta a garanzie procedurali appropriate in conformità dei principi generali del diritto dell'Unione e della Carta, inclusi l'effettiva tutela giurisdizionale e il giusto processo»[21]. In sostanza, dalla mancata quali-

[18] Su cui v. almeno C. Bistolfi, *I soggetti di controllo e verifica*, in *Il Regolamento Privacy europeo*, cit., 622 ss.

[19] L'opposizione tra "sanzioni" e "misure" appare consolidata nel diritto europeo, a partire dal regolamento (CE, EURATOM) n. 2988/95 del 18 dicembre 1995, relativo alla tutela degli interessi finanziari delle Comunità, il cui art. 4, par. 4 esplicitamente statuisce che «Le misure previste dal presente articolo non sono considerate sanzioni». In argomento, A.M. Maugeri, *Il regolamento n. 2988/95: un modello di disciplina del potere punitivo comunitario*, in G. Grasso (a cura di), *La lotta contro la frode agli interessi finanziari della Comunità europea tra prevenzione e repressione: l'esempio dei fondi strutturali*, Milano, 2000, 149 ss.

[20] È noto da tempo del resto che le sanzioni pecuniarie non sono le uniche concepibili né sempre le più efficaci (anche quando di importo elevato) per la repressione degli illeciti delle imprese. Al riguardo, v. almeno C. De Maglie, *Sanzioni pecuniarie e tecniche di controllo dell'impresa*, in *Riv. it. dir. proc. pen*., 1995, 88 ss.

[21] In tema v. da ultimo M. Lipari, *Il sindacato* pieno *del giudice amministrativo sulle sanzioni secondo i principi della CEDU e del diritto UE. Il recepimento della direttiva n. 2014/104/EU sul* private enforcement *(decreto legislativo n. 2/2017): le* valutazioni tecniche opinabili *riservate all'AGCM*, in *federalismi.it*, 11 aprile 2018.

ficazione dei poteri correttivi come sanzionatori potrebbe giungersi a desumere una relativa dequotazione delle rispettive garanzie processuali nei confronti dei relativi provvedimenti[22].

Sembra, del resto, difficile identificare una funzione unica o preponderante, comune a tutti i provvedimenti corrispondenti all'esercizio di «poteri correttivi», potendosi in essi rinvenire sia profili ripristinatori e cautelari, sia componenti afflittive e stigmatizzanti. In forza dell'art. 58, ad esempio, alle Autorità è consentito di rivolgere sia "avvertimenti" che "ammonimenti" in caso, rispettivamente, di rischio di violazioni o di violazioni già avvenute[23]; ma le stesse possono giungere anche a «imporre una limitazione provvisoria o definitiva di trattamento, incluso il divieto di trattamento» (lett. f). Orbene, quantomeno a fronte di un provvedimento di divieto definitivo di trattamento, la dimensione sanzionatoria della misura appare innegabile; la stessa ben può anzi, rappresentare per un'impresa la "pena capitale", comportando la totale estromissione dal "mercato dei dati".

La tesi di una (almeno concorrente) natura sanzionatoria delle misure in discorso sembra, inoltre, trovare indiretta conferma in quanto affermato nel considerando 129 (per cui «ogni misura dovrebbe essere appropriata, necessaria e proporzionata al fine di assicurare la conformità al presente regolamento...») che nelle Linee guida, laddove queste affermano che «Le autorità di controllo sono incoraggiate a ricorrere alle misure correttive con un approccio ponderato ed equilibrato, al fine di reagire in maniera effettiva, dissua-

[22] Ed invero, al riguardo, appare assai meno incisivo il tenore garantista del considerando 129 per cui «È opportuno che i poteri delle autorità di controllo siano esercitati nel rispetto di garanzie procedurali adeguate previste dal diritto dell'Unione e degli Stati membri, in modo imparziale ed equo ed entro un termine ragionevole».

[23] Per la considerazione di tali misure come «least severe sanctions» previste dal regolamento, in quanto non comportano obblighi diretti per il titolare di cessare o modificare il trattamento, P. Voigt-A. von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide*, Cham, 2017, 209. Propende per l'inquadramento come sanzione nell'ordinamento italiano, sebbene «nel Considerando 150 non è chiarissimo se l'avvertimento è considerato una sanzione o cosa diversa dalla sanzione come tale», F. Pizzetti, *La protezione dei dati personali dalla direttiva al nuovo regolamento: una sfida per le Autorità di controllo e una difesa per la libertà dei moderni*, in *MediaLaws - Rivista di diritto dei media*, n. 1/2018, 118, nt. 16.

siva e proporzionata alla violazione»; riprendendo, quindi, il trinomio – efficacia, proporzione, dissuasività – classicamente riferito, come si è visto, alle sanzioni a presidio del diritto UE (ma apposto nel testo regolamentare solo in relazione alle sanzioni pecuniarie e a quelle adottabili rimesse alla discrezionalità degli Stati membri)[24]. In tal senso, inoltre, pare deporre il dato testuale che apparenta a loro volta le sanzioni amministrative pecuniarie alle misure di cui all'art. 58, annoverando le prime, ai sensi della lett. i), tra le forme di poteri correttivi e ribadendone la possibile inflizione «in aggiunta alle misure di cui al presente paragrafo, o in luogo di tali misure, in funzione delle circostanze di ogni singolo caso».

Rimane a ogni modo piuttosto oscuro quali parametri debbano guidare, in fase applicativa, il riparto tra poteri correttivi e propriamente sanzionatori e il loro eventuale esercizio congiunto. Al riguardo, un interessante, seppur parziale, indicazione operativa proviene dal considerando n. 148, a mente del quale «In caso di violazione minore o se la sanzione pecuniaria che dovrebbe essere imposta costituisse un onere sproporzionato per una persona fisica, potrebbe essere rivolto un ammonimento anziché imposta una sanzione pecuniaria»; affermazione che oltre a corroborare una lettura dell'ammonimento come "sanzione minore" pare introdurre un parametro di valutazione equitativa (l'onerosità per il patrimonio della persona fisica) non espressamente richiamato tra i quelli elencati dall'art. 83 par. 2. Più in generale, non risulta risolutiva la consultazione delle citate Linee guida, limitandosi le stesse ad osservare che «Le sanzioni pecuniarie rappresentano un importante strumento che le autorità di controllo dovrebbero utilizzare nelle opportune circostanze» e «Il punto non è qualificare le sanzioni pecuniarie come misure di

[24] In tal senso, pare indicativo anche quanto recentemente affermato dal Presidente del Garante per la protezione dei dati personali Soro nell'audizione sull'Atto del Governo n. 22 (Adeguamento normativa nazionale circa la protezione delle persone fisiche con riguardo al trattamento dei dati personali) presso le Commissioni speciali su atti urgenti del Governo congiunte Senato e Camera (in *www.garanteprivacy.it*, 5) per cui «nella sistematica del Regolamento si delinea un continuum tra provvedimenti inibitori, prescrittivi e monitori da un lato e sanzioni amministrative pecuniarie, dall'altro. Pertanto, la misura minima suscettibile di applicazione a fronte di un illecito è da identificarsi in quelle di cui all'articolo 58, par. 2, secondo la gradazione lì indicata [...]».

ultima istanza, né evitare di irrogarle, bensì utilizzarle in un modo che non ne riduca l'efficacia come strumento»[25].

Ne emerge, insomma, confermata la diagnosi sull'amplissima discrezionalità non solo sul *quantum* ma prima ancora sull'*an* della sanzione che il legislatore europeo ha voluto assicurare alle Autorità di controllo, quali organi di amministrazione indiretta dell'Unione, dotandoli di poteri estremamente duttili e al contempo (stante la loro previsione nel corpo stesso del regolamento) suscettibili di integrazione ma non di restrizione da parte dei legislatori nazionali[26]. Tale flessibilità rischia, tuttavia, di andare a discapito della prevedibilità delle conseguenze giuridiche per i soggetti dell'ordinamento come pure di riverberarsi in negativo sull'obiettivo primario del regolamento stesso, ossia il raggiungimento di un «livello equivalente» di protezione all'interno del territorio UE (che postula, ai sensi del considerando 11, «poteri equivalenti per controllare e assicurare il rispetto delle norme di protezione dei dati personali e sanzioni equivalenti per le violazioni negli Stati membri»)[27]. La tutela di tali essenziali esigenze rimane affidata al consolidarsi di una prassi omogenea delle Autorità di controllo e, soprattutto, all'attività di coordinamento e indirizzo del comitato europeo per la protezione dei dati[28]; quest'ultima, peraltro, destinata a tradursi in atti di "diritto soffice" (le linee guida) dotate di indubbia autorevolezza ma che paiono almeno formalmente sprovviste di natura cogente.

[25] Gruppo di lavoro articolo 29 per la protezione dei dati, *WP 253 - Linee guida riguardanti l'applicazione e la previsione delle sanzioni amministrative pecuniarie ai fini del regolamento (UE) n. 2016/679 adottate il 3 ottobre 2017*, 7.

[26] Così ad esempio è da escludere che la normativa nazionale possa vincolare le Autorità di controllo a un massimo edittale diverso da quello direttamente previsto dal regolamento (v. M. Ratti, *op. cit.*, 611).

[27] In tal senso, non pare affatto scontato che l'elevato importo massimo delle nuove sanzioni e la trasversalità rispetto alle legislazioni degli Stati membri siano sufficienti a garantirne l'efficacia. Cfr. S. Golla, *Is Data Protection Law Growing Teeth? The Current Lack of Sanctions in Data Protection Law and Administrative Fines under the GDPR*, in *Journal of Intellectual Property, Information Technology and E-Commerce Law*, n. 1/2017, 70 ss.

[28] Il quale infatti ai sensi dell'art. 70 garantisce «l'applicazione coerente» del regolamento ed elabora appunto «linee guida riguardanti l'applicazione delle misure di cui all'articolo 58, paragrafi 1, 2 e 3, e la previsione delle sanzioni amministrative pecuniarie ai sensi dell'articolo 83».

3. Il possibile concorso di ulteriori sanzioni a livello nazionale e il problema del *ne bis in idem*

La problematica più densa, in termini sistematici, del nuovo strumento di armonizzazione sanzionatoria in discorso è rappresentata dalla controversa apertura del regolamento a forme di tutela ulteriori a quanto in esso previsto, e, segnatamente, a forme di tutela penale a presidio dei precetti dello stesso, con necessaria collocazione sul piano della normativa nazionale degli Stati membri[29].

Al riguardo, assumono rilievo, oltre al già citato art. 83 del regolamento, i considerando 149 (per cui «Gli Stati membri dovrebbero poter stabilire disposizioni relative a sanzioni penali per violazioni del presente regolamento, comprese violazioni di norme nazionali adottate in virtù ed entro i limiti del presente regolamento. Tali sanzioni penali possono altresì autorizzare la sottrazione dei profitti ottenuti attraverso violazioni del presente regolamento. Tuttavia, l'imposizione di sanzioni penali per violazioni di tali norme nazionali e di sanzioni amministrative non dovrebbe essere in contrasto con il principio del *ne bis in idem* quale interpretato dalla Corte di giustizia») e 152 (in forza del quale «Se il presente regolamento non armonizza le sanzioni amministrative o se necessario in altri casi, ad esempio in caso di gravi violazioni del regolamento, gli Stati membri dovrebbero attuare un sistema che preveda sanzioni effettive, proporzionate e dissuasive. La natura di tali sanzioni, penali o amministrative, dovrebbe essere determinata dal diritto degli Stati membri»).

La portata poco perspicua di queste statuizioni può spiegarsi con una certa cautela del legislatore europeo, necessitata dalla presa d'atto che – come è noto – nell'ambito del diritto derivato UE i regolamenti non sono fonti idonee a veicolare obblighi espliciti di repressione penale. Su tale versante del diritto punitivo, infatti, l'Unione dispone esclusivamente di una potestà sanzionatoria

[29] Il rinvio alle normative nazionali operato dagli artt. 83-84 introduce nel sistema sanzionatorio elementi di flessibilità che sono, ovviamente, passibili di tradursi in divergenze anche significative tra gli Stati membri (A. Ferrarotti-L. Raponi, *La struttura multilivello della protezione dei dati personali in Europa*, in *Riv. It. Sc. Giur.*, 2017, 415).

indiretta che si esprime unicamente con l'adozione di direttive recanti norme minime in tema di reati e di sanzioni, ai sensi e nei limiti dell'art 83 Tr. FUE[30]. Al tempo stesso, è pacificamente riconosciuto che ogni atto di diritto europeo, ivi inclusi i regolamenti, possa in certi casi far sorgere in capo agli Stati membri obblighi impliciti di criminalizzazione, come precipitato del principio di leale cooperazione o "fedeltà comunitaria" (*ex* art. 4, par. 3 Tr. FUE) che richiede comunque la predisposizione, a garanzia dell'osservanza dei precetti europei, di sanzioni efficaci proporzionate e dissuasive.

Ciò premesso, appare evidente come il disposto dell'art. 83, par. 1 (per cui «Gli Stati membri stabiliscono le norme relative alle altre sanzioni per le violazioni del presente regolamento in particolare per le violazioni non soggette a sanzioni amministrative pecuniarie a norma dell'articolo 83, e adottano tutti i provvedimenti necessari per assicurarne l'applicazione. Tali sanzioni devono essere effettive, proporzionate e dissuasive») abbia valenza fondamentalmente ricognitiva, con implicito rinvio allo stato dell'arte della giurisprudenza di Lussemburgo; la formula impiegata costituisce, invero, una clausola di stile, rinvenibile nella quasi generalità dei regolamenti.

Pertanto, il regolamento nulla toglie e nulla aggiunge agli ipotetici obblighi penali di fonte europea connessi al proprio contenuto (escluso il formalistico onere di notifica alla Commissione delle misure eventualmente adottate in questo ambito); né potrebbe farlo perché – come si è già sottolineato – un regolamento non può costituire strumento per l'esercizio della competenza di armonizzazione penale. Ciò non toglie che in una prospettiva non remota l'ambito della privacy possa costituire oggetto idoneo per l'esercizio della competenza di armonizzazione penale accessoria (*ex* art. 83, par. 2, TFUE), in quanto settore già interessato da una ormai compiuta armonizzazione extrapenale[31].

[30] Sul punto v. per tutti G. Grasso, *Il Trattato di Lisbona e le nuove competenze penali dell'Unione Europea*, in *Studi in onore di Mario Romano*, IV, Napoli, 2011, 2326 ss.

[31] Cfr. A. Bernardi, *La competenza penale accessoria dell'unione europea: problemi e prospettive*, in *Dir. pen. cont. – Riv. trim.*, n. 1/2012, 59 ss.

Resta da considerare il monito finale con cui il considerando 149 esorta comunque al rispetto del principio del *ne bis in idem*[32]. L'elaborazione di tale principio (già consacrato nell'art. 50 della Carta europea dei diritti fondamentali e dell'art. 4 del Protocollo 7 della Convenzione Europea dei diritti dell'uomo), ha incontrato un tumultuoso sviluppo nella recente giurisprudenza delle Corti europee. Un determinante impulso in tal senso è provenuto dalla nozione allargata di "materia penale" ai sensi dell'art. 7 CEDU, interpretata dalla giurisprudenza di Strasburgo come comprensiva non solo delle disposizioni sanzionatorie formalmente previste come incriminatrici ma anche di quelle sanzioni da ritenersi "sostanzialmente" penali[33]. Per l'effetto, sono entrati in potenziale conflitto con il divieto di *bis in idem* numerosi casi di "doppio binario" di tutela (penale e punitivo-amministrativa) rinvenibili in svariati ordinamenti statali europei[34].

Nell'arco di tempo successivo all'adozione del regolamento, tuttavia, si osserva nella giurisprudenza delle Corti europee un'evoluzione fortemente mitigatrice del rigore delle affermazioni iniziali. Invero, dalla iniziale tendenziale inderogabilità del divieto di *bis in idem* si è da ultimo approdati a sancirne la bilanciabilità, in quanto diritto fondamentale ma non immune da contemperamenti con altri diritti e interessi; aprendo, conseguentemente, a una modulazione della tutela caso per caso mirante non tanto alla proibizione del doppio

[32] Il riferimento al *ne bis in idem* va inteso nel contesto come limitato alla accezione nazionale, rispetto al rischio di doppia punizione nell'ambito del medesimo ordinamento. Tuttavia, la possibilità che per una stessa violazione l'autore sia sottoponibile a più procedimenti (e sanzioni) da diverse Autorità dei Paesi membri, comporta una problematicità anche a rispetto alla dimensione transnazionale-orizzontale del principio. Sebbene il regolamento non detti una specifica disciplina, pare persuasivo che in caso di violazione con carattere transnazionale il potere di irrogare la sanzione spetti solo alla Autorità capofila competente per i trattamenti transfrontalieri del titolare o responsabile del trattamento, individuato in base all'art. 56. Cfr. O. Lynskey, *The 'Europeanisation' of Data Protection Law*, in *Cambridge Yearbook of European Legal Studies*, 2017, 274.

[33] Secondo i noti criteri elaborati a partire dal caso *Engel*; v. per tutti F. Mazzacuva, Nulla poena sine lege, in F. Viganò-G. Ubertis (a cura di), *Corte di Strasburgo e giustizia penale*, Torino, 2016, p. 249 ss.

[34] Cfr. G. De Amicis, *Diritto dell'UE e della CEDU e problema del* bis in idem, in *Il Libro dell'anno del Diritto*, Roma, 2015, 660 ss.; B. Nascimbene, Ne bis in idem, *diritto internazionale e diritto europeo*, in www.penalecontemporaneo.it, 2 maggio 2018.

binario quanto all'equilibrio complessivo del risultato sanzionatorio (anche quando sia riconosciuta la natura "sostanzialmente penale" della concorrente sanzione amministrativa)[35].

Alla luce di tali approdi giurisprudenziali, appare ragionevole la cautela accolta nel decreto legislativo di adeguamento del codice dei dati personali che ha previsto al sesto e ultimo comma dell'art. 167 (riferito anche ai nuovi reati di cui agli artt. 167 *bis* e *ter*) una attenuante a effetto comune e di natura obbligatoria, da applicarsi nei procedimenti penali vertenti su fatti per cui sia stata applicata dal Garante (ed effettivamente riscossa) una sanzione amministrativa pecuniaria. Va altresì ricordato come tra le disposizioni della legge n. 689 del 1981 richiamate dal codice novellato vi sia anche l'art. 9 (principio di specialità) in base al quale se il medesimo fatto risulta punibile sia in forza di norme penali che di norme amministrative, si applica la disposizione speciale. La proposta inizialmente redatta dalla Commissione ministeriale, per contro, prevedeva (in uno con l'abrogazione del decreto legislativo n. 196/2003) di fare *tabula rasa* di ogni disposizione incriminatrice speciale, in forza di una interpretazione prudenziale della portata del divieto europeo di *bis in idem*[36].

4. La tormentata riforma delle fattispecie penali speciali a protezione dei dati personali

Il tema introduce la spinosa questione della sorte delle fattispecie penali a presidio della disciplina dei dati personali nell'ordinamento italiano[37].

[35] Cfr. Corte giust., Grande Sezione, 20 marzo 2018, C-524/15, *Menci*, su cui N. Recchia, *Note minime sulle tre recenti sentenze della Corte di giustizia dell'Unione europea in tema di* ne bis in idem, in *Eurojus*, 22 marzo 2018; *amplius* A. Vallini, *Tracce di* ne bis in idem *sostanziale lungo i percorsi disegnati dalle Corti*, in *Dir. pen. proc.*, n. 4/2018, 525 ss.

[36] Così lo schema di decreto approvato in via preliminare dal Consiglio dei Ministri il 21 marzo 2018. Cfr. M. Bassini-O. Pollicino, *Decreto Gdpr, «perché abbiamo depenalizzato il trattamento illecito di dati personali»*, in agendadigitale.eu, 17 aprile 2018.

[37] Sulla legittima eleggibilità della protezione dati personali come bene giuridico penalmente protetto non sembrano esservi dubbi, stante l'elevato rango ormai riconosciuto a tale diritto anche sul piano internazionale (v. per tutti M. Gambini,

Al riguardo, si deve anzitutto constatare come il Parlamento, seguendo una consolidata prassi di recepimento del diritto UE (indubbiamente in tensione con la *ratio* garantista della riserva di legge di cui all'art. 25 Cost.) abbia sostanzialmente abdicato a un effettivo ruolo decisionale in sede di delega, omettendo di formulare specifici e pregnanti criteri direttivi[38]. La legge di delegazione europea, infatti, si limita a indicare la necessità di adeguare il sistema sanzionatorio vigente alle disposizioni del Regolamento mediante la previsione di «sanzioni penali e amministrative efficaci, dissuasive e proporzionate alla gravità della violazione delle disposizioni stesse»[39].

La formula usata traduce, verosimilmente, la volontà parlamentare di lasciare "carta bianca" al legislatore delegato: indicazioni così generiche paiono, difatti, intrinsecamente compatibili con soluzioni riformatrici anche diametralmente opposte, quali in effetti appaiono quelle succedutesi nei lavori preparatori. Tuttavia, a un attento

La protezione dei dati personali come diritto fondamentale della persona: meccanismi di tutela, in *Espaço Jurídico*, 2013, 149 ss.). Con particolare riferimento al contesto del *Cyberspace*, L. Picotti, *La tutela penale della persona e le nuove tecnologie dell'informazione*, in Id. (a cura di), *Tutela penale della persona e nuove tecnologie*, Padova, 2013, 65 ss. Un ricorso alla sanzione penale per casi di notevole gravità risultava prefigurato già nel seminale contributo di L.D. Brandeis-S.D. Warren, *The Right to Privacy*, in *Harvard Law Review*, 1890, 4, 219.

[38] La perplessità deriva non tanto, o necessariamente, dalla condivisione della lettura (autorevole ma minoritaria) dell'art. 25 Cost. come riserva alla legge formale (su cui v. per tutti C. Cupelli, *La legalità delegata. Crisi e attualità della riserva di legge nel diritto penale*, Napoli, 2012) bensì dal rilievo che il conferimento, in materia penale, di deleghe dai criteri direttivi generici e stereotipati, definite sostanzialmente *per relationem* (con riferimento all'atto UE da recepire) finisce per ridurre il parlamento a mera cinghia di trasmissione, verso il Governo, degli obblighi di tutela sanzionatoria di matrice europea, trasferendo totalmente in capo a quest'ultimo ogni residua discrezionalità politico-criminale in ordine alla loro attuazione. In argomento, con riferimento alle leggi comunitarie, v. già M.V. Del Tufo, *Il diritto penale sommerso: diritto europeo e modifiche al sistema penale*, in *Dir. pubbl. comp. eur*., 2001, 1026 ss.; volendo, E. Cottu, «*Morte e trasfigurazione*» *di una legge comunitaria*, in *Riv. it. dir. pubbl. com*., 2011, 1376 ss. Sulla persistente problematicità dell'apporto parlamentare nella fase discendente anche a seguito della riforma della partecipazione alla formazione e attuazione della normativa UE, C. Grandi, *Processo decisionale europeo e democrazia penale. Osservazioni a margine della "legge quadro" n. 234 del 2012*, in *Dir. pen. cont. – Riv. trim*., n. 2/2013, 72.

[39] Cfr. art. 13, comma 3, lett. e, l. 25 ottobre 2017, n. 163.

esame appare dubbio che questo intento corrisponda effettivamente alla portata del potere normativo devoluto al Governo e proietta su larga parte della componente penalistica della novella il sospetto dell'eccesso di delega.

Com'è noto, la prima bozza di decreto legislativo elaborata dalla commissione ministeriale contemplava l'abrogazione del codice della privacy e quindi delle specifiche incriminazioni previste in tale sede[40]. Tale scelta depenalizzatrice, pur indubbiamente lineare, non ha mancato di suscitare perplessità ed è stata, infine, accantonata a favore della estesa novella del codice delineata in un secondo schema governativo[41]. Sulla scorta di quest'ultimo il testo adottato nel decreto legislativo n. 101/2018 rappresenta ora non solo una conferma dell'opzione di tutela penalistica in tema di privacy, ma, altresì, un suo netto rinvigorimento, reso palese anzitutto dalla previsione di nuove fattispecie delittuose[42].

Tuttavia, la legittimazione del legislatore delegato a innovare in tale ultimo senso appare quantomeno dubbia, ove si consideri che i

[40] V. al riguardo G. Finocchiaro, *Lo schema di decreto legislativo sulla privacy*, in *www.filodiritto.com*, 5 aprile 2018. Rispetto a tale scelta era stata asserita anche una illegittimità per eccesso di delega, rispetto alla indicazione di "adeguare il sistema sanzionatorio"; v. al riguardo *Gdpr, Bolognini: "Da schema di riordino del governo rischi di incostituzionalità"*, in *www.corrierecomunicazioni.it*, 29 marzo 2018; *contra*, G. De Gregorio, *Sull'eccesso di delega del decreto legislativo di adeguamento della disciplina italiana sulla privacy al Regolamento (UE) 679/2016*, in *MediaLaws- Rivista di diritto dei media*, n. 2/2018, 420 ss. A parere di chi scrive, a prescindere dall'opportunità il carattere davvero anodino del termine impiegato ben consentiva di ricomprendervi anche un adeguamento "per sottrazione" che (come nella proposta in discorso) si limitasse ad assicurare la piena operatività delle nuove sanzioni amministrative di matrice europea. Per contro, il testo normativo adottato ci pare esporsi al sospetto di eccesso di delega, per aver introdotto nuove sanzioni penali più gravi di quelle da ritenersi consentite dalla legge di delegazione europea (cfr. *infra*).

[41] Cfr. Atto Governo n. 22 (trasmesso alle Camere il 10 maggio 2018).

[42] Decreto legislativo 10 agosto 2018, n. 101 (*Disposizioni per l'adeguamento della normativa 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 (regolamento generale sulla protezione dei dati*), in G.U. n. 205 del 04-09-2018.

criteri e principi direttivi informanti la legge di delegazione europea si rinvengono non solo nella stessa ma altresì in quelli previsti, in via generale, dalla legge-quadro sull'adempimento degli obblighi europei (legge n. 234 del 2012). Con particolare riferimento alla materia sanzionatoria, detta legge prevede che «al di fuori dei casi previsti dalle norme penali vigenti, ove necessario per assicurare l'osservanza delle disposizioni contenute nei decreti legislativi» gli stessi possano essere corredati dalla previsione di sanzioni sia amministrative che penali; queste ultime, nei limiti pena dell'ammenda fino a 150.000 euro e dell'arresto fino a tre anni, in via alternativa o congiunta, ovvero delle sanzioni alternative previste agli articoli 53 e seguenti previste dal decreto legislativo 28 agosto 2000, n. 274 per i reati di competenza del giudice di pace[43]. La comminatoria delle specie di pena tipiche dei delitti risulta pertanto preclusa al legislatore delegato, a meno che non sia autorizzata dai criteri di delega particolari recati dalla legge di delegazione; i quali, nel caso di specie, nulla dicono in tal senso, limitandosi (come si è visto) a invitare un generico "adeguamento" del sistema sanzionatorio. Pare, allora, giocoforza ritenere che quantomeno nella parte in cui introduce nuovi delitti la riforma rischi di risultare esorbitante dai vincoli della delega, come ricavabili dal combinato disposto della legge di delegazione europea 2016-2017 con la legge quadro.

Ferma questa problematica premessa, e venendo al merito politico-criminale della novella, tra i suoi tratti salienti non può non risaltare anzitutto l'elemento "conservativo", ossia il mantenimento (in senso opposto a quanto prefigurato nel progetto iniziale) della fattispecie incriminatrice cardine della materia, rappresentata dal reato di illecito trattamento di cui all'art. 167. Al riguardo, può osservarsi come nonostante i nuovi poteri sanzionatori conferiti al Garante, e a dispetto di una non vasta casistica giurisprudenziale, il reato di illecito trattamento pare trovare ancora una ragion d'essere, se non altro come risposta a violazioni delle garanzie in materia

[43] In tema, sia consentito il rinvio a E. Cottu, *Sub* art. 33 *(Delega al Governo per la disciplina sanzionatoria di violazioni di atti normativi dell'Unione europea)*, in L. Costato-L.S. Rossi-P. Borghi (a cura di), *Commentario alla Legge 24.12.2012, n. 234. Norme generali sulla partecipazione dell'Italia alla formazione e all'attuazione della normativa e delle politiche dell'Unione europea*, Napoli, Ed. Scientifica, 2015, 301-317.

dati personali ridondanti in danno della dignità della persona, e per i quali la valenza stigmatizzante della sanzione penale apporta un "valore aggiunto", sotto il profilo della generalprevenzione, rispetto a una sanzione amministrativa pecuniaria (per quanto di elevatissimo importo). Tale è il caso, ad esempio, del c.d. *revenge porn* (come viene definita la diffusione, contro la volontà del soggetto ritratto, di materiale audiovisivo di contenuto sessuale) preoccupante fenomeno criminoso che la Suprema Corte di Cassazione ha recentemente ribadito rientrare nel fuoco dell'art. 167[44]; o del c.d. cyberbullismo, rispetto al quale pare essere lo stesso Legislatore a sancire la rilevanza della fattispecie[45].

Al contempo, è parso da tempo evidente come il reato in questione abbia mostrato vistosi limiti applicativi quale fattore di "governo penale" di internet e dell'economia dei dati; basti pensare, al riguardo, alle conclusioni negative cui è pervenuta la giurisprudenza di legittimità in ordine alla configurazione di una responsabilità da omesso controllo in capo ai soggetti amministratori della piattaforma digitale per i contenuti caricati dagli utenti[46].

[44] Cfr. Cass. pen., sez. III, sent. 14 giugno 2017, n. 29549, in *Quotid. giuridico*, 26 giugno 2017, con nota di A. Scarcella, *La diffusione di foto osè è condotta idonea a creare "nocumento" alla vita sessuale della coppia*; ma già Cass. pen., Sez. III, 10 settembre 2015, n. 40356, in *Dir. & Giust.*, 2015, 10 e ss. con nota di S. Gentile (*Pubblica su YouTube il video che ritrae le pose oscene della vittima: condannato*). Tali condotte, per inciso, non sono suscettibili di rientrare nel nuovo delitto di diffusione di riprese e registrazioni fraudolente previsto dall'art. 617-*septies* c.p., il quale non colpisce appunto i casi in cui il soggetto abbia prestato il consenso alla ripresa (sebbene non alla diffusione). In tema v. *amplius* G.M. Caletti, "*Trust me: it's only for me!*". *La repressione penale del* Revenge Porn *a livello internazionale* (in corso di pubblicazione in *www.penalecontemporaneo.it*).

[45] L'art. 1, comma 2, l. 29 maggio 2017, n. 71, definisce infatti il cyberbullismo come «qualunque forma di pressione, aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione, *furto d'identità*, alterazione, acquisizione illecita, manipolazione, *trattamento illecito di dati personali in danno di minorenni*, realizzata per via telematica, nonché la diffusione di contenuti on-line aventi ad oggetto anche uno o più componenti della famiglia del minore il cui scopo intenzionale e predominante sia quello di *isolare* un minore o un gruppo di minori ponendo in atto un serio abuso, un attacco dannoso, o la loro messa in ridicolo».

[46] Si tratta del noto caso *Google-Vividown* definito da Cass., sez. III pen., il 3 febbraio 2014, n. 3672.

Alla luce di questi rilievi, non sembra irrealistico l'auspicio che il nuovo assetto "multilivello" della disciplina sanzionatoria veda una effettiva complementarietà tra lo strumento penale (calibrato sulla repressione di fatti realmente forieri di allarme sociale, oltre che di dinamiche interindividuali particolarmente odiose) e le nuove sanzioni amministrative, queste ultime dotate (per natura, entità e presupposti) di ben più considerevole impatto, a ben vedere, per i professionisti del trattamento, attingibili direttamente nella loro dimensione organizzativa e imprenditoriale. Ciò anche in considerazione del dato che le fattispecie contemplate nel codice della privacy non rientrano nel pur amplissimo novero dei reati-presupposto della responsabilità degli enti *ex* d.lgs. 231/2001[47]. Pertanto, sotto questo profilo, non sussiste il rischio di una duplicazione sanzionatoria nei confronti della persona giuridica, quale invero potrebbe profilarsi se la stessa – oltre a essere direttamente sanzionata in base al regolamento europeo – potesse altresì essere chiamata a rispondere, per gli stessi fatti, di illeciti penali commessi nel suo interesse o a suo vantaggio.

Il giudizio di opportunità sul mantenimento di un presidio penalistico non comporta, però, facili soluzioni all'interrogativo sulla dosimetria ottimale della correlata risposta punitiva. Al riguardo, è difficile sottrarsi all'impressione che le innovazioni apportate dal decreto legislativo, quasi ribaltando la direzione depenalizzatrice della prima bozza, si concretino in una complessiva "iperpenalizzazione"[48].

Vero è, infatti che il decreto reca anche talune modifiche *in mitius*, quali il restringimento del compasso edittale per la condotta base di trattamento illecito di dati (punita ora con la reclusione da sei a diciotto mesi in luogo di ventiquattro) nonché l'eliminazione della contravvenzione di cui all'art. 169 (omessa adozione delle misure minime di sicurezza di cui all'art. 33 del Codice)[49]. Oltre al ri-

[47] In argomento cfr. M. Lamanuzzi, *Diritto penale e trattamento dei dati personali. I reati previsti dal Codice della privacy e la responsabilità amministrativa degli enti alla luce del regolamento 2016/679/UE*, in *JusOnline*, n. 1/2017, spec. 256 ss.

[48] A. Cherchi, *Sulla privacy restano i reati*, in *Il Sole 24 ore*, 12 maggio 2018.

[49] Si tratta, secondo la Relazione illustrativa allo schema A. G. 22 approvato in via preliminare dal Consiglio dei ministri, (p. 35) di «un'opera di mirata e limitata

cordato art. 167, rimangono peraltro in vigore, con pena invariata, i reati di cui agli artt. 171 (Violazioni delle disposizioni in materia di controlli a distanza e indagini sulle opinioni dei lavoratori), 168 (Falsità nelle dichiarazioni al Garante) e 170 (Inosservanza di provvedimenti del Garante)[50]. Al contempo, tuttavia, vengono introdotte ben cinque ulteriori incriminazioni di nuovo conio, di cui due collocate sotto i nuovi commi, rispettivamente terzo e secondo, inseriti sotto gli articoli 167 e 168 e le rimanenti sotto gli inediti artt. 167-*bis* (primo e secondo comma) e 167-*ter* (rispettivamente rubricati "Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala" e "Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala"). Queste ultime disposizioni segnano altresì un significativo innalzamento della pena massima minacciata nell'ambito della protezione dei dati personali, sino a sei anni (art. 167-*bis)* e quattro anni (167-*ter*) di reclusione, laddove in precedenza nessun tetto edittale superava i tre anni già previsti al secondo comma dell'art. 167.

Non è naturalmente possibile, in questa sede, una completa disamina della novella. Merita tuttavia soffermarsi, per la sua perdurante centralità sistematica, sulla revisione della "storica" fattispecie di illecito trattamento di dati cui all'art. 167. Al riguardo, può essere constatato come la stessa – a dispetto di quanto affermato nella relazione illustrativa – sia rimasta pressoché immutata nella struttura di base: la descrizione della condotta tipica, in particolare, è tuttora imperniata sulla tecnica del rinvio, configurando la norma incriminatrice come meramente sanzionatoria[51]. A seguito del

depenalizzazione» motivata «in ragione della forte dissuasività esercitata dalle sanzioni amministrative alla luce dell'articolo 83 del Regolamento».

[50] Quest'ultima norma incriminatrice, abrogata nello schema A. G. 22, è stata da ultimo reinserita a seguito di esplicito invito del Garante. Cfr. il *Parere sullo schema di decreto legislativo recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679*, 22 maggio 2018 [doc. web n. 9163359], punto 1.4, in *www.garanteprivacy.it*.

[51] Dato strutturale immediatamente evidenziato in dottrina per le sue ricadute negative sulla determinatezza e conoscibilità del precetto e, quindi, sulla sua funzione orientativa per i consociati. V. per tutti A. Manna, Il *quadro sanzionatorio penale ed amministrativo del codice sul trattamento dei dati personali*, in *Diritto dell'informazione e dell'informatica*, 2003, 748 ss.; G. Corrias Lucente, *La nuova*

parere negativo delle Camere[52], è venuta meno l'unica innovazione di rilievo prevista nello schema di decreto, ossia la restrizione del dolo specifico al solo fine di trarre profitto per sé o per altri e non più anche (alternativamente) di recare danno. Sul piano dogmatico, l'elisione del danno dall'elemento soggettivo avrebbe rafforzato la tesi ermeneutica – attualmente minoritaria – che ravvisa nella causazione dello stesso, sul versante oggettivo della fattispecie, un elemento costitutivo e non condizione obiettiva (sia pur intrinseca) di punibilità[53]. In termini pratici, peraltro, pare verosimile che l'incidenza di una siffatta modifica sarebbe stata alquanto contenuta, in considerazione della nozione ampia di profitto (non necessariamente patrimoniale) su cui è da tempo assestata la giurisprudenza[54].

Venendo alle fattispecie dei nuovi artt. 167 *bis* e *ter* (e premessa la grave riserva sulla loro compatibilità con i criteri di delega, per le ragioni sopra esposte) emerge immediatamente, come elemento cardine delle stesse, il comune oggetto materiale delle condotte incriminate – cioè l'«archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala» – che ha sostituito il riferimento, nell'ultimo schema di decreto, alla commissione del fatto in danno di «un numero rilevante di persone offese», ri-

normativa penale a tutela dei dati personali, in F. Cardarelli-S. Sica-V. Zeno-Zencovich (a cura di), *Il codice dei dati personali. Temi e problemi*, Milano, 2004, 631 ss. La necessità di fare riferimento (in svariate ipotesi) a provvedimenti emanati dal Garante ai fini dell'identificazione della condotta punibile ha altresì suscitato il dubbio che l'art. 167 costituisca una "norma penale in bianco" in tensione con la riserva di legge *ex* art. 25 Cost. (Cfr. P. Troncone, *Il delitto di trattamento illecito dei dati personali*, Torino, 2011, 135 ss.).

[52] A. Ciccia Messina, *Decreto privacy. Il Parlamento è favorevole, con correttivi: quali?*, in *IPSOA Quotidiano*, 22 giugno 2018.

[53] Su tale contrasto giurisprudenziale v., con ampi riferimenti, A. Scarcella, *Trattamento illecito di dati personali: la qualificazione della lesione influisce sulla fattispecie*, in *IPSOA Quotidiano*, 28 gennaio 2016.

[54] Per questa notazione in riferimento al dolo del reato di illecito trattamento, v. C. Flick, *Privacy e legge penale nella società dell'informazione e della comunicazione*, in M. Cuniberti (a cura di), *Nuove tecnologie e libertà della comunicazione. Profili costituzionali e pubblicistici*, Milano, 2008, 283; G. Gaudino, *Il sistema sanzionatorio*, in R. Panetta (a cura di), *Libera circolazione e protezione dei dati personali*, II, Milano, 2006, 2240.

tenuto eccessivamente indeterminato[55]. La nozione di «trattamento di larga scala», mutuata dal testo del Regolamento UE (ancorché lo stesso non ne dia una specifica definizione) parrebbe funzionale ad assicurare l'aderenza teleologica delle nuove incriminazioni alla normativa europea[56]. Sul piano della politica del diritto, è forte l'impressione che un fattore propulsivo determinante per la loro introduzione (e per la previsione delle relative ampie cornici edittali) sia stato costituito dal recente scandalo *Cambridge Analytica*, e, quindi, dall'allarme verso forme mirate di manipolazione informativa (che hanno nel "furto di dati" di massa un necessario e strumentale antecedente) sospettate di poter influire sull'opinione pubblica e financo sugli andamenti elettorali[57]. In tal senso, la tutela penale dei dati personali parrebbe arricchirsi di ulteriori sfumature pubblicistiche (che ne confermerebbero, del resto, il già acquisito rilievo ultraindividuale).

Pare, infine, possibile chiedersi se la riforma, una volta scartata la via della depenalizzazione, potesse costituire occasione per rimeditare la generalizzata procedibilità d'ufficio dei reati nel settore. Al riguardo, quantomeno per la fattispecie più lieve di illecito trattamento, prevista al primo comma dell'art. 167 (punita ora con la reclusione sino a diciotto mesi) non sarebbe stato irragionevole considerare l'introduzione, sulla scorta di quanto previsto per la diffamazione non aggravata, della procedibilità a querela di parte (con *dies a quo* individuato, anche in questo caso, alla presa di conoscenza dell'offesa)[58]. Una scelta simile ha guidato il legislatore tedesco, il

[55] Una messa in guardia da possibili contrasti col principio di tassatività-determinatezza è venuta da componenti della stessa commissione ministeriale: G. Finocchiaro-O. Pollicino, *Fattispecie da definire con maggiore precisione*, in *Il Sole 24 Ore*, 12 maggio 2018.

[56] In prospettiva critica S. Aterno, *Ecco contenuti e prospettive del nuovo decreto privacy*, in *formiche.net*, 10 agosto 2018, ritiene che connotando la condotta di trasferimento «su larga scala» si sia impropriamente cercato di tradurre nella fattispecie il peculiare concetto di Big Data.

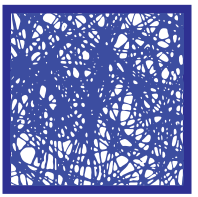
[57] Al riguardo cui v. almeno O. Pollicino, *La "terza stagione" delle informazioni*, in *Il Sole 24 Ore*, 23 marzo 2018.

[58] Come già autorevolmente auspicato, in dottrina, da L. Picotti, *I diritti fondamentali nell'uso ed abuso dei Social Network. Aspetti penali*, in *Giur. di merito*, n.12/2012, 2547, il quale evidenzia la verosimilmente elevatissima "cifra oscura", rispetto a tale reato, di fatti punibili ma non perseguiti.

quale nella nuova *Datengesetz* ha sottratto le incriminazioni speciali in materia alla procedibilità di ufficio, seppure annoverando tra i legittimati a proporre querela, oltre che ai diretti interessati, anche taluni soggetti pubblici particolarmente qualificati (tra cui il Commissario per la protezione dei dati)[59]. La procedibilità condizionata, oltre a non apparire necessariamente incompatibile con la tutela di beni personalistici (come dimostra, appunto, la tutela penale dell'onore) potrebbe invero sortire effetti positivi sia in chiave deflattiva sia in termini di stimolo a condotte riparatorie e reintegrative (in funzione anche, ma non solo, del pronto ed effettivo ristoro economico della vittima)[60].

[59] Cfr. il paragrafo 42 (*Strafvorschriften*), frase 3, della nuova *Bundesdatenschutzgesetz* del 30 giugno 2017 (*Die Tat wird nur auf Antrag verfolgt. Antragsberechtigt sind die betroffene Person, der Verantwortliche, die oder der Bundesbeauftragte und die Aufsichtsbehörde*).

[60] Anche in forza della applicabilità, in conseguenza della procedibilità a querela, del recente 162-*ter* c.p. (Estinzione del reato per condotte riparatorie), su cui v. per tutti e da ultimo A.M. Siagura, *L'estinzione del reato per condotte riparatorie nel bilanciamento tra mediazione e deflazione*, in *Arch. pen.*, *Speciale riforme (web)*, 28 maggio 2018.



Regolare le tecnologie

La gestione del rischio nel GDPR: limiti e sfide nel contesto dei Big Data e delle applicazioni di Artificial Intelligence*

Alessandro Mantelero

Sommario: 1. Il rischio e le radici della disciplina a tutela dei dati personali – 2. I nuovi paradigmi di trattamento dati basati su Big Data ed Artificial Intelligence ed i limiti del Regolamento (EU) 2016/679 – 3. La dimensione superindividuale dell'uso dei dati: verso una più ampia analisi del rischio

1. Il rischio e le radici della disciplina a tutela dei dati personali

Il nuovo Regolamento (UE) 2016/679 in materia di protezione dei dati personali (di seguito anche Regolamento) è sovente presentato come un punto di svolta nell'approccio regolatorio al tema. L'aspetto innovativo viene ravvisato in diverse disposizioni, ma soprattutto nel principio di *accountability* (art. 5, par. 2 del Regolamento) e nel *focus* sulla gestione del rischio correlato all'impiego dei dati personali (artt. 35 e 36).

* Il testo riprende con l'aggiunta di alcune note la relazione tenuta dall'autore nel corso del Convegno "L'entrata in vigore del Regolamento (UE) 2016/679: la riforma alla prova della prassi in Italia e in Spagna". L'attività di ricerca volta all'elaborazione del presente contributo è stata parzialmente finanziata dal Ministero dell'Istruzione, dell'Università e della Ricerca ("TESUN-83486178370409 finanziamento dipartimenti di eccellenza CAP. 1694 TIT. 232 ART. 6").

Con riferimento al tema della gestione del rischio, l'intento di questo contributo non è quello di procedere ad un'analisi delle disposizioni del Regolamento, già condotta altrove[1], bensì quello di guardare alle ragioni dell'adozione di un approccio incentrato sul rischio ed alle eventuali criticità applicative del modello proposto dal legislatore europeo.

A tal riguardo, occorre in primo luogo mettere in luce come il rischio e la sua gestione non rappresentino elementi nuovi della disciplina del trattamento dei dati personali. A ben vedere, infatti, il rischio è da sempre aspetto essenziale e caratterizzante questa disciplina, di cui costituisce invero la ragione primaria.

Sin dalle prime leggi in materia, l'intento del legislatore è stato infatti quello di contrastare o, quantomeno, limitare le potenziali conseguenze negative correlate all'impegno dei dati riferiti a persone fisiche. A fronte di una crescente domanda di dati ed alla progressiva digitalizzazione delle informazioni strumentali alla realizzazione delle politiche di *welfare state* nella seconda metà del Novecento, i cittadini si sentivano come spogli innanzi al potere pubblico, artefice di quella che – per l'epoca – era una raccolta massiva di informazioni.

L'avvento della gestione automatizzata delle informazioni comportava dunque un potenziale conflitto. Da un lato v'era l'interesse collettivo ed individuale allo stato di benessere economico e sociale dei cittadini. Dall'altro, l'interesse individuale (ma anche collettivo) ad evitare forme di discriminazione e controllo sociale, note sia in epoca bellica che durante la c.d. Guerra Fredda[2]. Proprio al fine

[1] Cfr. volendo A. Mantelero, *Il nuovo approccio della valutazione del rischio nella sicurezza dei dati. Valutazione d'impatto e consultazione preventiva (artt. 32-39)*, in G. Finocchiaro (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, Zanichelli, 2017, 287 ss.; A. Mantelero, *Responsabilità e rischio nel Reg. UE 2016/679*, in *Nuove Leggi Civ. Comm.*, 2017, 144 ss.

[2] Cfr. *ex multis*, A.R. Miller, *The Assault on Privacy Computers, Data Banks, Dossiers*, Ann Arbor, University of Michigan Press, 1971, 54-67; V. Mayer-Schönberger, *Generational development of data protection in Europe?*, in P.E. Agre-M. Rotenberg (a cura di), *Technology and privacy: The new landscape*, Cambridge, MA, MIT Press, 1997, 221-225; G. González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Cham-New York, Springer International Publishing, 2014, 28-36.

di gestire questo *trade-off*, i legislatori di diverse nazioni adottarono le prime previsioni volte a fornire garanzie a tutela dei dati personali.

È dunque la preoccupazione per i potenziali rischi dell'impiego dei dati che induce l'affermarsi della protezione dell'individuo rispetto al trattamento delle informazioni che lo riguardano. Per questo, il libero flusso delle informazioni e la protezione dei singoli e dei loro diritti sono sin dall'origine, ed ancora nel Regolamento (UE) 2016/679 (art. 1, par. 3), interessi coesistenti e congiuntamente perseguiti dal legislatore.

Non è dunque un caso che, ad esempio, proprio con riguardo alle informazioni maggiormente suscettibili di impiego con finalità discriminatorie, atte a rivelare le origini razziali o etniche, opinioni politiche, convinzioni religiose o filosofiche, le disposizioni in materia di trattamento dei dati personali si premurino di offrire maggiori garanzie e tutele.

Nel corso degli anni, l'iniziale rischio del controllo sociale ad opera dei soggetti pubblici si è poi evoluto, assumendo nuove forme. Alla preoccupazione originaria legata alla sorveglianza governativa si sono aggiunte inquietudini inerenti lo sfruttamento economico delle informazioni personali, frutto di una progressiva affermazione dell'informatica distribuita e del crescente impiego dei dati con fini di *direct marketing*, nonché del loro uso nel contesto di processi decisionali. Si è così passati dai rischi di una occhiuta sorveglianza pubblica ad una diffusa e potenzialmente altrettanto invasiva profilazione ad opera di soggetti privati, fino ai più recenti casi di cooperazione fra enti governativi e società private nella raccolta ed utilizzo di informazioni personali per finalità di controllo sociale.

Nel contempo, quantomeno a partire dagli anni '80 del secolo scorso, una maggiore alfabetizzazione informatica, unita all'affermarsi della c.d. informatica distribuita, hanno dato luogo ad una crescente conoscenza e consapevolezza delle modalità e conseguenze del trattamento informatizzato dei dati personali. Da questo è derivato che i cittadini non potessero essere più considerati come mero oggetto di protezione rispetto ai rischi potenziali dell'impiego dei dati. Andava riconosciuto un nuovo e più attivo ruolo a quelli che fino ad allora erano soggetti indirettamente tutelati dalla procedimentalizzazione del trattamento, dagli obblighi incombenti sugli

autori dello stesso, dal ruolo di sorveglianza e controllo delle autorità per la protezione dei dati personali.

Mentre dunque nelle prime "generazioni" di normative sul trattamento dati[3], gli interessati erano solo in minima parte garantiti in ragione di un loro eventuale ruolo attivo (si pensi ai c.d. diritti di accesso e, ove prevista, alla possibilità di ricorso alle autorità garanti o al giudice ordinario), la maggior consapevolezza circa le modalità del trattamento, unito all'accresciuto valore economico delle informazioni personali, inducono a riconoscere anche al singolo la possibilità di divenire partecipe del procedimento di gestione del rischio.

Con l'affermarsi del consenso informato, parte della valutazione del rischio si è infatti spostata sull'interessato. In quest'ottica il consenso non è solo una forma di autodeterminazione informativa circa la scelta di comunicare o meno i propri dati, né una mera componente del modello circolatorio di questi ultimi, ma è anche e soprattutto il risultato di una valutazione posta in esser dal singolo circa i rischi del trattamento come descritti nell'informativa ricevuta.

Questo mutamento di prospettiva fu suggellato nella Dir. 95/46/CE con il riconoscimento del ruolo determinante del consenso informato. Un consenso che, all'epoca, poteva essere idonea garanzia della libertà del singolo rispetto ad una consapevole previsione e gestione delle conseguenze del trattamento delle informazioni che lo riguardavano. In termini di rischio, non erano più solo gli autori del trattamento ed eventualmente le autorità garanti a farsi carico di valutare l'impatto del trattamento sul singolo, ma era anche quest'ultimo a stimare da sé tali conseguenze in un modello più complesso e partecipato di gestione del rischio. Un modello che vedeva non solo un processo predefinito dal titolare, ma la scelta del singolo di aderire o meno a tale processo e, sovente, la possibilità di selezionare le modalità (anche tecniche) con cui prendervi parte (e.g. personalizzazione delle preferenze circa le modalità del trattamento dati).

[3] Cfr. Mayer-Schönberger, *Generational development of data protection in Europe?*, cit., 221-227.

2. I nuovi paradigmi di trattamenti dati basati su Big Data ed Artificial Intelligence ed i limiti del Regolamento (EU) 2016/679

Negli ultimi due decenni sono venuti in essere mutamenti tecnologici e sociali che hanno parzialmente scardinato questo modello di gestione del rischio. Da un lato la complessità e l'oscurità delle nuove forme di trattamento dati[4] hanno significativamente indebolito il ruolo del consenso quale strumento di effettiva autodeterminazione[5]. D'altro canto, la scala dimensionale su cui vengono poste in essere le operazioni di trattamento è diventata sempre meno quella individuale e guarda invece sempre più alla dimensione superindividuale e collettiva.

Riguardo al primo aspetto, senza voler qui riprendere le considerazioni già formulate altrove[6], il consenso trova nel contesto delle applicazioni di *Artificial Intelligence* e Big Data due ordini di limiti: il primo concernente la natura delle operazioni di trattamento dati ed il secondo riguardante le modalità con cui il consenso viene disciplinato dalle norme in esame (artt. 6 e 7, Reg. (EU) 2016/679).

Nello specifico, la complessità dell'elaborazione basata su Big Data ed *Artificial Intelligence* esacerba i già noti limiti caratterizzanti il consenso informato. Sia che vengano fornite informative estremamente generiche ed onnicomprensive, sia che invece vengano offerte descrizioni dettagliate dei procedimenti da realizzare, il soggetto interessato pare sovente privato della concreta possibilità di

[4] Cfr. F. Pasquale, *The Black Box Society. The Secret Algorithms That Control Money and Information*, Cambridge, Ma, Harvard University Press, 2015, *passim*.

[5] Cfr. in tal senso A. Acquisti-L. Brandimarte-G. Loewenstein, *Privacy and human behavior in the age of information*, in *Science*, 2015, 347(6221), 509-514; L. Brandimarte-A. Acquisti-G. Loewenstein, *Misplaced Confidences: Privacy and the Control Paradox*, relazione tenuta al Ninth Annual Workshop on the Economics of Information Security, 2010, consultabile al seguente indirizzo: http://www.heinz.cmu.edu/~acquisti/papers/acquisti-SPPS.pdf; D.J. Solove, *Introduction: Privacy Self-management and The Consent Dilemma*, in *Harv. L. Rev.*, 2013, 126, 1883-1888.

[6] Cfr. A. Mantelero, *The future of consumer data protection in the E.U. Rethinking the "notice and consent" paradigm in the new era of predictive analytics*, in *Comp. Law & Sec. Rev.*, 2014, 30(6), 643-660.

manifestare un consenso consapevole ed effettivo. Nel primo caso, mancherà infatti la specificità della descrizione delle finalità e modalità del trattamento, mentre nel secondo il tecnicismo e la complessità dell'informativa ne scoraggeranno la lettura o renderanno il testo comprensibile solo a pochi.

A ciò si aggiunga che la crescita esponenziale delle occasioni di raccolta dati sottopone i soggetti interessati ad un profluvio di richieste, rispetto alle quali molti sono indotti a non prendere più in considerazione il contenuto delle informative ricevute ed a valutare su altre basi (e.g. fiducia nel titolare del trattamento, necessità del servizio[7]) l'opportunità di fornire o meno i dati richiesti. È infine noto dagli studi sul c.d. *dynamic consent* come l'iterazione delle richieste di consenso al trattamento possa portare a fenomeni di assuefazione e ad automatismi[8].

Nel contesto dei processi ad alta intensità di elaborazione dei dati, il consenso informato rischia quindi di perdere la sua funzione originaria di garanzia dell'effettiva autodeterminazione del singolo, anche con riguardo all'assunzione del rischio. Al contrario, il consenso diviene un facile *escamotage* per legittimare la raccolta dei dati su ampia scala.

Vero che il nuovo Regolamento (cfr. in particolare art. 7) pare voler rafforzare l'effettività del consenso. Permane tuttavia il dubbio che queste disposizioni – in sé non particolarmente innovative – possano davvero mutare la prassi esistente.

Queste considerazioni valgono poi in maggior misura con riferimento ai sistemi che impiegano soluzioni di *Artificial Intelligence* come ad esempio gli algoritmi di *machine learning*. Sono questi i casi in cui le modalità operative degli algoritmi risultano in ampia parte ignote agli stessi sviluppatori, poiché frutto di un'auto-organizzazione delle componenti informatiche di tali sistemi sulla base di processi di

[7] Per un riscontro empirico in tal senso, con riferimento al contesto italiano, cfr. A. Mantelero, *Children online and the future EU data protection framework. Empirical evidences and legal analysis*, in *International Jour. Tech. Policy & Law*, 2016, 2 (2/3/4), 169-181.

[8] Cfr. J. Kaye-E.A. Whitley-D. Lund-M. Morrison-H. Teare-M. Melham, *Dynamic consent: a patient interface for twenty-first century research networks*, in *European Journal of Human Genetics*, 2015, 23 (2), 141-146.

auto-apprendimento[9]. Risulta quindi difficile sia rendere esplicabili[10] sia, lato interessato, comprendere le modalità del trattamento[11].

Non più agevole è la situazione nel caso di sistemi che fanno uso di Big Data *analytics*, ove vengono impiegati algoritmi basati su modelli matematici che possono essere oggetto di descrizione, ma la cui complessità e numerosità di variabili non rende certo accessibile a chiunque l'effettiva comprensione delle modalità di trattamento dati, oltre ad aprire un dibattito sul livello di trasparenza astrattamente esigibile.

Incidentalmente, con riguardo al dibattuto rapporto fra algoritmi e trasparenza[12], va rilevato come la nozione di trasparenza – che si riflette anche nello strumento dell'informativa – può essere intesa in varie maniere. Principalmente può consistere nell'accesso all'algoritmo e – nei casi di *machine learning* – ai dati impiegati per generare ed addestrare lo stesso, ovvero nell'accesso alla mera logica dell'algoritmo.

Le norme a protezione della proprietà intellettuale possono tuttavia porre diversi ostacoli rispetto all'accesso all'algoritmo. Vi sono poi casi in cui una simile forma di trasparenza confligge con le finalità

[9] Cfr. The Norwegian Data Protection Authority, *Artificial Intelligence and Privacy Report*, gennaio 2018 consultabile al seguente indirizzo: *https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf*

[10] Cfr. B. Goodman-S. Flaxman, *European Union Regulations on Algorithmic Decision-Making and a "Right to Explanation"*, in *ArXiv:1606.08813 [Cs, Stat]*, 28 giugno 2016, consultabile al seguente indirizzo: *http://arxiv.org/abs/1606.08813*

[11] Vero che queste ultime non vengono esplicitamente indicate fra le informazioni da fornire all'interessato, tuttavia l'applicazione dei principi di correttezza e trasparenza nel trattamento (art. 5.1 e considerando n. 6, Reg. (UE) 2016/679) paiono rendere difficile prescindere da un'indicazione circa le modalità dell'elaborazione dei dati, specie ove queste ultime siano funzionali all'inferenza di nuove informazioni ed al supporto di processi decisionali riguardanti gli interessati, come accade nel caso di modelli di *Artificial Intelligence*.

[12] Cfr. e.g. S. Wachter-B. Mittelstadt-Luciano Floridi, *Why a right to explanation of automated decision - making does not exist in the General Data Protection Regulation*, in *International Data Privacy Law*, 2017, 7(2), 76–99; A.D. Selbst-J. Powles, *Meaningful Information and the Right to Explanation*, in *International Data Privacy Law*, 2017, 7(4), 233-242; L. Edwards-M. Vale, *Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For*, in *Duke Law and Technology Review*, 2017, 16(1), 18-84.

perseguite da soggetti pubblici (e.g. algoritmi di *predictive policing*[13]). La soluzione incentrata sulla trasparenza della logica dell'algoritmo pare essere quindi maggiormente sostenibile. Essa comprende però un vasto *range* di ipotesi operative (dalla conoscenza delle informazioni sui dati di input e l'output atteso alla descrizione delle variabili impiegate, al peso attribuito a queste ultime). A ciò si aggiunga che la natura dinamica di molti algoritmi, continuamente aggiornati o variati, confligge con questa idea statica di trasparenza. Molte volte dunque non vi è accesso e se anche vi fosse accesso, il problema sarebbe costituito dalla variabilità degli algoritmi e dalla possibilità di renderli esplicabili (v. *supra*).

In tema di Big Data, la maggior criticità riguarda poi la natura indefinita delle finalità perseguite mediante il ricorso a tali strumenti. Questi ultimi consistono infatti in sistemi predittivi di elaborazione dei dati, ragion per cui – raccolte grandi quantità di dati – vengono estratte inferenze circa possibili correlazioni esistenti fra i dati esaminati, inferenze che sono quindi per loro natura imprevedibili *ex ante* al momento della raccolta[14].

Ne deriva quindi che le stesse modalità con cui il consenso viene disciplinato dalle norme vigenti paiono essere difficilmente compatibili con modelli di trattamento connotati da oscurità delle modalità (*Artificial Intelligence*) o da un'individuazione approssimativa delle finalità perseguite (Big Data). A ciò si aggiunga che vincoli di mercato, sociali e tecnologici esacerbano questa situazione con riferimento a

[13] Cfr. W.L. Perry-B. McInnis-C.C. Price-S.C. Smith-J.S. Hollywood, *Predictive Policing.The Role of Crime Forecasting in Law Enforcement Operations*, The RAND Corporation 2013, consultabile al seguente indirizzo: http://www.rand.org/content/dam/rand/pubs/research_reports/RR200/RR233/RAND_RR233.pdf

[14] In ragione dell'economia del presente scritto, per una più puntuale analisi del funzionamento degli algoritmi di *Big Data analytics* e del loro impatto sull'applicazione della disciplina sul trattamento dei dati personali si rinvia a A. Mantelero, *Big Data nel quadro della disciplina europea della tutela dei dati personali*, in V. Cuffaro-F. Di Ciommo-M.L. Gambini-A. Mantelero-R. D'Orazio (a cura di) *Trattamento dei dati personali e Regolamento UE n. 2016/679*, Milano, Wolters Kluwer, 2018, 46-60 e A. Mantelero, *Big Data: i rischi della concentrazione del potere informativo digitale e gli strumenti di controllo*, in *Dir. informaz. informatica*, 2012, 135-144. Cfr. anche volendo, più ampiamente, A. Mantelero, *Personal data for decisional purposes in the age of analytics: from an individual to a collective dimension of data protection*, in *Computer Law & Security Rev.*, 2016, 32 (2), 238-255.

molti servizi della società dell'informazione, laddove la crescente concentrazione del potere informativo, la mancanza di standard uniformi (si pensi ad esempio al settore dei dispositivi IoT) ed il cosiddetto "effetto rete", minano ulteriormente la libertà di scelta degli utenti.

Certamente i richiami alla trasparenza e le norme in materia di portabilità dei dati contenuti nel Regolamento potranno contribuire a migliorare il quadro esistente, tuttavia l'ideale degli anni '90 secondo cui il soggetto era in grado di auto-determinarsi sulla base dell'informativa ricevuta è comunque destinato ad un inevitabile superamento, come confermato anche dalle evidenze empiriche[15]. Da qui non solo la necessità di cercare di recuperare sul fronte del consenso una capacità di auto-determinazione[16], che tuttavia – a parere di chi scrive – sembra ormai quasi irrimediabilmente perduta nella prassi, ma soprattutto l'urgenza di un mutamento di prospettiva che consideri l'effettiva auto-determinazione del singolo non come meramente circoscritta al modello del consenso informato.

A tal riguardo, il dibattito dottrinale internazionale ha suggerito soluzioni alternative a quelle del modello fatto proprio dal legislatore europeo, incentrate ora su una revisione radicale del quadro esistente, volta nella sostanza a sostituire il principio di finalità su cui si regge il consenso con una nozione ampia di interesse legittimo[17], ora orientate all'adozione di forme più ampie e flessibili di consenso[18] o, infine, indirizzate a spostare l'attenzione dalle finalità

[15] Cfr. *supra* nota 5.

[16] Si pensi ad esempio all'adozione di sigilli e marchi di protezione dei dati (art. 42, Regolamento) o all'adozione di forme maggiormente incisive di informativa, cfr. Council of Europe, *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data*, IV.5.1 ed anche R.M. Calo, *Against Notice Skepticism in Privacy (and Elsewhere)*, in *Notre Dame L. Rev.*, 2013, 87(3), 1027, 1050-1055.

[17] Cfr. L. Moerel, *Big Data Protection: How to Make the Draft EU Regulation on Data Protection Future Proof*, Tilburg, Tilburg University, 2014, consultabile al seguente indirizzo: *http://www.debrauw.com/wp-content/uploads/NEWS%20-%20PUBLICATIONS/Moerel_oratie.pdf*

[18] Cfr., in tal senso, D. Hallinan-M. Friedewald-P. De Hert, *Genetic Data and the Data Protection Regulation: Anonymity, multiple subjects, sensitivity and a prohibitionary logic regarding genetic data?*, in *Comp. Law & Sec. Rev.*, 2013, 29 (4), 317-329; Kaye *et al.*, *Dynamic consent: a patient interface for twenty-first century research networks*, cit. Cfr. anche Considerando n. 33 del Regolamento.

del trattamento da indicarsi al momento della raccolta dati all'uso concreto del dato via via posto in essere[19].

Questi approcci teorici mostrano la tensione esistente in ambito accademico su come superare i limiti di un modello che, nonostante le criticità, è stato nuovamente ribadito nel Regolamento (UE) 2016/679. È tuttavia altamente improbabile che questi suggerimenti possano essere presi in considerazione dal legislatore europeo in un prossimo futuro, a causa del grande sforzo investito nel raggiungere un compromesso tra le diverse parti interessate nel testo finale del nuovo Regolamento. Da qui la necessità di guardare ad altri ambiti della regolamentazione in materia, il cui potenziale sia suscettibile di essere ampliato. È questo il caso delle disposizioni circa la gestione del rischio.

Se si muove, infatti, dall'idea che nel consenso dell'interessato è possibile ravvisare in primo luogo una forma di gestione del rischio, ovvero di quella che è poi la quintessenza della disciplina sul trattamento dati, bisogna allora guardare proprio alla valutazione del rischio per tentare di trovare una risposta alla crisi del modello esistente.

In proposito, ancorché il consenso venga prestato in ragione delle finalità del trattamento, è infatti di tutta evidenza come l'interessato non guardi alle finalità in quanto tali, ma in ragione delle conseguenze che da quest'ultime possono derivare in capo allo stesso. È dunque una dinamica di valutazione del rischio che è sottesa alla decisione inerente alla prestazione del consenso.

Con il modello in essere (consenso informato) tale dinamica è in larga parte demandata all'interessato ed alla sua valutazione, ma i fattori di complessità di cui si è detto dovrebbero indurre un movimento centrifugo che porti dall'interno (volontà dell'interessato) all'esterno (sicurezza dei modelli di trattamento dati) tale valutazione.

A ben vedere tale soluzione non è nuova, perché affine a quella in essere agli albori della rivoluzione informatica, propria delle prime

[19] Cfr. F.H. Cate-V. Mayer-Schönberger, *Data Use and Impact. Global Workshop*, The Center for Information Policy Research and The Center for Applied Cybersecurity Research, Indiana University, 2013; A. Mantelero, *The future of consumer data protection in the E.U. Rethinking the "notice and consent" paradigm in the new era of predictive analytics*, in *Comp. Law & Sec. Rev.*, 2014, 30 (6), 643-660.

generazioni di leggi sui dati personali, ove – come si è accennato – non era riconosciuto un ruolo al consenso dell'individuo, ma l'attenzione era posta sulle modalità del trattamento.

All'epoca dei primi *mainframes*, come nuovamente oggigiorno, la complessità dei trattamenti è fuori dalla portata della stragrande maggioranza delle persone e se è vero che gruppi di esperti potrebbero svolgere un ruolo sostitutivo nella valutazione degli effetti del trattamento, anche in questo caso l'attenzione passa dal consenso individuale all'analisi dei rischi. A ciò si aggiunga che oggigiorno la quantità di processi di analisi basati sui nostri dati si misura su ampia scala, rendendo pressoché improbabile una risposta alle sfide che pongono meramente incentrata sull'attivismo e sull'agire di gruppi di esperti.

In un contesto di elaborazione dati in gran parte difficilmente dominabile dal singolo, sia in termini di conoscenza che di attitudine sociale e psicologica ad interrogarsi circa il trattamento dati, appare quindi urgente passare da un modello in cui i rischi dell'uso dei dati sono valutati *ex ante* in maniera oggettiva. Questo comporta ricadute che vanno al di là della sfera meramente giuridica, poiché implica la rinuncia ad un modello di economia e società digitale che guarda alla quantità (i.e. numerosità dei servizi/prodotti offerti, rapida e continua evoluzione degli stessi) per evolvere in un più maturo modello di sviluppo che garantisca all'interessato di operare in un contesto sicuro in termini di rischio per i diritti e le libertà, nonostante questo comporti un più lungo sviluppo del prodotto.

Questo sforzo nel senso di un cambiamento di paradigma è presente *in nuce* nel Regolamento (UE) 2016/679 e, in particolare, nelle norme sulla gestione del rischio (artt. 24, 25, 35 e 36). Guardando però al riferimento a "la prova della prassi" presente nel titolo del Convegno che ha dato origine al presente volume viene da chiedersi se, ad oggi, queste disposizioni diano concretamente adito a soluzioni efficaci, tali da rispondere alle sfide del prossimo futuro. Un futuro in cui, nell'arco di pochi anni, la realtà circostante e le interazioni fra uomo ed oggetti, fra gli individui medesimi e fra le macchine saranno governate in maniera significativa da sistemi basati su algoritmi di *Artificial Intelligence*. Saranno tali sistemi a regolare dunque ampie aree della vita individuale ed associata, non solo in termini di trattamento di dati personali, ma anche e soprattutto di valori etici e sociali che necessariamente vengono incorporati nei modelli decisionali.

Di fronte a queste sfide future, il Regolamento (UE) 2016/679 sembra tuttavia uno strumento ancora immaturo, venuto alla luce negli anni in cui il pieno potenziale delle tecnologie qui esaminate era ancora in parte inesplorato. Per questa ragione l'articolato in esame offre un punto di partenza per una nuova regolazione piuttosto che una risposta concreta e puntuale agli interrogativi posti dalla società algoritmica[20].

Così, in primo luogo, l'analisi del rischio descritta nell'art. 35 del Regolamento risulta essere un procedimento largamente interno e di auto-valutazione prevalentemente incentrato sulla qualità dei dati e sulla sicurezza dei medesimi. Questo a fronte dell'impatto sociale delle tecnologie qui in esame e dei modelli di gestione del rischio elaborati in altri ambiti connotati da analogo impatto, i quali mostrano una diversa impostazione, maggiormente orientata a valorizzare la trasparenza della valutazione e la dimensione partecipativa della gestione del rischio.

In secondo luogo, con riferimento alla disamina delle diverse e potenziali conseguenze dell'impiego dei dati personali e quindi di una coerente e compiuta valutazione dei rischi correlati al trattamento, poche sono le indicazioni del Regolamento. Se è vero infatti che il Considerando n. 75, in termini di conseguenze del trattamento, fa riferimento a «qualsiasi altro danno [...] sociale significativo» e che le varie norme in materia di rischio guardano all'ampia categoria dell'impatto sui «diritti e le libertà delle persone fisiche», mancano indicazioni su come tradurre tali riferimenti in termini operativi.

In questo senso le nuove disposizioni non paiono aver mutato, per il momento, le prassi in essere con riferimento ai modelli di c.d. *impact assessment*, stando alle nuove versioni di tali modelli adottati dalle principali autorità per la protezione dei dati dei vari stati dell'Unione. Né le generiche indicazioni provenienti dal Gruppo di lavoro Articolo 29 per la protezione dei dati personali (per altro non sempre puntuali nel delineare le fattispecie concrete) sembrano offrire soluzioni operative a quanti vogliano porre in essere una reale e completa valutazione d'impatto del trattamento dati sui diritti e sulle libertà degli individui. Tantomeno sono presenti indicazioni su

[20] V. Mayer-Schönberger-Y. Padova, *Regime Change? Enabling Big Data through Europe's Data Protection Regulation*, in *Colum. Sci. & Tech. L. Rev.*, 2016, XVII, 315-35.

come adottare eventuali modelli inclusivi e partecipativi che guardino alle potenziali categorie di soggetti interessati. Si ammette anzi l'esistenza di una pluralità di possibili modelli, lasciando sulle spalle degli operatori il difficile onere di destreggiarsi fra modelli esistenti, per altro non pensati per l'ambito del trattamento dati, ma per le valutazioni di impatto sociale[21].

La rilevanza di tale attenzione alla dimensione partecipativa ed al potenziale impatto del trattamento, al di là della mera incidenza sulla sicurezza e qualità dei dati, è conseguenza dell'impiego delle soluzioni incentrate su Big Data ed *Artificial Intelligence*, laddove l'impiego di tali tecnologie comporta conseguenze che vanno al di là della sfera individuale e che, su scala collettiva[22], concernono una pluralità di diritti e libertà[23].

Guardando dunque all'interazione fra dimensione individuale e sociale, va ricordato come «l'individuo comune diventa persona con una identità propria solo nel periodo dell'Umanesimo e del Rinascimento; nei secoli anteriori, l'individuo comune "semplice numero",

[21] Cfr. dal Gruppo di lavoro Articolo 29 per la protezione dei dati personali, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*, adottate il 4 aprile 2017 e riviste in data 4 ottobre 2017, 15 («The controller must "seek the views of data subjects or their representatives" (Article 35(9)), "where appropriate". The WP29 considers that: – those views could be sought through a variety of means, depending on the context»).

[22] Cfr. A. Vedder-L. Naudts, *Accountability for the use of algorithms in a big data environment*, in *International Rev. Law, Comp. & Tech.*, 2017, 31 (29), 206-224; A. Mantelero, *From Group Privacy to Collective Privacy: Towards a New Dimension of Privacy and Data Protection in the Big Data Era*, in L. Taylor-L. Floridi-B. van der Sloot (a cura di), *Group Privacy: New Challenges of Data Technologies*, Cham., Springer International Publishing, 2017, 139-158; D. Wright-M. Friedewald, *Integrating privacy and ethical impact assessments*, in *Science and Public Policy*, 2013, 40(6), 755-766; D. Wight-E. Mordini, *Privacy and Ethical Impact Assessment*, in D. Wright-P. De Hert (a cura di), *Privacy Impact Assessment*, Dordrecht-New York, Springer Netherlands, 2012, 397-418; A.H. Vedder, *Privatization, Information Technology and Privacy: Reconsidering the Social Responsibilities of Private Organizations*, in G. Moore (a cura di), *Business Ethics: Principles and Practice*, Business Education Publishers,1997, 215-226.

[23] Stante la natura del presente contributo si rinvia alla più ampia analisi di tali nuove implicazioni svolta in A. Mantelero, *AI and Big Data: A blueprint for a human rights, social and ethical impact assessment*, in *Comp. Law & Sec. Rev.*, 2018, 34 (4), 754-772.

fa parte, della folla, dei sudditi, mentre hanno individualità solo coloro che ricoprono un potere e quindi hanno uno status nella compagine sociale»[24]. A ciò si aggiunga che un tempo «il singolo, all'atto della nascita, era collocato in una determinata casta sociale, cui erano collegati diritti e doveri, – si pensi alla posizione del "servo" nel Medioevo, di nobile, di ecclesiastico, di militare, di rentier»[25]. Solo con il tempo, con l'evolvere della società e della cultura giuridica, il singolo è uscito dalla folla indistinta e si è affrancato da uno *status* che lo connotava in maniera spesso permanente.

Rispetto a questo scenario di evoluzione storica del rapporto fra individuo e classificazioni sociali, i nuovi modelli algoritmici creano una sorta di nuovo medioevo digitale. Riemerge il rischio di una società connotata da una segmentazione per caste, ove lo *status* non è però dato dalla nascita o dall'appartenenza a classificazioni sociali tradizionali (quelle su cui vigilano le norme in materia di non-discriminazione), ma da algoritmi e dai valori di coloro che li generano. Classificazioni che sono poi impiegate per prendere decisioni che coinvolgono una pluralità di soggetti, i quali però non hanno contezza della propria posizione. È questo, ad esempio, il modello di *credit scoring* sociale in corso di elaborazione in Cina, ma anche dei meno aberranti – seppur non per questo privi di conseguenze per i singoli e la società – modelli di discriminazione algoritmica diffusi in una pluralità di processi decisionali[26].

3. La dimensione superindividuale dell'uso dei dati: verso una più ampia analisi del rischio

Da quanto brevemente esposto nel precedente paragrafo, emerge l'urgenza di porre attenzione alla dimensione superindividuale dell'uso dei dati e di coglierne le peculiarità. Una dimensione che risulta di-

[24] Cfr. G. Alpa, *La persona fisica*, in G. Alpa-G. Resta (a cura di), *Le persone fisiche e diritti della personalità*, Torino, UTET, 2006, 3.

[25] Cfr. G. Alpa, *Status e capacità*, Roma-Bari, Laterza, 1993, 15.

[26] Cfr., e.g., Federal Trade Commission, *Data Brokers: A Call for Transparency and Accountability*, 2014, consultabile al seguente indirizzo: https://www.ftc.gov/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014

versa da quelle già note in precedenza che accomunavano soggetti in posizione di squilibrio di potere (si pensi ai lavoratori, non a caso oggetto delle prime disposizioni in materia di trattamento dati adottate in Italia) o appartenenti a gruppi sociali storicamente oggetto di atti discriminatori (gruppi religiosi o etnici, ad esempio).

Nel caso della discriminazione su base algoritmica, i soggetti in questione appartengono a classi generate dai creatori degli algoritmi o generate dagli algoritmi medesimi attraverso processi di *machine learning*. Tali soggetti, così aggregati, non sanno di appartenere ad una data classe, né conoscono gli altri individui accomunati dalla stessa classificazione, la quale può inoltre mutare – anche frequentemente – in ragione del variare del comportamento soggettivo o di gruppo.

In questo contesto, qui brevemente delineato[27], emerge dunque l'ulteriore limite che incontra il Regolamento nell'affrontare le dinamiche della società algoritmica, la quale richiede – quantomeno sul piano rimediale – di elaborare soluzioni atte a rappresentare ed a tener in debito conto le esigenze e implicazioni collettive del trattamento dati.

Da qui la necessità di muovere verso una visione più ampia dell'analisi del rischio, che, in linea con la traiettoria indicata dal Regolamento (ma non ancora adeguatamente sviluppata), vada oltre una mera attenzione ai dati e consideri le implicazioni che l'uso degli stessi può avere sulla società. Occorre dunque elaborare modelli più articolati di analisi che guardino ai diritti umani in generale e non solo alla tutela dei dati personali[28], traducendo in maniera operativa le indicazioni presenti solo *in nuce* nel Regolamento.

In linea con le sollecitazioni provenienti da varie fonti[29] è poi opportuno adottare una più ampia visione che non si limiti a considerare

[27] Per una più ampia disamina si rinvia alle considerazioni espresse in A. Mantelero, *Personal data for decisional purposes in the age of analytics: from an individual to a collective dimension of data protection*, cit.

[28] Cfr. A. Mantelero, *AI and Big Data: A blueprint for a human rights, social and ethical impact assessment*, cit.

[29] Cfr., e.g., EDPS - Ethics Advisory Group, Towards a digital ethics, 2018, consultabile al seguente indirizzo: *https://edps.europa.eu/sites/edp/files/publication/18-01-25_eag_report_en.pdf*; Council of Europe-Committee of experts on internet intermediaries (MSI-NET), *Study on the Human Rights Dimensions of Automated Data Processing Techniques (in Particular Algorithms) and Possible*

l'impatto sui diritti e sulle libertà ma tenga altresì conto dell'impatto etico e sociale delle scelte concernenti il demandare ad algoritmi l'assunzione di decisioni basate sui dati personali. La conformità alla legge non esclude, infatti, di per sé un giudizio di opportunità delle scelte da adottarsi, guardando ai valori etici e sociali di una comunità. Questo specie in presenza di sistemi algoritmi chiamati a concorrere nei processi decisionali riguardanti aspetti di rilievo per i singoli ed i consociati.

In questo senso, le *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data* adottate nel 2017 dal Consiglio d'Europa[30] hanno sottolineato la necessità che «Personal data processing should not be in conflict with the ethical values commonly accepted in the relevant community or communities and should not prejudice societal interests, values and norms, including the protection of human rights».

Proprio la complessità di questa diversa e più ampia valutazione dovrebbe valorizzare l'adozione di un approccio partecipativo all'analisi del rischio, non solo in quanto più compiuta espressione del diritto dei consociati a prendere parte alle decisioni che li riguardano, ma anche quale mezzo per superare le limitazioni (*bias*) che sovente affliggono le logiche proprie di chi crea i sistemi algoritmici. Non si può infatti immaginare che gli sviluppatori di tali sistemi – sovente espressione di una limitata parte della società per formazione, estrazione sociale e culturale, origine geografica e genere – possano definire in maniera autoreferenziale e senza rischio di distorsioni implicite i valori che vengono ad essere codificati negli algoritmi impiegati per governare le società. Da qui la necessità di ampliare la valutazione del rischio e di renderla operativa anche mediante il ricorso a comitati di esperti o comitati etici portatori di ulteriori e

Regulatory Implications, 2018, consultabile al seguente indirizzo: *https://rm.coe.int/algorithms-and-human-rights-en-rev/16807956b5;* Access Now, The Toronto Declaration: Protecting the rights to equality and non-discrimination in machine learning systems, 2018, consultabile al seguente indirizzo: *https://www.accessnow.org/the-toronto-declaration-protecting-the-rights-to-equality-and-non-discrimination-inmachine-learning-systems/*

[30] Il testo delle linee guida è consultabile al seguente indirizzo: *https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806ebe7a*

più specifiche competenze atte a considerare le ricadute sociali delle soluzioni tecnologiche elaborate[31].

Nel concludere queste brevi note si possono richiamare alla memoria le parole di Norberto Bobbio che, benché risalenti, paiono ancora vive nell'additare i rischi dell'evoluzione della società della tecnologia: «l'ideale del potente è sempre stato quello di vedere ogni gesto e di ascoltare ogni parola dei suoi soggetti (possibilmente senza essere visto né ascoltato): questo ideale oggi è raggiungibile [...] La vecchia domanda che percorre tutta la storia del pensiero politico: "Chi custodisce i custodi?" oggi si può ripetere con quest'altra formula: "Chi controlla i controllori?" Se non si riuscirà a trovare una risposta adeguata a questa domanda, la democrazia, come avvento del governo visibile, è perduta. Più che di una promessa non mantenuta si tratterebbe in questo caso addirittura di una tendenza contraria alle premesse: la tendenza non già verso il massimo controllo del potere da parte di cittadini ma al contrario verso il massimo controllo dei sudditi da parte del potere»[32].

Rispondendo a questo interrogativo ed estendendolo ad una figura di potente che non è più ristretta al solo ambito pubblico, ma comprende anche i nuovi e, per molti versi, più forti poteri privati che l'economia digitale ha contribuito a generare, occorre guardare alla nozione di rischio ed operare affinché vengano realizzati ambienti digitali sicuri. Ove la sicurezza non è più la mera sicurezza informatica o la sicurezza del processo di trattamento dati, ma è la sicurezza che deriva dalla garanzia del rispetto dei diritti e delle libertà fondamentali. Solo in questa maniera il primato dell'Unione Europea nel regolare il trattamento dei dati personali potrà rimanere tale, mantenendo fermo un paradigma valoriale, in cui la tutela dei diritti e libertà dei singoli e della collettività prevale su modelli di innovazione dominati dalle dinamiche di mercato.

[31] Cfr. A. Mantelero, *AI and Big Data: A blueprint for a human rights, social and ethical impact assessment*, cit.

[32] N. Bobbio, *Il futuro della democrazia*, Einaudi, Torino, 1995, 19.

La portabilità dei dati tra privacy e regole del mercato

Guido Scorza

Sommario: 1. Introduzione – 2. L'interpretazione estensiva del diritto alla portabilità dei dati proposta dal Gruppo ex art. 29 – 3. I rischi connessi alla moltiplicazione dei dati al loro trattamento al di fuori del controllo dell'interessato e del titolare – 4. Portabilità e regole antitrust – 5. Conclusioni

1. Introduzione

L'articolo 20 del regolamento generale sulla protezione dei dati (GDPR) introduce il nuovo diritto alla portabilità dei dati. Tale diritto, come è noto, consente all'interessato di ricevere i dati personali forniti a un titolare, in un formato strutturato, di uso comune e leggibile da dispositivoautomatico, e/o di otterne la trasmissione direttamente a un altro titolare del trattamento.

«Il diritto in questione – secondo le linee guida del Gruppo di lavoro art. 29 adottate il 13 dicembre 2016 e, successivamente, emendate il 5 aprile 2017 – è soggetto a determinate condizioni e mira a promuovere la libertà di scelta degli utenti, il loro controllo sui trattamenti e i loro diritti».

Lo stesso Gruppo art. 29, nel tracciare il perimetro del diritto in questione chiarisce che «seppure il diritto alla portabilità possa fungere da fattore di promozione della concorrenza fra i singoli servizi proprio perché facilita il passaggio da un servizio all'altro, il GDPR disciplina il trattamento dei dati personali e non la concorrenza fra imprese».

Una norma in materia di privacy più che di mercato, quindi.

Si tratta, naturalmente, di una conclusione in linea teorica incontrovertibile sotto il profilo sistematico stante, appunto, la sua collocazione all'interno del GDPR.

Se, tuttavia, ci si muove dalla teoria alla pratica e dalla sistematica alla valutazione degli effetti possibili derivanti dall'applicazione della disposizione di legge in commento – che si tratti di conseguenze volute o non volute, ponderate o non ponderate – è difficile negare che la disposizione in questione mentre, allo stato, appare idonea ad aggiungere poco al diritto di accesso già riconosciuto agli interessati dalla precedente Direttiva 95/46/CE e, oggi, confermato come diritto centrale nel nuovo sistema di protezione dei dati personali regolato dal GDPR, appare, invece, destinata a produrre effetti significativi sui mercati.

Con un mercato dei dati – anche personali – che, nella sola Unione europea, oggi vale 60 miliardi di euro e che nel 2020 è festinato a sfondare la soglia dei 106 miliardi di euro diviso tra grandi oligopoli – nella più parte dei casi extra-europei – è, infatti, evidente che la disposizione in commento sia destinata a diventare uno strumento di mercato, offensivo o difensivo, a seconda dei casi ed a incidere significativamente sulla libera circolazione dei dati che, per inciso, costituisce la "cenerentola" degli obiettivi perseguiti dalla nuova disciplina europea della materia.

È, infatti, facile prevedere che il diritto alla portabilità dei dati sia destinato a essere utilizzato più che "dagli" interessati, "attraverso" gli interessati, dai titolari del trattamento il cui business dipende, in misura diversa, dalla capacità di accumulare grandi quantità di dati personali e di analizzarli al fine di costruire profili sempre più attendibili di utenti e consumatori e/o implementare i propri modelli di business.

In questa prospettiva – e si tratta della tesi centrale di questo breve intervento – il dubbio che sorge è che il diritto alla portabilità dei dati potrebbe finire con il produrre effetti e conseguenze contrapposti rispetto a quelli sperati in termini di protezione dei dati personali e, forse, conseguenze non adeguatamente ponderate sui mercati.

2. L'interpretazione estensiva del diritto alla portabilità dei dati proposta dal Gruppo *ex* art. 29

L'art. 20 GDPR, secondo l'interpretazione letterale del suo contenuto, dovrebbe riconoscere all'interessato esclusivamente il diritto di ottenere dal titolare del trattamento «i dati personali che lo riguardano forniti a un titolare del trattamento» e, peraltro, ciò a condizione che l'esercizio del diritto in questione non leda i diritti e le libertà altrui come, in linea di principio, potrebbe accadere ogni qualvolta l'accoglimento di un'istanza di portabilità da parte di un interessato imponga il trasferimento da un titolare a un altro anche di dati personali di soggetti terzi, a loro insaputa.

Come è noto, il Gruppo *ex* art. 29, attraverso le sue richiamate linee guida ha, tuttavia, proposto un'interpretazione estensiva del contenuto della norma, stabilendo, innanzitutto, che «questo nuovo diritto non può essere svuotato di contenuto limitandolo ai dati personali che sono comunicati direttamente dall'interessato, per esempio compilando un modulo online» e, suggerendo, pertanto che «In linea di principio e alla luce delle finalità sottese al diritto alla portabilità dei dati, l'espressione "forniti dall'interessato" deve essere interpretata in modo estensivo escludendo unicamente "dati inferenziali" e "dati derivati", i quali comprendono i dati personali generati da un fornitore di servizi (per esempio, i risultati prodotti da un algoritmo)».

Si tratta di una prospettiva interpretativa che amplia – e anzi trasforma – in maniera significativa la portata della disposizione suggerendo di passare da una sua lettura in termini di norma eccezionale applicabile solo a una categoria eccezionale di dati personali – quelli, appunto, forniti dall'interessato al titolare del trattamento – a una sua lettura in termini di generale applicazione salvo un'unica eccezione: quella relativa ai dati inferenziali e derivati attraverso l'applicazione di algoritmi e *know how* del titolare del trattamento.

Ma l'interpretazione estensiva della norma proposta dal Gruppo art. 29 non si ferma a tale previsione.

Anche l'ultimo comma dell'art. 20, infatti, ha formato oggetto di una generosa proposta interpretativa in forza della quale la semplice circostanza che, in attuazione di un'istanza di portabilità, possa rendersi necessario trasferire da un titolare a un altro dati

personali di soggetti terzi rispetto all'interessato non può essere sufficiente a considerare detta istanza inaccoglibile in quanto suscettibile di determinare una lesione dei diritti e delle libertà dei terzi.

Tale interpretazione estensiva della norma in questione, ovviamente, amplifica le perplessità espresse nel paragrafo che precede perché aumenta sensibilmente la quantità e tipologia dei dati destinati a trovare nell'art. 20 GDPR la base giuridica per una loro moltiplicazione e circolazione tra una pluralità di titolari del trattamento diversi.

E, d'altra parte, che lo stesso Gruppo art. 29, sebbene implicitamente e, anzi, forse affermando, a livello di petizione di principio, l'esatto contrario, guardi alla norma in questione come un veicolo concorrenziale più che di protezione dei dati personali, è suggerito da taluni degli esempi proposti nelle stesse linee guida.

In questo contesto il più esemplificativo è probabilmente quello che ipotizza il trasferimento, da un titolare all'altro, delle playlist musicali composte dall'interessato attraverso i servizi di un determinato fornitore.

Si tratta di un'ipotesi nella quale mentre il valore – in termini di privacy – dei dati oggetto di istanza di portabilità appare modesto, il loro valore in termini di mercato appare significativo consentendo, nella sostanza, a un fornitore di servizi di *streaming* musicale concorrente quello con il quale l'interessato ha in essere un rapporto di offrirgli un servizio a condizioni sostanzialmente identiche facendo, anzi, tesoro di quanto su tale interessato, il primo titolare del trattamento ha appreso nel corso del relativo rapporto.

Ma, a prescindere dagli esempi, nelle linee guida si annota espressamente che «l'aspettativa [ndr legata al diritto alla portabilità] è che, oltre ad ampliare il margine di controllo dei consumatori impedendo forme di "lock-in" tecnologico, il diritto alla portabilità dei dati promuova l'innovazione e la condivisione di dati personali fra titolari del trattamento in piena sicurezza e sotto il controllo dell'interessato. Il diritto alla portabilità può favorire la condivisione controllata e limitata delle informazioni personali fra più soggetti e, quindi, arricchire l'esperienza dell'utente nella fruizione di determinati servizi8. La portabilità, inoltre, può favorire la trasmissione e il riutilizzo di dati personali fra più servizi di interesse per il singolo utente».

Come si dirà meglio nel paragrafo successivo, a ben vedere, non sembrano mancare motivi per non condividere, fino in fondo, l'ottimismo del Gruppo art. 29 su tale punto.

3. I rischi connessi alla moltiplicazione dei dati al loro trattamento al di fuori del controllo dell'interessato e del titolare

L'attuazione dell'art. 20 GDPR ha come naturale conseguenza la moltiplicazione delle copie dei dati personali oggetto di un trattamento.

I dati personali oggetto di un'istanza di portabilità, infatti, mentre continuano, normalmente – salvo contestuale richiesta di cancellazione – a essere trattati dal titolare originario finiscono, a seconda dei casi, archiviati sul dispositivo dell'interessato o sui server del titolare autonomo del trattamento destinatario del servizio.

In entrambi i casi, se si esce dalla dimensione teorica e si entra nella dimensione pratica, sussiste un rischio concreto che i dati personali siano esposti a minacce superiori rispetto a quelle cui sarebbero rimasti esposti in assenza di esercizio del diritto alla portabilità.

Nel primo caso, ovvero qualora i dati sono esportati dal titolare, fornitore di un servizio all'interessato tale rischio è conseguenza diretta di una duplice circostanza: (a) innanzitutto i dati personali una volta entrati nella disponibilità esclusiva dell'interessato, essendo trattati, ovviamente, in un contesto personale, sono sottratti all'ambito di applicazione del Regolamento e ciò sia in relazione ai dati personali dell'interessato che a quelli di eventuali terzi e (b) l'interessato, naturalmente, anche a prescindere dalla disciplina applicabile o non applicabile al trattamento in questione, normalmente, non dispone di sistemi e misure di sicurezza affidabili e "sicuri" quanto quelli del titolare del trattamento che originariamente li trattava.

Nel secondo caso giacché l'art. 20 non si preoccupa di dettare le modalità di attuazione del diritto alla portabilità nell'ipotesi di trasferimento da titolare a titolare, sussiste – e, allo stato, appare elevato – il rischio che il titolare del trattamento di destinazione, che nella costruzione della previsione regolamentare può essere e restare completamente all'oscuro della richiesta dell'interessato di fargli ricevere i dati del titolare del trattamento, non sia preparato all'ac-

quisizione dei dati ricevuti dal titolare originario del trattamento, alla loro conservazione e gestione.

Si tratta di un profilo di criticità importante.

È, infatti, ovvio che il titolare del trattamento mittente nel trasmettere i dati al titolare del trattamento ricevente non assume alcuna responsabilità in ordine all'autonomo trattamento che quest'ultimo, ricevuti i dati, porrà in essere.

Il titolare del trattamento destinatario, dal canto suo, benché sotto il profilo strettamente normativo sia, evidentemente, tenuto a ispirare il trattamento dei dati ricevuti al rispetto della disciplina vigente, nella pratica, sarà spesso impossibilitato ad adempiere tempestivamente agli obblighi nascenti da tale disciplina perché è possibile che non abbia, come si è anticipato, nessuna informazione relativa alla qualità e quantità dei dati oggetto di portabilità in proprio favore.

In questo senso la nuova disciplina di cui all'art. 20 è sensibilmente diversa rispetto a quella, sulla quale si tornerà più avanti, in materia di portabilità dei numeri telefonici giacché nell'ambito di quest'ultima, la portabilità è attivata dall'operatore telefonico di destinazione e, dunque, in nessun caso questi può trovarsi a "subire" la portabilità senza esserne consapevole.

In tale contesto, ad esempio, farà, ovviamente, difficoltà a garantire il rispetto dei principi di pertinenza e non eccedenza giacché dovrà prima archiviare e esaminare le informazioni ricevute e, solo in un secondo momento, potrà procedere alla cancellazione di quelle non necessarie.

In sede di ricevimento delle informazioni in questione, tuttavia – salva l'ipotesi nella quale la portabilità sia stata sollecitata dal titolare del trattamento ricevente e i due titolari del trattamento abbiano raggiunto tra di loro uno specifico accordo connesso al trasferimento e alla raccolta dei dati in questione – il titolare del trattamento ricevente si troverà a violare la disciplina in materia di privacy non potendo disporre dell'organizzazione e dei processi necessari a garantire l'immediata cancellazione dei dati in eccesso.

In linea di principio, ovviamente, il titolare del trattamento destinatario potrebbe anche rifiutare l'acquisizione in tutto o in parte dei dati oggetto di portabilità.

Il regolamento, tuttavia, non prevede se e quanto selettiva possa essere la richiesta di portabilità dall'interessato al titolare originario

ovvero se quest'ultimo possa considerarsi obbligato a trasmettere a un autonomo titolare del trattamento individuato dall'interessato anche una selezione dei dati da esso trattati.

In tale contesto è difficile escludere che l'esercizio del diritto alla portabilità, nella forma di richiesta di trasferimento da titolare a titolare non esponga i dati personali dell'interessato a taluni rischi diversi ed ulteriori rispetto a quelli che avrebbero corso qualora il trattamento fosse semplicemente proseguito sotto il controllo esclusivo del titolare originario del trattamento.

Anche le considerazioni svolte, al riguardo, nelle linee guida del Gruppo art. 29 appaiono poco utili giacché esse si limitano a prevedere che «Il soggetto ricevente assume il ruolo di titolare nei riguardi dei dati personali in questione ed è tenuto all'osservanza dei principi fissati nell'art. 5 del RGPD. Ne deriva che il nuovo titolare ricevente deve specificare con chiarezza le finalità di ogni nuovo trattamento prima che sia formulata la richiesta di trasmissione diretta dei dati portabili, conformemente con i requisiti di trasparenza fissati all'art. 12 del regolamento. Come per qualunque altra operazione di trattamento svolta sotto la sua responsabilità, il titolare dovrà applicare i principi di cui all'art. 5 del RGPD – quali liceità, correttezza e trasparenza, limitazione della finalità, minimizzazione dei dati, esattezza, integrità e riservatezza, conservazione limitata e responsabilizzazione».

Ciò, tuttavia, è difficilmente conciliabile con la lettera dell'art. 20 che, come si è anticipato, non prevede che tra titolare del trattamento mittente e trattamento del mittente destinatario vi debba essere un qualche specifico accordo né subordina l'accoglibilità dell'istanza rivolta dall'interessato all'originario titolare del trattamento a una preventiva richiesta – o anche semplice interlocuzione – tra l'interessato medesimo e il titolare del trattamento destinatario della trasmissione dei dati.

Forse, sotto questo profilo, sarebbe stato opportuno che l'art. 20 subordinasse il trasferimento dei dati personali oggetto di portabilità a un preventivo accordo tra i due titolari dei trattamenti ovvero tra il mittente e il destinatario.

La tensione tra diritto alla portabilità, sicurezza e protezione dei dati personali, d'altra parte, non può considerarsi una novità assoluta trattandosi di un fenomeno già emerso – in Europa e all'estero – tra le diverse forme di diritto di accesso e, appunto, la sicurezza dei dati.

Già nel 2000, ad esempio, negli Stati Uniti, il *Federal Trade Commission Advisory Committeee* riferiva al Congresso circa l'esistenza di "una vera e propria tensione" tra diritto di accesso e sicurezza dei dati personali *(Final Report of the Federal Trade Commission Advisory Committee on Online Access and Security 19-25, May 2000*).

È, d'altra parte, in dottrina è già stato rilevato che la nuova disciplina sulla portabilità, per come è strutturata, «è idonea a creare problemi quali privacy e sicurezza»[1]. Questo perché «se i dati sono portabili, una singola frode può tradursi in una duratura violazione dei dati personali»[2].

4. Portabilità e regole antitrust

Come si è anticipato nei paragrafi precedenti è circostanza pacifica che il diritto alla portabilità dei dati abbia almeno, se non per scopo, per effetto quello di intervenire sui mercati dei dati personali come strumento anti *lock-in* e come leva proconcorrenziale.

In questo senso, benché il Gruppo *ex* art. 29 ne sottolinei la natura di disciplina in materia di privacy più che di concorrenza, non appare possibile sottrarsi alla valutazione dell'art. 20 anche nella prospettiva antitrust.

D'altra parte l'istituto più prossimo rispetto a quello introdotto nell'Ordinamento europeo con la disposizione in esame è, inequivocabilmente, quello della c.d. "portabilità dei numeri telefonici" previsto dalla direttiva 2002/22/CE (direttiva 2002/22/CE del Parlamento europeo e del Consiglio, del 7.3.2002, "Direttiva Servizi Universali").

In particolare, come è noto, all'art. 30, la direttiva prevede il diritto per l'utente di cambiare operatore telefonico, mantenendo tuttavia il numero precedente.

Per questa via l'istituto contribuirebbe a riequilibrare il libero gioco della concorrenza e a prevenire possibili abusi di posizione dominante da parte degli operatori più in posizione di forza sui rispettivi mercati.

[1] E. Pelino, *Diritti di controllo*, in L. Bolognini, E. Pelino, C. Bistolfi, *Il Regolamento privacy europeo*, Milano, Giuffrè, 2017, 247.

[2] T.E. Jouglux, P. Markou, C. Prastitou, EU Internet Law: Regulation and enforcement, Springer, 2017.

Ai fini di questo breve intervento e della tesi in esso sostenuta, tuttavia, è opportuno tener presente che la citata previsione sulla portabilità dei numeri telefonici è applicabile a un singolo mercato predeterminato, mercato che riguarda la fornitura di servizi qualificati come "universali" nell'Ordinamento europeo e non è quindi – a differenza di quanto accade nel caso della disposizione del GDPR in esame – destinata a trovare generalizzata applicazione su più mercati.

Si tratta, d'altra parte, di una conclusione cui, anche in dottrina, si è già pervenuti[3].

E letta in questa prospettiva la disposizione in esame lascia perplessi e solleva talune preoccupazioni.

L'art. 20, innanzitutto, impone, nella sostanza, a qualsiasi titolare del trattamento che nell'esercizio della sua attività di impresa abbia raccolto direttamente dall'interessato o da terzi importanti quantità di dati personali di porli a disposizione di qualsiasi concorrente al quale l'interessato medesimo gli chieda di trasmetterli.

Tale obbligo prescinde completamente dalla posizione occupata dal titolare del trattamento originario sul mercato ovvero si applica a prescindere dalla circostanza che tale imprenditore si trovi in una posizione dominante oppure no e abbia posto in essere, oppure no, qualsiasi genere di comportamento escludente.

Si tratta, evidentemente, di un importante elemento di rottura rispetto alla disciplina antitrust nell'ambito della quale un intervento di compressione dell'*asset* di un'impresa non sarebbe in alcun caso ipotizzabile qualora tale azienda non occupasse una posizione dominante sul mercato considerato e di tale posizione non avesse in qualche modo abusato attraverso comportamenti escludenti nei confronti dei concorrenti.

In questa prospettiva l'assetto del diritto alla portabilità non convince né in una prospettiva teorica, né in una prospettiva pratica.

Sotto il primo profilo è evidente che la raccolta di dati personali di consumatori e utenti costituisce sui mercati un obiettivo in vista del cui raggiungimento le imprese investono risorse importanti e costituisce ragione di investimento in ricerca e sviluppo finalizza-

[3] A.D. Vanberg - M.B. Unver, *The right to Data Portability in the GDPR and EU Competition Law: odd couple or dynamic duo?*, VIII, in *European J. Law & Tech.*, 2017, 6.

ti alla realizzazione di soluzioni informatiche capaci di garantire il conseguimento del predetto obiettivo.

In questo contesto l'esistenza di taluni *switching cost* rappresenta essa stessa un incentivo agli investimenti.

Tanto per intendersi, infatti, difficilmente gli attuali oligopolisti del mercato dei dati avrebbero, negli anni, investito le ingenti risorse invece investite nella realizzazione delle proprie piattaforme in presenza di una norma che, semplificando un problema evidentemente più complesso, nella sostanza riconosce ai loro titolari il diritto di "espropriarli" del loro *asset* più prezioso: i dati personali dei propri utenti.

In questo senso, ad esempio, si è già espressa parte della dottrina[4].

Se, tuttavia, la circostanza che l'art. 20 del GDPR possa costituire strumento di erosione di oligopoli dei dati personali come quelli formatisi in capo alle grandi piattaforme online può, in una certa misura considerarsi effetto auspicabile e, anzi, voluto dal legislatore europeo, la circostanza che, la stessa disposizione, possa produrre analoghi effetti di svalutazione degli assets rappresentati dai giacimenti di dati personali raccolti da soggetti privi di analoga posizione dominante sui diversi mercati è motivo di preoccupazione e rappresenta, probabilmente, effetto non voluto, non adeguatamente ponderato e indesiderato.

In assenza dei tre requisiti che nell'ambito del diritto antitrust presidiano, di norma, all'attuazione di iniziative di "espropriazione" o "compressione" di *assets* aziendali – ovvero la posizione dominante dell'imprenditore, il suo coinvolgimento in comportamenti escludenti e, infine, l'esistenza di una condizione di inefficienza delle dinamiche di mercato – l'applicazione della nuova disposizione minaccia di produrre effetti idonei a comprimere gli investimenti e lo sviluppo tecnologico.

Sotto il secondo profilo – ovvero quello pratico – è, allo stato, almeno lecito dubitare della circostanza che la disposizione in oggetto sia effettivamente in grado di produrre l'effetto "politicamente" auspicato cui si è fatto cenno ovvero quello redistribuzione degli immensi giacimenti di dati personali oggi detenuti dagli oligopolisti dei mercati.

[4] P. Swire - Y. Lagos, *Why the right to data portability likely reduces consumer welfare: antitrust and privacy critique*, 72 *Maryland L. Rev.*, 2013, 335.

L'osservazione dei mercati più interessati dall'applicazione della norma, infatti, suggerisce che proprio i gestori delle grandi piattaforme rappresentino i soggetti che più e meglio di ogni altro saranno in grado di mettere a profitto il nuovo strumento della portabilità dei dati inducendo i propri utenti – attraverso adeguate politiche commerciali – a invertire la direzione dei flussi di dati personali: dagli altri soggetti detentori minori verso gli oligopolisti anziché viceversa.

In questa prospettiva di indagine occorre, in particolare, tener presente che i gestori delle grandi piattaforme, per un verso, dispongono di tecnologie e interfacce attraverso le quali, più facilmente, suggerire agli utenti di delegarli alla raccolta – dai fornitori di altri servizi [energia elettrica, acqua, telecomunicazioni, editori ecc.] dei dati personali che li riguardano e da questi ultimi trattati.

E, nella medesima prospettiva, occorre altresì tener presente l'ormai nota crisi degli strumenti negoziali tradizionali e, in particolare, del consenso: nella società dell'accetta e continua – come è già stata definita l'epoca che stiamo vivendo – infatti, sarà straordinariamente facile, soprattutto per i più grandi, "carpire" una richiesta di portabilità dei dati da rivolgere ai predetti fornitori terzi dai propri utenti.

Un esempio, sul punto, varrà a chiarire lo scenario, assai poco rassicurante, del quale l'art. 20 del GDPR potrebbe costituire involontaria base giuridica: se Facebook domani volesse, non faticherebbe molto a inserire nel proprio flusso di iscrizione ai propri servizi, una delega a richiedere telematicamente – per conto dei propri utenti – i dati personali a questi ultimi riferibili detenuti da fornitori terzi di diversi servizi, ad esempio una banca, dei quali gli utenti si servono.

In questo modo si assisterebbe a una convergenza sempre maggiore di dati personali sulle grandi piattaforme e a un conseguente rafforzamento degli oligopoli da loro detenuti.

5. Conclusioni

La strada segnata dall'art. 20 del GDPR è, probabilmente, la strada giusta. La norma in questione, infatti, appare, effettivamente, dotata di grandi potenzialità in termini di garanzie riconosciute agli utenti dal rischio di *lock-in* identitari ovvero dal rischio che le loro identità

in digitale diventino ostaggio delle grandi piattaforme online che, nella sostanza, potrebbero garantirsene la sempiterna fedeltà come utenti semplicemente rendendo difficile la migrazione su piattaforme concorrenti.

Allo stesso tempo, tuttavia, è innegabile che la disposizione in questione – probabilmente l'unica nell'intero GDPR che manca completamente di qualsivoglia "sperimentazione" a livello nazionale – evidenzi talune criticità legate, in particolare, al rischio – comunque per la verità a quello sollevato dal diritto di accesso ma, nella portabilità indiscutibilmente accresciuto – di una moltiplicazione incontrollata e incontrollabile delle basi di dati personali destinate a essere presidiate non sempre a un adeguato livello di sicurezza e a non essere sempre trattati nei rispetto della disciplina vigente.

E, egualmente, la norma in questione fa fatica – e farà sempre più fatica in futuro – a scrollarsi di dosso quel carattere di "*dual use*", una norma geneticamente concepita nella dimensione della disciplina sulla protezione dei dati personali ma destinata a produrre effetti – forse quelli più rilevanti – come se si trattasse di una disposizione di diritto antitrust del quale, tuttavia – in ragione del suo ambito di applicabilità generalizzato – viola alcuni principi consolidati.

GDPR e Intelligenza Artificiale: i primi passi tra *governance*, privacy, trasparenza e *accountability*

Matteo Trapani

Sommario. 1. I sistemi di intelligenza artificiale e la loro applicazione alla PA – 2. Il GDPR e la spirale pubblicistica dei dati – 3. *Governance*, *accountability* e trasparenza: una dimensione costituzionale collettiva – 4. Alcune questioni ancora aperte e l'uscita dalla caverna

«è esso a produrre le stagioni e gli anni
e a governare tutte le cose del mondo
visibile e ad essere causa, in certo modo
di tutto quello che egli e i suoi compagni
vedevano»
Platone, *La Repubblica*, Libro VII

1. I sistemi di intelligenza artificiale e la loro applicazione alla PA

I sistemi di intelligenza artificiale rappresentano un importante strumento al servizio della Pubblica Amministrazione (di seguito PA) che possono determinare importanti effetti sull'efficienza, sull'efficacia e sulla trasparenza[1].

[1] Numerosi gli studi che analizzano l'impatto dei sistemi di IA. Tra i molti, si ricordano H. Mehr, *Artificial Intelligence for Citizen Services and Government*, Harvard Ash Center for Democratic Governance and Innovation, 2017; G.N. Kouziokas,

La definizione di Intelligenza Artificiale (di seguito IA) è ad oggi controversa[2] così come lo è la sua evoluzione scientifica[3]. Dalla difficoltà definitoria e dalla complessa evoluzione scientifica dipendono le difficoltà da parte del legislatore di poter creare un complesso di norme che ne disciplinino l'utilizzo limitandone le criticità e promuovendone le potenzialità[4].

Le applicazioni dell'IA alla PA sono molteplici e rispondono a svariate esigenze collegate ad altrettanti diritti che ne consolidano la necessità di una loro regolamentazione.

La maggiore innovazione che i sistemi di IA hanno introdotto è rappresentata dalla potenzialità diffusa di elaborazione, ricerca, interconnessione ed analisi dei dati presenti non solo sul territorio nazionale ma in luoghi spesso lontani tra loro.

Esistono sostanzialmente tre gradi di coinvolgimento di questi sistemi nei procedimenti amministrativi: un primo di supporto, un secondo di integrazione ed un terzo di sostituzione.

Nel primo caso mediante queste tecniche è possibile potenziare l'azione dell'amministrazione creando l'effetto di una "burocrazia

The application of artificial intelligence in public administration for forecasting high crime risk transportation areas in urban environment, 2017; The White House, *Artificial Intelligence, Automation, and the Economy*, 2016.

[2] Si vedano, ad esempio, le definizioni della Stantford University in *Artificial Intelligence and life in 2030. One hundred year study on Artificial Intelligence* (IA come scienza ed insieme di tecniche computazionali che vengono ispirate dal modo in cui gli esseri umani utilizzano il proprio sistema nervoso e il proprio corpo per sentire, imparare, ragionare e agire) e dell'Oxford Dictionary (la teoria e lo sviluppo di sistemi informatici in grado di svolgere compiti che normalmente richiedono l'intelligenza umana, come la percezione visiva, il riconoscimento vocale, il processo decisionale e la traduzione tra le lingue).

[3] Si faccia riferimento a G. Italiano, *Intelligenza Artificiale: passato, presente, futuro*, in F. Pizzetti (a cura di), *Intelligenza Artificiale, protezione dei dati personali e regolazione*, Torino, Giappichelli, 2018, 207 ss.

[4] Si veda sul tema generale U. Pagallo, *Il diritto nell'età dell'informazione*, Torino, Giappichelli, 2014; specificamente sull'IA F. Rossi, *Intelligenza Artificiale benefica e sicura: iniziative accademiche, governative e industriali*, in *Sistemi Intelligenti*, il. Mulino, 3/2017, 545 ss.; A. Santosuosso-C. Boscarato-F. Caroleo, *Robot e diritto: una prima ricognizione, in La nuova giurisprudenza civile commentata*, 2012, 494 ss.; C. Salazar, *Umano… troppo umano o no? Robot, androidi e cyborg nel "mondo del diritto"*, in *BioLaw Journal*, 1/2014, 259 ss.

aumentata" che, non sostituendosi in alcun modo al ruolo del funzionario pubblico, trova nelle tecnologie informatiche un incremento delle proprie qualità di azione.

Nel secondo è la PA che cede il passo a tecniche di IA che integrano l'azione amministrativa con lo scopo di colmare il differenziale tra il risultato atteso e quello effettivo, in relazione ad una spesa definita. In questo caso i sistemi di IA possono soddisfare esigenze che il solo agire del funzionario pubblico potrebbe disattendere data la difficoltà da parte dell'essere umano di compiere alcune azioni o la possibilità che queste azioni siano compiute con ritardo.

Un terzo grado, senza dubbio quello che produce i maggiori effetti sia sulla PA che su questioni quali la trasparenza o la privacy, è l'integrale sostituzione dei procedimenti della PA con azioni compiute da sistemi di IA. Questo livello porta molteplici criticità legate sia al fatto che l'eventuale soddisfacimento di interessi legittimi, e di diritti connessi, sarà possibile solo a seguito di una azione completamente automatizzata e programmata da chi non fa parte della PA, con difficoltà nella stessa attribuzione della responsabilità oltre che della legittimità amministrativa, sia alla necessità che un tale procedimento venga normato in via diretta e non segua la disciplina che deriva, in via giurisprudenziale, da questioni similari ma non del tutto assimilabili.

Le questioni che si pongono sono di natura pubblicistica interessando numerosi temi che intrecciano senza dubbio gli elementi costitutivi della *governance* dello Stato e, più in generale, alterano i principi e le garanzie previste in Costituzione.

Una PA che agisce mediante sistemi di IA altera, potenziandola, la propria attività sul territorio, potendo facilmente accedere ad informazioni e compiere azioni che vanno ben oltre al territorio nazionale. Viene modificato lo stesso funzionamento della PA, dalla quale deriva sia la garanzia del principio di legalità che la previsione di una legittimità funzionale del decisore legata ad un necessario accesso per concorso (politica nel caso in cui si tratti di competenza dei rappresentanti politici) e rispetto delle regole di andamento che il funzionario può garantire. Vengono modificate anche le garanzie che attengono lo stesso concetto di interessati dato che gli effetti potranno sia espandersi territorialmente ma anche sui singoli o sui gruppi andando a ledere principi quali l'eguaglianza, il principio personalista e le garanzie personali.

L'Intelligenza Artificiale si inserisce in un ampio processo di digitalizzazione della PA che negli ultimi anni ha interessato ampi settori, cambiando la concezione degli stessi: si passa così da un'organizzazione della PA che garantisce mediante i suoi uffici servizi e politiche pubbliche, ad una classificazione dei settori strategici, ai quali corrispondono molteplici diritti, chiamati ad oggi ecosistemi, entro i quali viene organizzata la PA[5].

La "trasformazione digitale" ha interessato tutta la PA ed è stata accompagnata negli ultimi anni dalle previsioni contenute nel Piano Triennale ICT[6] che ha identificato una nuova strategia digitale. La garanzia dei servizi, e dei connessi diritti ed interessi legittimi, trovano la propria effettività nella capacità degli uffici pubblici nell'unire una maggiore propensione alla garanzia della privacy e della sicurezza delle informazioni, una razionalizzazione dei dati e dei *data center*, un incremento della connettività e del capitale umano ed infine uno sviluppo della tecnologia digitale e la trasformazione dei servizi pubblici in "servizi pubblici digitali".

Insieme ai servizi pubblici digitali vi è stato un incremento del "mercato digitale" che ha interessato numerose realtà ed ha inciso sulla PA sia in modo attivo, mediante una nuova offerta di strumenti al servizio dei processi amministrativi, sia in modo passivo, chiedendo agli uffici pubblici una maggiore velocità e chiarezza dei procedimenti burocratici avviati. Il mercato digitale, oltre ad avere una importante incidenza sull'economia, ha facilitato il nascere di nuove professionalità, di nuove esigenze di tutela, di nuovi ambiti disciplinari.

Il mercato digitale è in continua evoluzione ed è influenzato da tecnologie quali la *Blockchain*, la *Big Data Analytics* e la stessa Intelligenza Artificiale. Queste tecnologie hanno quindi forti effetti sull'economia, sulla Pubblica Amministrazione, sul rapporto tra organi e sulla individuazione della *governance*. Il nuovo regolamento per la protezione dei dati personali va proprio nella direzione di garantire uno sviluppo del mercato digitale, attraverso una

[5] La trasformazione digitale della Pubblica Amministrazione ha avuto un suo sviluppo a partire dall'Agenda digitale del 2014 fino all'approvazione del Piano Triennale per l'informatica nella PA.

[6] Si veda il testo del Piano sul sito *pianotriennale-ict.italia.it*.

più chiara e netta regolazione delle modalità con la quali i dati, in particolare quelli personali, vengono trattati, raccolti, utilizzati e cancellati[7].

Oggi quindi i sistemi di IA pongono numerose questioni che non possono essere risolte unicamente mediante una interpretazione delle regole esistenti proprio perché vanno a modificare sostanzialmente la realtà e non la vanno solamente ad integrare, creando nuove questioni che la tecnica sta affrontando e che il giurista deve sentire la necessità di disciplinare. Gli ambiti di applicazione sono molteplici e si basano su rami di ricerca in forte evoluzione quali *machine learning*, *deep learning*, *computer vision*, *human computation*, *natural language*, la robotica e molti altri. Tutte questi ambiti hanno due vettori principali: i dati e gli algoritmi che derivano da questi dati.

Tramite queste tecniche è altresì possibile, anche con l'utilizzo di analisi predittive, garantire una maggiore trasparenza su settori quali gli appalti o i pagamenti e un'incidenza forte sul contrasto ed il controllo degli atti corruttivi[8].

2. Il GDPR e la spirale pubblicistica dei dati

Il GDPR ha modificato la natura della disciplina in tema di privacy mediante un ripensamento del ruolo e della natura dei dati.

Il dato non viene più inteso come un insieme informatico di codici che creano algoritmi portatori di notizie ma come il fulcro dei diritti della persona. L'uomo, inteso come persona virtuale corrispondente ad una persona fisica, viene tutelato fin dalla sua naturale trattazione dei dati non più solamente mediante una possibilità di dare la propria accettazione al trattamento, ma fin dall'esistenza dell'individuo e del coacervo di dati ed algoritmi che ne delineano la propria sfera personale.

[7] Si veda il prezioso contributo di F. Pizzetti (a cura di), *Intelligenza Artificiale*, *op. cit*.

[8] Mi sia permesso rimandare a quanto già sostenuto in M. Trapani, *La prevenzione e il controllo della corruzione e dell'etica pubblica mediante l'utilizzo delle nuove tecnologie*, in *Forum Costituzionale*, 2018.

I dati vengono così intesi come un intreccio di algoritmi che, nel contenere notizie relative a persone fisiche, condizionano e limitano la garanzia dei diritti e, per questo, devono essere trattati in modo trasparente e controllato sia nella fase della progettazione del software o del sistema automatizzato, sia per impostazione predefinita.

La privacy quindi non ha come principale obiettivo quello della tutela dell'interesse del singolo quanto quello di garanzia che i diritti della comunità siano riconosciuti in un sistema che, seppur permetta la libera circolazione dei dati, ne garantisca la sicurezza e la controllabilità da parte di tutti gli interessati, e della società stessa, sin dalla fase di acquisizione fino all'eventuale cancellazione.

Risulta così nettamente modificata la disciplina nel senso di una tutela che tiene conto di una spirale pubblicistica di diritti e doveri che le varie figure interessate hanno l'obbligo di osservare e veder garantiti.

Il dato quindi entra in una spirale di tutela pubblicistica perché ad esser meritevole di tutela non è tanto, e solo, la sfera dell'individuo, quanto la tutela della libertà dei diritti di tutti mediante, come cita l'art. 1 del GDPR, il continuo bilanciamento tra la tutela del diritto fondamentale alla protezione dei dati e la libera circolazione, in una visione d'insieme, dove l'utilizzo del dato interessa una serie di numerosi altri diritti. Tutto ciò viene sviluppato nell'ottica dell'economia digitale europea, come da considerando 7, e come sviluppo logico di quanto affermato nel Trattato di Lisbona[9].

Non è un caso se proprio all'art.1, paragrafo 2, indica nella "protezione dei diritti e libertà fondamentali delle persone", la *ratio* dell'intera disciplina.

Il legislatore europeo ha quindi mutato notevolmente l'approccio culturale alla disciplina ponendo l'individuo al centro, non più solo come interessato ma soprattutto come persona fisica, ponendo i dati e i loro trattamenti come diritti inviolabili e costituzionalmente protetti.

[9] Lo stesso Trattato di Lisbona considera la protezione dei dati personali come un architrave della garanzia dei diritti e delle libertà delle persone.

3. *Governance*, *accountability* e trasparenza: una dimensione costituzionale collettiva

L'applicazione del GDPR ai sistemi di IA ha quindi un forte impatto su numerosi settori. L' IA, come abbiamo avuto modo di vedere, non è più concepita come un "prodotto" ma come un "agente" che utilizza i dati, gestisce le informazioni, limita o garantisce diritti.

Le numerose normative che hanno interessato questi sistemi evidenziano una difficoltà da parte del legislatore sia di individuare la fonte idonea a regolarli sia di risolvere questioni inerenti "all'etica dell'IA"[10], alla "morale", causato anche da una sostanziale imprevedibilità di azioni e comportamenti di questi sistemi.

La dottrina[11] ha risposto a questa difficoltà di regolamentazione sostenendo che sia necessario superare la volontà di disciplinare gli ambiti di innovazione tecnologica ed informatica mediante fonti primarie, recuperando una flessibilità propria della normativa secondaria. Proprio una regolamentazione dei rapporti che determini la possibilità di un bilanciamento ed un'opera di rinnovamento continuo degli operatori del diritto, potrebbe agevolare una maggiore diffusione consapevole, connessa ad un forte sviluppo, dell'utilizzo di sistemi di IA nella PA.

Le norme che interessano, seppur indirettamente, la disciplina dei sistemi IA sono molteplici e, solo per ricordarne alcune, vanno dalla cosiddetta "direttiva macchine" (2006/42/EC), alle direttive sulla sicurezza del mercato europeo (2001/95/CE e 2008/765/CE), fino alla recente risoluzione sulla robotica del febbraio 2017 per arrivare al Regolamento europeo sul trattamento dei dati personali. Le normative in questione, se da un lato hanno registrato la crescita economica e scientifica di questo fenomeno, riconoscendone le potenzialità e la eventuale soggettività giuridica di tali sistemi, dall'altra hanno lasciato l'intera disciplina priva di una regolamentazione unitaria

[10] Si vedano sul punto K. Abney, *Robotics, Ethical Theory, and Metaethics; A Guide for the Perplexed*, in P. Lin-K. Abney-G.A. Bekey (a cura di), *Robot Ethics: The ethical and social implications of robotics*, Cambridge, The MIT Press, 35 ss.

[11] Si veda su tutti quanto sostiene U. Pagallo, *Intelligenza Artificiale e diritto. Linee guida per un oculato intervento normativo*, in *Sistemi intelligenti*, Bologna, il Mulino, 2017, 618 ss.

ed organica, mancando quindi di fissare standard e regole condivise, risultando altresì carenti perché non interamente, e di *default*, pensate per le fasi di progettazione ed implementazione di questi sistemi che, per natura, mutano il proprio modo di operare con una velocità più consistente di quanto non faccia il diritto.

Lo stesso GDPR prende atto sin dai "considerando" di questa dicotomia tra scienza e diritto sempre più evidente con l'avanzare delle nuove tecnologie. Non è un caso infatti che al "considerando 6" si richiami subito l'esigenza di garantire maggiore protezione dei dati in un contesto in cui questi ultimi hanno la maggiore possibilità di essere condivisi e di "transitare" più velocemente a causa della rapidità dell'evoluzione tecnologica, permettendo la creazione di un clima di fiducia nello sviluppo dell'economia digitale (come aggiunto dal "considerando 7"). Tale riferimento viene ripreso al "considerando 91" dove si afferma che è necessario prestare particolare attenzione alla valutazione d'impatto nei trattamenti su larga scala e in particolare laddove «in conformità con il grado di conoscenze tecnologiche raggiunto, si utilizzi una nuova tecnologia [...] specialmente qualora tali trattamenti rendano più difficoltoso, per gli interessati, l'esercizio dei propri diritti».

Fin dalle premesse si svela quindi l'approccio pubblicistico che il nuovo regolamento ha inteso dare alla disciplina ponendo al centro l'adeguatezza sia dei trasferimenti sia dell'utilizzo dei dati personali.

Non è casuale la previsione dell'art. 45 secondo cui il principio di adeguatezza, riferito in quel caso specifico ai limiti del trasferimento dei dati (evento assai probabile nei sistemi di IA), elenchi la garanzia dei diritti umani e delle libertà fondamentali, la presenza di una autorità di controllo e gli impegni assunti dal Paese terzo in materia di protezione, come elementi di valutazione dell'eventuale legittimità,

Il regolamento quindi, se da una parte apre al "mercato digitale", dall'altro lo imbriglia con principi e garanzie di rango costituzionale, determinando una nuova *governance* collettiva che la tecnologia ha solamente favorito.

I sistemi di IA, seppur non siano richiamati esplicitamente nel testo, rappresentano il convitato di pietra che assicura al regolamento una propria proiezione spazio-temporale, in stretta connessione con la già citata risoluzione del 16 febbraio 2017 riguardante le "Norme di diritto civile sulla robotica".

Il potenziamento delle capacità umane in un continuo scambio di informazioni e stimoli hanno cambiato gli stessi scenari della scienza e, di conseguenza, quelli del diritto. Intento del giurista non sarà più quello di porsi la domanda di come adeguare le norme presenti ad un uomo potenziato nelle proprie capacità ma di come disciplinare sistemi di IA che si sostituiscono all'uomo, imparano come questo, agiscono come questo, ma hanno capacità potenzialmente infinite.

Le conseguenze di tutto ciò sono presenti in vari settori poiché non si è in presenza di una semplice "riproduzione" delle fattezze umane ma di una realtà che ha una propria facoltà cognitiva. Sarebbe necessario chiedersi se e come i sistemi di IA possano unire le immense facoltà conoscitive ad anche minime potenzialità emotive che, in molti casi, sono alla base della discrezionalità dell'agente e ne agevolano quella flessibilità che anche il diritto riconosce come elemento essenziale di valutazione. Questo ampliamento delle potenzialità ha come conseguenza anche un cambiamento epocale di alcune situazioni fattuali legate alla vita umana che portano con sé numerose conseguenze sui diritti e sulla dimensione costituzionale stessa[12].

Ritornando così al GDPR è necessario precisare che alcune previsioni erano state sollecitate proprio dalla risoluzione richiamata che definisce l'autonomia di un robot come «la capacità di prendere decisioni e metterle in atto nel mondo esterno, indipendentemente da un controllo o da una influenza» ponendo anche la questioni di una nuova regolamentazione con l'aumentare della loro autonomia, sempre meno inquadrabile nelle categorie giuridiche esistenti[13].

Oltre ciò richiama anche l'esigenza che la scelta umana non sia mai costituita completamente da processi automatizzati ma che, in qualche modo, possa sempre essere controllata dall'intervento uma-

[12] Si pensi, ad esempio, alla possibilità che sistemi di IA possano incidere positivamente sulla cura dei pazienti affetti da dislessia o a sistemi che contrastino i sistemi di invecchiamento o, ancora, sistemi che siano in grado di profilare la vita delle persone, le loro abitudini, le loro scelte, per poi elaborare politiche pubbliche. In tutti questi casi si pongono problemi legati al principio di eguaglianza, all'accessibilità alle cure, all'human divide, al principio di rappresentanza e responsabilità. Si veda C. Salazar, *Umano*, cit., 265 ss.

[13] Si veda la Risoluzione ai punti AA, AB e AC sulla "Responsabilità".

no. Il GDPR, infatti, all'art. 22 afferma che «l'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida allo stesso modo significativamente sulla sua persona»[14].

Il GDPR affronta così numerosi aspetti che possono riguardare anche i sistemi di IA. Ai limitati fini della trattazione è necessario richiamare il diritto di accesso ai dati personali ed alle modalità di trattamento, alle stesse definizioni di "profilazione" e "pseudonimizzazione", alla liceità, correttezza e trasparenza del trattamento dati, al diritto all'oblio[15] fino alle valutazioni d'impatto.

La responsabilità quindi del trattamento dei dati nei casi di IA prende una propria forma e deve essere letta alla luce dei principi richiamati nella consapevolezza che permangono, ad oggi, numerosi dubbi e questioni aperte anche per la difficoltà di tracciare in tali sistemi quali siano stati i processi e gli scambi di dati avvenuti.

L'applicazione del GDPR ai sistemi di IA comporta una centralità della ricerca della trasparenza dei processi e della raccolta dei dati (che, ad esempio, non possono quindi sottostare unicamente a scelte prese da sistemi automatizzati) ed una rinnovata richiesta di *accountability* al fine di analizzare quale sia il livello di responsabilità dei vari attori[16].

Tutto ciò comporta quindi una nuova *governance* del mercato digitale e del sistema dei diritti della persona, sempre più al centro del Regolamento, che devono rappresentare uno stimolo per il giurista e per il legislatore affinché venga analizzata una normativa specifica

[14] Al riguardo è necessario richiamare la sentenza TAR Lazio-Roma, Sez. III-*bis*, n. 3769/2017, secondo la quale, nel caso in cui algoritmi vengano utilizzati per l'attività amministrativa e una decisione derivi proprio da questo processo, debba essere sempre garantito il diritto di accesso all'algoritmo, in modo da consentire di verificare che la PA abbia agito correttamente.

[15] Interessante in questo caso il cambio di prospettiva. Il diritto all'oblio non è un diritto assoluto ma condizionato all'effettiva possibilità che la tecnologia lo permetta e, questa la vera rivoluzione, siano sostenibili i costi.

[16] Si veda la derivazione del "principio di fiducia", ripreso dal considerando 7, che rappresenta il fine ultimo della disciplina in F. Pizzetti, *Intelligenza artificiale, protezione dei dati personali e regolazione*, Torino, Giappichelli, 2018, 170 ss.

e si propongano categorie giuridiche che possano essere idonee a regolare il sistema diffuso di IA[17].

Tutto ciò mette quindi al centro la persona, i suoi diritti e la sua dimensione collettiva, interessando sia le libertà personali che la propria autodeterminazione, il diritto alla vita, alla salute, il principio di eguaglianza e una serie di altri previsioni costituzionali che ne rideterminano la specie e la categoria giuridica.

4. Alcune questioni ancora aperte e l'uscita dalla caverna

Permangono così numerose questioni aperte che meritano di essere riportate alla fine di questa breve trattazione affinché diventino il campo principale di analisi ed approfondimento dei giuristi.

Secondo l'art. 4, paragrafo 1, numero 7 del GDPR il titolare del trattamento è colui che agisce avendo la possibilità di determinare finalità e mezzi del trattamento dei dati personali. Il primo interrogativo è quindi relativo al ruolo della macchina dotata di sistemi di IA. Quest'ultima può infatti essere identificata come titolare del trattamento, sottoposta quindi direttamente agli obblighi di trasparenza, responsabilità ed eventuale sanzionabilità, o come responsabile del trattamento *ex* art. 28 GDPR[18]. In questo caso è necessario che venga individuato il titolare del trattamento, che potrebbe essere il produttore ossia colui che lo programma, analizzare quale sia il reale rapporto con il proprietario e verificare che il titolare possa veramente in ogni momento avere un rapporto con il robot affinché sorga la responsabilità.

Evidentemente la questione non è di netta e facile soluzione, *in primis* perché sarebbe necessario riconoscere la personalità giuridica del sistema IA, questione ancora ampiamente dibattuta, ma altresì perché la stessa evoluzione tecnologica modifica continua-

[17] A conclusione simile sono pervenuti recentemente anche M. Bassini-L. Liguori-O. Pollicino, *Sistemi di Intelligenza Artificiale, responsabilità e accountability. Verso quali paradigmi?*, in F. Pizzetti (a cura di), *Intelligenza Artificiale*, cit., 369 ss.

[18] Sul punto si è soffermato F. Pizzetti, *Intelligenza artificiale, protezione dei dati personali e regolazione*, cit.

mente l'autonomia dei sistemi, allontanandoli sempre di più dalla prima programmazione.

La stessa questione relativa all'equilibrio tra la trasparenza e la privacy[19] viene ampliata con l'utilizzo delle nuove tecnologie di IA che comportano, a fronte di una maggiore capacità di calcolo, analisi e raccolta di dati, dei limiti sia all'accessibilità della conoscenza dei processi attivati sia una difficoltà di garanzia assoluta della tutela della privacy. I principi della *privacy by design* e *by default* sono concepiti per essere validi anche per i nuovi sistemi di IA e hanno come primo obiettivo quello di prevedere la tutela del dato personale sin dalla nascita della progettazione del sistema. Come abbiamo detto il sistema di regolamentazione del GDPR non è incentrato principalmente sulle figure dell'interessato o del titolare ma direttamente sulla persona fisica, sulla totalità degli individui, e sulla tutela dei diritti e delle libertà e della loro funzione sociale.

Risulta necessario quindi una costante opera sia da parte dei giuristi che della PA e della stessa Autorità affinché questo difficile equilibrio sia sempre presente nella coscienza che una buona regolamentazione ed un buon utilizzo di questi sistemi permettono una migliore efficienza della PA e una più adeguata predisposizione di politiche pubbliche. Questo potrebbe altresì porre dubbi proprio sulla legittimazione ad agire ogni qualvolta la discrezionalità amministrativa si identifichi totalmente in capo ad una "macchina" e non anche ad un funzionario della PA che, da Costituzione, riceve la propria legittimità funzionale dall'accesso mediante concorso e dal proprio ruolo ricoperto o, nel caso in cui questi sistemi svolgano il ruolo proprio di un decisore politico, dai processi utili al soddisfacimento del principio di rappresentanza.

Ulteriori questioni sono sia quelle relative ai registri delle attività di trattamento, comportando quindi i sistemi di IA una particolare

[19] Numerosi sono i contributi relativi a questo difficile equilibrio. Si rimanda, *ex multis*, E. Carloni-M. Falcone, *L'equilibrio necessario*, in *Diritto Pubblico*, 3/2017, 723 ss.; L. Califano, *Trasparenza e privacy: la faticosa ricerca di un bilanciamento mobile*, in L. Califano-C. Colapietro (a cura di), *Le nuove frontiere della trasparenza nella dimensione costituzionale*, Napoli, Editoriale Scientifica, 2014; I.A. Nicotra, *La dimensione della trasparenza tra diritto alla accessibilità totale e protezione dei dati personali: alla ricerca di un equilibrio costituzionale*, in Federalismi.it, 11/2015.

attenzione data la quantità di dati che possono essere processati anche da più sistemi di IA integrati, che alla valutazione d'impatto *ex* art. 35 del GDPR.

Proprio l'art. 35 (che già richiamava ad una particolare attenzione allorché si preveda l'utilizzo di particolari tecnologie) al punto 3, nell'elencare i casi in cui è indispensabile una particolare valutazione, indica che è necessario porre attenzione in quelli ove vi è «una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche».

Risulta evidente come sia necessario un impegno della ricerca scientifica, sia relativa alla tecnica che alla parte giuridica, nell'intento di poter specificare meglio nei sistemi di IA come possano essere condotte analisi di questo tipo data la peculiarità di questi processi ed essendo molto complicato poter fare una valutazione sufficientemente adeguata.

Proprio per fare ciò è altresì necessario quindi un incremento ed una predisposizione di linee guida e codici di condotta, oltre a brevetti, che ne permettano l'utilizzo idoneo, anche alla luce della previsione della necessità che il concetto di privacy sia presente sin dalla progettazione.

Insomma, non avendo la presunzione di voler elencare le pluralità di questioni che l'utilizzo di IA ha aperto nel nostro ordinamento, risulta almeno verificabile che con l'entrata in vigore del GDPR sia cambiato lo stesso punto di osservazione della tutela del dato.

Oltre ciò vi è stato un rafforzamento della tutela ed una maggiore attenzione alle nuove tecnologie inserendo la disciplina in una dimensione collettiva costituzionale attenta sia a principi quali quelli personalista e di autodeterminazione, che a diritti e libertà come quelli relativi alla libera circolazione, alla trasparenza (dell'utilizzo del dato e della stessa PA), allo sviluppo dell'economia digitale oltre alla garanzia della sfera dei diritti minimi della persona in quanto "persona fisica" e non solo in quanto "interessata". Il rischio viene quindi posto alla base della tutela dei diritti della persona nella società, alla possibilità che questa possa essere vista non come un *unicum* ma come un soggetto i cui dati creano diritti e libertà. Sono altresì essi stessi ed il loro buon utilizzo, e trattamento, che per-

mettono la garanzia dello sviluppo della persona. Un buon utilizzo dei dati permette anche che questi non creino diseguaglianze[20] che rischierebbero di alterare fortemente il paradigma della crescita digitale come strumento per l'accesso diffuso ai servizi della PA e ai connessi diritti dei cittadini.

Concludendo, il GDPR, ha reso maggiormente evidente l'esigenza di uno sviluppo del diritto di frontiera legato alle nuove tecnologie ponendo al centro sia la flessibilità del diritto che la necessaria precisione nella disciplina e la collaborazione con la scienza. Questo approccio cambia il ruolo del giurista: il nodo di discussione non è più quale sia l'impatto delle nuove tecnologie ma come i diritti e i doveri possano essere più efficacemente garantiti mediante l'utilizzo delle nuove tecnologie. Il giurista, ed in particolare il costituzionalista[21], tramite questo cambiamento di prospettiva avrà nei prossimi anni la possibilità di uscire dalla caverna e poter vedere, oltre alle ombre, la vera essenza delle cose con l'arduo compito di doverla riportare "alla dimora della prigione".

[20] Si vedano non solamente le differenti possibilità di accesso a questi sistemi ma anche, nel caso dell'accesso, all'eventualità che un dato mal utilizzato o mal annotato crei dei *bias* e conseguenti diseguaglianze.

[21] Interessante la riflessione sul fattore tecnologico ed il costituzionalismo in P. Costanzo, *Il fattore tecnologico e le trasformazioni del costituzionalismo*, in Aa. Vv., *Costituzionalismo e globalizzazione*, *Atti del XXVII Convegno annuale*, Napoli, Jovene, 2014.

Dati, algoritmi e Regolamento europeo 2016/679

Fernanda Faini

Sommario: 1. Big Data, algoritmi e diritto – 2. Il regolamento (UE) 2016/679: strumenti di tutela della persona – 3. La data protection nella sfida degli algoritmi – 3.1. Dati personali, informazioni e consenso. – 3.2. Trasparenza, apertura e controllo collettivo – 4. Riflessioni conclusive

1. Big Data, algoritmi e diritto

Nell'era digitale, gli ordinamenti giuridici sono chiamati al difficile compito di regolare il "diluvio" di dati che caratterizza la contemporaneità, al fine di tutelare i diritti e sanare i conflitti che scaturiscono dall'"esistenza digitale" dell'uomo, parte integrante ormai "dirompente" della vita.

La società odierna si basa sulla pervasiva centralità dei dati e delle informazioni quali risorse essenziali per lo sviluppo economico, sociale e culturale, "materia prima" di cui si nutre la tecnologia[1]. Nella trasformazione epocale che ha reso i dati protagonisti, si assiste a un superamento dei "confini" abituali della vita e del diritto, ossia all'abbattimento delle barriere geografiche, che crollano nel delinearsi di una società globale, e degli ostacoli temporali, dal momento che l'utilizzo dei dati per estrarne conoscenza è veloce e semplice e la conoscenza che se ne ricava non si limita al presente, ma si spinge a predire quello che sarà.

[1] Cfr. M. Castells, *The rise of the Network society*, Oxford, Oxford University Press, 2000.

In tale contesto di riferimento, pertanto, elementi privilegiati per osservare la società sono costituiti dalle configurazioni attuali assunte dai dati, i Big Data, e dagli algoritmi, capaci di estrarne il valore, protagonisti indiscussi dell'evoluzione della conoscenza in senso dinamico e "attivo".

I Big Data consistono in enormi volumi di dati detenuti da grandi organizzazioni, come governi e multinazionali, provenienti da diverse fonti e analizzati per mezzo di algoritmi, tecniche di *data mining*, *Big Data analytics*, *machine learning* e altre tecniche specifiche[2]. Dalla definizione stessa emerge una caratteristica fondamentale dei Big Data, ossia l'eterogeneità dei dati che li compongono: dati forniti su base volontaria (Google, Facebook, Amazon); dati "scambiati" o "comprati" a fronte di utilità conseguibili (raccolte punti, tessere fedeltà, applicazioni che assicurano sconti); dati forniti in modo più o meno consapevole (GPS, rilevatori, sensori); dati registrati automaticamente (*cookie*); dati residui (*data exhaust*) o ricavati da altri dati; dati raccolti dai soggetti pubblici. Ne fanno parte, altresì, i dati prodotti dall'*Internet of Things* (IoT), dalle "case intelligenti", dai dispositivi indossabili, dalle automobili autonome e, più ampiamente, da tutti gli "oggetti" che si basano sull'utilizzo di dati[3]; anche le soluzioni di intelligenza artificiale si basano su enormi quantità di dati e su algoritmi che sfruttano l'insieme dei dati a disposizione.

Nella società contemporanea si tende a "datizzare" tutto ciò che ci circonda, convertendo i fenomeni in dati e, di conseguenza, inserendo sensori e rilevatori nella nostra realtà al fine di produrre enormi quantità di dati analizzabili da potenti algoritmi: gli algoritmi costituiscono il "motore" capace di "animare" i dati e generare valore grazie all'utilizzo, all'analisi e all'elaborazione di dati eterogenei[4].

[2] Esistono molte definizioni di Big Data; una definizione nel senso proposto nel contributo è presente nell'*Opinion* 03/2013 *on purpose limitation*, adottata il 2 aprile 2013 da parte dell'*Article 29 Data Protection Working Party*.

[3] In tal senso S. Faro-N. Lettieri, *Big Data: una lettura informatico-giuridica*, in L. Lombardi Vallauri (a cura di), *Scritti per Luigi Lombardi Vallauri*, Padova, Cedam, 2016, vol. I, 503 ss.

[4] Cfr. V. Mayer-Schönberger-K. Cukier, *Big data. Una rivoluzione che trasformerà il nostro modo di vivere e che già minaccia la nostra libertà*, trad. it., Milano, Garzanti, 2013, 103 ss.

L'analisi delle caratteristiche degli algoritmi permette di far emergere le difficoltà che incontra il diritto nel momento in cui è chiamato ad affrontarli.

Oggi è tecnicamente possibile analizzare una quantità di dati inimmaginabile nel passato, ossia tendenzialmente tutti quelli disponibili, rinunciando all'esattezza e accettando una dose di imprecisione a fronte della possibile conoscenza che ne deriva. Gli algoritmi portano a rinunciare alle ipotesi predeterminate e alla ricerca della causalità nei fenomeni, affidandosi invece alle correlazioni e alle inferenze e poggiando sulla probabilità (e sulla correlata dose di "confusione"): così, in un percorso inverso rispetto al passato, si risale dai fenomeni alla valutazione delle probabili cause. In altri termini, si presta attenzione alle correlazioni che emergono dalle analisi sui dati, senza che siano necessariamente predefiniti l'oggetto di indagine e gli obiettivi[5]: questo aspetto, come sarà esaminato, è particolarmente rilevante quando viene in gioco la disciplina in materia di *data protection*.

Gli algoritmi sono capaci di strutturare le informazioni e automatizzare i processi[6]: «codificano il mondo, lo classificano e predicono il nostro futuro»[7]. Non a caso, la dimensione che caratterizza i Big Data, accanto alla varietà[8] e al volume[9], è proprio la velocità, che richiama la capacità degli algoritmi di analizzare i dati e che sottende la rilevanza della dinamicità[10].

[5] Cfr. A. Mantelero, *Big data: i rischi della concentrazione del potere informativo digitale e gli strumenti di controllo*, in *Il diritto dell'informazione e dell'informatica*, 2012, fasc. 1, 135-144; G. Sartor-M. Viola De Azevedo Cunha, *Il caso Google e i rapporti regolatori USA/EU*, in *Il diritto dell'informazione e dell'informatica*, 2014, fasc. 4-5, 657-680.

[6] Cfr. M. Orefice, *I big data. Regole e concorrenza*, in *Politica del diritto*, 2016, fasc. 4, 703.

[7] D. Cardon, *Che cosa sognano gli algoritmi. Le nostre vite al tempo dei* big data, Milano, Mondadori Università, 2016, 5.

[8] La varietà riguarda l'eterogeneità della tipologia e dei formati dei dati, provenienti da fonti diverse (strutturate e non).

[9] Il volume si riferisce alla capacità di acquisire, memorizzare, accedere ed elaborare enormi quantità di dati.

[10] In dottrina sono considerate quali caratteristiche dei Big Data anche due dimensioni ulteriori: il valore, ossia quanto i Big Data valgono come insieme, e la veracità o veridicità, ossia la qualità e l'accuratezza dell'analisi. Da questi profili

Il funzionamento degli algoritmi evidenzia sotto diversi profili il contrasto ontologico con il diritto e con il modo di vedere la realtà da parte dei giuristi.

Gli algoritmi prediligono, come esaminato, un metodo descrittivo che si differenzia dal carattere prescrittivo del diritto; gli algoritmi si basano su fenomeni, numeri e calcoli, mentre il diritto è orientato ai valori della società di riferimento; l'algoritmo si nutre di dinamicità, mentre il diritto è "formale" e, in un certo senso, necessariamente "lento". Più ampiamente gli algoritmi sono fondati su metodologie deterministiche, che si basano su fenomeni, su circostanze oggettive e su probabilità e che rischiano, così, di inficiare le scelte individuali e la libera volontà, su cui poggiano i nostri ordinamenti giuridici[11].

Proprio nelle caratteristiche e nel funzionamento degli algoritmi emerge il valore e la conseguente attenzione rivolta al fenomeno, che si collega strettamente a ciò che i Big Data permettono di raggiungere.

Le analisi compiute sui Big Data permettono di estrarre conoscenza, che si traduce nell'interpretazione dei bisogni, nella profilazione degli utenti, nell'ottimizzazione della produzione, nel supporto alle decisioni.

Gli algoritmi si atteggiano a moderni oracoli, dal momento che la conoscenza che consentono può consistere anche in una vera e propria capacità predittiva: ferme restando le connessioni false o apparenti, elevate correlazioni indicano alte probabilità, che permettono di fare previsioni sul futuro[12]. Gli algoritmi, di conseguenza, consentono di effettuare predizioni sui consumi e sugli andamenti di mercato, di indicare preventivamente l'usura di infrastrutture, di migliorare diagnosi e cure, di prevenire disastri, di prendere decisioni politiche e, anche, di vincere le elezioni[13].

deriva il paradigma delle 3, 4 o 5 "V" (a seconda degli aspetti presi in considerazione), su cui si basano i Big Data: volume, velocità, varietà, valore e veracità; cfr. F. Di Porto, *La rivoluzione* Big Data. *Un'introduzione*, in *Concorrenza e mercato*, 2016, 5 ss.

[11] Cfr. V. Zeno-Zencovich-G. Giannone Codiglione, *Ten legal perspectives on the "Big data revolution"*, in *Concorrenza e mercato*, 2016, 49 ss.

[12] Cfr. V. Mayer-Schönberger-K. Cukier, *Big data*, cit., 73 ss.

[13] Cfr., *inter alia*, D. De Pasquale, *La linea sottile tra manipolazione della rete e pubblicità*, in *Il Diritto industriale*, 2012, fasc. 6, 552 ss.; A. Mantelero, *Big data: i rischi della concentrazione del potere informativo digitale e gli strumenti di controllo*, cit., 138-139.

Naturalmente l'utilizzo delle predizioni può rispondere alla tutela di interessi generali, ma anche alla realizzazione di vantaggi economici, dal momento che la conoscenza può costituire valore da impiegare per essere competitivi e ottenere profitti[14]; in tal caso possono configurarsi anche sfruttamento economico e mercificazione dei dati personali[15].

Proprio la necessità di tutelare in modo efficace la persona nell'era dei Big Data deve essere considerata tra le ragioni che hanno portato al processo di riforma europeo e all'approvazione del regolamento (UE) 2016/679.

2. Il regolamento (UE) 2016/679: strumenti di tutela della persona

Il regolamento (UE) 2016/679, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, che abroga la direttiva 95/46/CE, è teso a rendere omogenea la tutela della persona nei diversi Stati e a rafforzarne l'effettività insieme alla correlata fiducia da parte della collettività.

Il Regolamento europeo 2016/679 non tratta esplicitamente i Big Data[16], ma anche alla loro gestione si attagliano alcuni principi innovativi della disciplina, che mirano a un approccio proattivo e a una ponderazione preventiva dell'impatto e dei rischi sulla *data protection*[17].

[14] Cfr. M. Orefice, *I big data. Regole e concorrenza*, cit., 706 ss.

[15] Cfr. G. Colangelo, Big data, *piattaforme e antitrust*, in *Mercato Concorrenza Regole*, 2016, fasc. 3, 426; C. Focarelli, *La privacy. Proteggere i dati personali oggi*, Bologna, il Mulino, 2015, 45 ss.

[16] Cfr. i documenti dell'*European Data Protection Supervisor*, come l'Opinion 8/2016, 23 settembre 2016, "EDPS Opinion on coherent enforcement of fundamental rights in the age of big data", e le "Guidelines on the Protection of Individuals with Regard to the Processing of Personal Data in a World of Big Data", adottate il 23 gennaio 2017 dal Comitato della Convenzione del Consiglio d'Europa per la protezione dei dati (Convenzione 108).

[17] Cfr. G. Finocchiaro, *Introduzione al regolamento europeo sulla protezione dei dati*, in *Le Nuove leggi civili commentate*, 2017, fasc. 1, 1-18.

In particolare si tratta degli strumenti della *privacy by design* e *by default* e del *Data Protection Impact Assessment*, nei quali il diritto si avvale della tecnologia per assicurare il suo rispetto e garantire la tutela della dignità e dello sviluppo della persona[18].

Il principio *privacy by design*, di cui all'art. 25, paragrafo 1 del regolamento (UE) 2016/679, prevede che, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso, il titolare debba mettere in atto «misure tecniche e organizzative adeguate, quali la pseudonimizzazione» (di cui all'art. 4, comma 1, n. 5), «volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del regolamento e tutelare i diritti degli interessati».

A tale criterio si lega il principio *privacy by default*, posto nel secondo paragrafo dell'art. 25 del regolamento (UE) 2016/679: il titolare deve mettere in atto «misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento». L'individuo è tutelato in modo rafforzato dal momento che la disposizione impedisce l'accesso a un numero indefinito di persone fisiche da parte di macchine (senza l'intervento della persona fisica) e prevede che l'obbligo sia calibrato su aspetti quali la quantità di dati, la portata del trattamento, il periodo di conservazione e l'accessibilità.

Interessante, altresì, l'art. 35 del reg. (UE) 2016/679, relativo al c.d. *Data Protection Impact Assessment*: quando un tipo di trattamento, allorché preveda in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare effettua, prima di procedere al trattamento, «una valutazione dell'impatto dei trattamenti previsti sulla protezione

[18] Cfr. C. Focarelli, *La privacy*, cit., 63; A. Mantelero, *Big data: i rischi della concentrazione del potere informativo digitale e gli strumenti di controllo*, cit., 159 ss.

dei dati personali». Tale valutazione è prevista in determinati casi descritti dalla normativa, quali trattamenti automatizzati, come le operazioni di profilazione degli utenti, che permettono una valutazione sistematica e globale di aspetti personali relativi a persone fisiche e fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche; trattamenti su larga scala di particolari categorie di dati o di dati relativi a condanne penali e a reati; sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

La disposizione prevede che la valutazione d'impatto sulla protezione dei dati debba contenere, almeno, i requisiti minimi indicati, quali una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità, una valutazione dei rischi per i diritti e le libertà degli interessati e le misure previste per affrontare i rischi.

L'approccio preventivo e proattivo è presente anche nell'innovativo diritto alla portabilità dei dati previsto all'art. 20 del regolamento europeo, idoneo a ridurre il rischio di *lock-in* e favorire la concorrenza tra le piattaforme[19]: l'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico, i dati personali che lo riguardano forniti a un titolare e di trasmettere tali dati a un altro titolare, senza impedimenti da parte del primo titolare cui li ha forniti.

Sotto il profilo della gestione dei Big Data risultano interessanti anche altre novità del regolamento (UE) 2016/679, come la consultazione preventiva (art. 36)[20], la *data breach notification* (artt. 33-34)[21] e il *Data Protection Officer* (DPO) o Responsabile della protezione dei dati (RPD) (artt. 37-39). La nomina di questa figura è prevista con la

[19] Cfr. G. Colangelo, Big data, *piattaforme e antitrust*, cit., 455.

[20] Il titolare, prima di procedere al trattamento, consulta l'autorità di controllo qualora la valutazione d'impatto indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate per attenuare il rischio.

[21] Le norme impongono al titolare l'obbligo di notificare eventuali violazioni dei dati personali all'autorità nazionale nei tempi e nelle modalità previste. Quando la violazione è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare comunica la violazione all'interessato senza ingiustificato ritardo.

funzione di garantire una corretta gestione dei dati in una serie di casi, come quello in cui il trattamento richieda il monitoraggio regolare e sistematico degli interessati su larga scala e quello di trattamento, su larga scala, di categorie particolari di dati personali.

In linea con l'approccio proattivo e preventivo di tutela si pone la logica di *accountability* e responsabilizzazione dei soggetti che trattano i dati personali[22] e la contitolarità, accompagnata dalla definizione delle rispettive responsabilità[23], disposizioni coadiuvate sia dall'attenzione alla sicurezza[24], sia dall'effettività e dall'efficacia del sistema sanzionatorio correlato[25].

Nell'applicazione della disciplina e nella promozione della consapevolezza al riguardo, un ruolo strategico è svolto in concreto dalle autorità di controllo indipendenti (nel caso italiano il Garante per la protezione dei dati personali)[26]. Nelle attività e nei poteri conferiti l'autorità di controllo assume una strategica funzione che dalla *data protection* più ampiamente si estende a una vera e propria *data governance*.

3. La data protection nella sfida degli algoritmi

L'approccio e gli strumenti che caratterizzano il regolamento (UE) 2016/679 sono tesi ad una tutela effettiva della persona e si attagliano alla società dei Big Data. Ma le caratteristiche che connotano Big Data e algoritmi mostrano, altresì, criticità ontologiche nel rispetto della disciplina in materia di *data protection*: in particolare, rischiano di scontrarsi apertamente con alcuni principi che caratterizzano ancora profondamente la normativa, tesi a garantire il rispetto dell'individuo e della sua libertà di autodeterminazione e, altresì, lo stesso mercato, ponendosi come limite alla creazione di posizioni dominanti.

[22] Art. 24, reg. (UE) 2016/679.

[23] Art. 26, reg. (UE) 2016/679.

[24] Art. 32, reg. (UE) 2016/679.

[25] Artt. 82-84, reg. (UE) 2016/679.

[26] Artt. 51-59, reg. (UE) 2016/679. Il regolamento prevede la cooperazione, l'assistenza reciproca e operazioni congiunte da parte delle autorità di controllo (art. 60 ss.).

Come esaminato, nell'utilizzo di Big Data non è necessariamente predefinito a priori l'oggetto di indagine e non sono prevedibili al momento della raccolta gli obiettivi e le finalità raggiungibili, dal momento che le elaborazioni sono capaci di condurre a interessanti risultati inattesi[27]. Di conseguenza l'utilizzo dei Big Data rende particolarmente difficile il rispetto del principio di limitazione della finalità, che prevede la raccolta per finalità determinate, esplicite e legittime e il successivo trattamento in modo che non sia incompatibile con tali finalità[28].

Le caratteristiche dei Big Data che consistono nel volume e nella varietà delle fonti rendono, inoltre, difficile il rispetto del criterio di minimizzazione dei dati e dei relativi principi di adeguatezza, pertinenza e limitazione dei dati personali a quanto necessario rispetto alle finalità del trattamento[29] e, allo stesso modo, rischiano di inficiare la qualità, l'esattezza e l'accuratezza dei dati[30].

I principi di limitazione della finalità, di esattezza e di minimizzazione dei dati rischiano quindi di essere depotenziati in un contesto dominato dagli algoritmi, a causa delle criticità esaminate.

Oltre a questi principi, non mancano disposizioni che destano perplessità dal momento che sembrano attente al mercato e alla tutela di interessi diversi rispetto alla protezione della persona.

In particolare è ascrivibile a tali norme la disposizione che prevede la finalità del marketing diretto e la connessa profilazione come legittimo interesse che consente il trattamento dei dati personali[31]. La disposizione, che pare non considerare lo squilibrio tra le parti in gioco, prevede un meccanismo di tutela basato sull'*opt-out* tramite

[27] Cfr. A. Mantelero, *Big data: i rischi della concentrazione del potere informativo digitale e gli strumenti di controllo*, cit., 135-144; V. Mayer-Schönberger-K. Cukier, *Big data*, cit., 42; G. Sartor-M. Viola De Azevedo Cunha, *Il caso Google e i rapporti regolatori USA/EU*, cit., 657-680.

[28] Art. 5, paragrafo 1, lett. b), reg. (UE) 2016/679.

[29] Art. 5, paragrafo 1, lett. c), reg. (UE) 2016/679.

[30] Art. 5, paragrafo 1, lett. d), reg. (UE) 2016/679.

[31] Art. 21, paragrafo 2, e considerando 47 del reg. (UE) 2016/679: «qualora i dati personali siano trattati per finalità di marketing diretto, l'interessato ha il diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano effettuato per tali finalità, compresa la profilazione nella misura in cui sia connessa a tale marketing diretto».

opposizione dell'interessato, che non sembra congruo e conforme all'approccio di tutela preventiva ed efficace dei dati personali.

Accanto al difficile rispetto di alcuni principi cardine del regolamento e alle problematiche sollevate da singole disposizioni, nelle caratteristiche stesse di funzionamento di Big Data e algoritmi emergono criticità profonde che rischiano di minare i fondamenti stessi della disciplina europea.

3.1. Dati personali, informazioni e consenso

Nel contesto dei Big Data, la rilevanza attribuita alle tecniche di anonimizzazione, che permettono di non applicare la disciplina, può sollevare criticità. Il rischio si annida nelle inferenze che possono essere tratte su gruppi o individui da dati anonimi, grazie anche alla disponibilità di dati ausiliari riferibili alla persona: semplificando, nella società caratterizzata da grandi dati e potenti algoritmi ogni dato può finire per essere identificativo e quindi personale, esigendo come tale l'applicazione della relativa disciplina[32].

Del resto anche il concetto di "dato personale" può risultare insufficiente, dal momento che, oltre ai dati anonimi che non è detto restino tali, ci possono essere dati afferenti a gruppi o comunità, che appartengono cioè a più persone, oltre ai metadati e ai frammentari *digital exhaust* delle operazioni compiute in rete, estremamente significativi nel contesto dei Big Data[33].

Inoltre, il mondo degli algoritmi fa vacillare il paradigma basato su informativa e consenso; in specifico, è dubbio che in tale contesto le informazioni rese siano capaci davvero di informare in modo completo ed efficace e che il consenso possa considerarsi libero.

Nella mutata società dei Big Data, infatti, la rilevanza, ancora significativa, del consenso individuale e preventivo come elemento capace di legittimare il trattamento e perfino, laddove esplicito, il processo decisionale automatizzato è ontologicamente problematica[34]: il consenso preventivo, libero ed esplicito può essere ottenuto

[32] Cfr. G. D'Acquisto-M. Naldi, *Big data e privacy by design. Anonimizzazione, pseudonimizzazione, sicurezza*, Torino, Giappichelli, 2017, 34 ss.; V. Zeno-Zencovich-G. Giannone Codiglione, *Ten legal perspectives on the "Big data revolution"*, cit., 33 ss.

[33] Cfr. C. Focarelli, *La privacy*, cit., 28 ss.

[34] Artt. 7 e 22, reg. (UE) 2016/679.

a fronte di vantaggi perseguibili, come prezzi personalizzati, e perdere per questo sostanzialmente le caratteristiche che devono connotarlo[35]. Del resto ne è consapevole lo stesso regolamento quando nel considerando 42 chiarisce che «il consenso non dovrebbe essere considerato liberamente espresso se l'interessato non è in grado di operare una scelta autenticamente libera o è nell'impossibilità di rifiutare o revocare il consenso senza subire pregiudizio»: la condizione dell'individuo nei rapporti con le piattaforme online è costituita da una libertà apparente e il mancato consenso espone in ogni caso senza dubbio al pregiudizio di non fruire delle possibilità offerte in termini relazionali, sociali, professionali.

Proprio tali criticità sostanziali, la mancata conoscenza preventiva delle finalità e le correlate difficoltà nel rispetto dei principi della normativa comportano difficoltà ad assicurare le informazioni da fornire da parte del titolare del trattamento[36] e il consenso libero, preventivo, specifico, inequivocabile e revocabile dell'interessato[37], che rischiano di vanificarsi e di inficiare la stessa liceità del trattamento[38]. Su cosa sarà informato e su cosa esprimerà il consenso l'interessato, se non si conoscono preventivamente le finalità di utilizzo dei Big Data?

Del resto anche altri fondamenti di liceità del trattamento, quali l'esecuzione di un contratto di cui l'interessato è parte o il legittimo interesse[39], non sono esenti da criticità: nell'esecuzione di un contratto emerge lo squilibrio tra le parti e nel secondo caso si affaccia il sospetto possa prevalere il legittimo interesse sui diritti e sulle libertà fondamentali dell'interessato, che richiedono la protezione dei dati personali.

A ben vedere, le criticità esaminate trovano condiviso fondamento nell'opacità e nella chiusura dei processi di gestione dei dati, nel significativo squilibrio tra le parti e nella conseguente inevitabile incapacità per il singolo di potersi tutelare da solo.

35 Cfr. G. Colangelo, Big data, *piattaforme e antitrust*, cit., 448 ss.

36 Artt. 12-14, reg. (UE) 2016/679.

37 Art. 7, reg. (UE) 2016/679.

38 Cfr. F.H. Cate-V. Mayer-Schönberger, *Notice and consent in a world of Big Data*, in *International Data Privacy Law*, 2013, vol. 3, n. 2, 67-73.

39 Art. 6, paragrafo 1, lett. b) e f), reg. (UE) 2016/679.

Pertanto, per affrontare Big Data e algoritmi in modo efficace è opportuno valorizzare e dare applicazione ad alcuni principi che si pongono quale antidoto a tali problemi e che possono essere sintetizzati in trasparenza, apertura e controllo collettivo.

3.2. Trasparenza, apertura e controllo collettivo

Per contrastare l'opacità che rischia di caratterizzare l'utilizzo dei dati personali nel contesto dei Big Data, è necessario affidarsi a una trasparenza sostanziale, che per essere tale deve tradursi in un dovere di lealtà dei titolari del trattamento nei confronti degli interessati e nella parallela conoscenza da parte dell'interessato della logica degli algoritmi, accompagnata dalla consapevolezza in merito alle conseguenze e all'impatto sulla persona.

Sotto tale profilo risulta significativo quanto previsto dagli art. 13, paragrafo 2, lett. f) e art. 14, paragrafo 2, lett. g) del regolamento (UE) 2016/679. Il titolare del trattamento è tenuto, infatti, ai sensi di tali disposizioni, a fornire all'interessato, tra le ulteriori informazioni necessarie per garantire un trattamento corretto e trasparente, «l'esistenza di un processo decisionale automatizzato, compresa la profilazione [...] e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato».

I Big Data si avvalgono di processi decisionali automatizzati; in tale contesto, pertanto, la norma si traduce nella necessità di fornire informazioni sulla logica utilizzata dagli algoritmi, ma anche sull'impatto e sulle conseguenze per l'interessato. In tal modo è possibile riequilibrare la profonda asimmetria tra le parti, mantenendo il valore economico delle tecniche impiegate in mano ai titolari, ma imponendo maggiore trasparenza in merito alla logica utilizzata dagli algoritmi stessi, al fine di garantire la consapevole autodeterminazione e la correlata libertà degli individui, valori protetti dalla disciplina e, più ampiamente, dagli ordinamenti democratici.

Con questo approccio si sposa l'istanza di apertura e il rilascio dei dati in *open data*, esigenza che emerge in modo evidente nella normativa relativa ai dati pubblici[40]. Sono *open data* i dati resi disponibili con le caratteristiche tecniche e legali necessarie per esse-

[40] In particolare artt. 1 e 50 ss., d.lgs. 82/2005.

re liberamente utilizzati, riutilizzati e ridistribuiti da chiunque, in qualsiasi momento e ovunque[41].

L'apertura dei Big Data potrebbe contribuire a sanare, insieme alla trasparenza, le asimmetrie informative, mettendo a disposizione della collettività i dati, anche se inevitabilmente provocherebbe una perdita di potere per i titolari degli stessi[42].

Il significativo squilibrio tra le parti in gioco si traduce, altresì, nel rischio di "solitudine" e mancata consapevolezza del singolo, conseguentemente incapace di potersi tutelare in modo efficace. I valori della dignità e dello sviluppo della persona e dell'uguaglianza a fronte delle possibili manipolazioni e delle eventuali discriminazioni, che gli algoritmi sono capaci di realizzare, sono valori che interessano la collettività; parimenti, di conseguenza, può essere opportuno immaginare una tutela collettiva dell'individuo, che si affianchi a quella individuale[43].

Sotto il profilo della tutela collettiva del diritto emerge la disposizione contenuta nell'art. 80 del regolamento europeo 2016/679[44]; è particolarmente significativo il secondo paragrafo: «Gli Stati membri possono prevedere che un organismo, organizzazione o associazione [...], indipendentemente dal mandato conferito dall'interessato, abbia il diritto di proporre, in tale Stato membro, un reclamo all'autorità di controllo competente, e di esercitare i diritti di cui agli articoli 78 e 79 [diritto a un ricorso giurisdizionale effettivo nei confronti dell'autorità di controllo e diritto a un ricorso giurisdizionale effettivo nei confronti del titolare del trattamento o del responsabile

41 In tal senso l'*International Open Data Charter*; cfr. *https://opendatacharter.net*.

42 Cfr. A. Mantelero, *Big data: i rischi della concentrazione del potere informativo digitale e gli strumenti di controllo*, cit., 140 ss.

43 Cfr. A. Mantelero, *I Big Data nel quadro della disciplina europea della tutela dei dati personali*, in *Il Corriere giuridico*, ed. speciale, 2018, 54 ss.

44 La norma prevede, al paragrafo 1, il diritto dell'interessato di «dare mandato a un organismo, un'organizzazione o un'associazione senza scopo di lucro, che siano debitamente costituiti secondo il diritto di uno Stato membro, i cui obiettivi statutari siano di pubblico interesse e che siano attivi nel settore della protezione dei diritti e delle libertà degli interessati con riguardo alla protezione dei dati personali, di proporre il reclamo per suo conto e di esercitare per suo conto i diritti [...]», «nonché, se previsto dal diritto degli Stati membri, il diritto di ottenere il risarcimento [...]».

del trattamento], qualora ritenga che i diritti di cui un interessato gode a norma del [...] regolamento siano stati violati in seguito al trattamento». La protezione del singolo "si sgancia" dalla necessità di azione da parte dell'individuo stesso e può essere attivata da organizzazioni e associazioni nel momento in cui siano violati quei valori collettivi protetti dalla disciplina.

Il combinato disposto di trasparenza, apertura e controllo collettivo, che si collegano nel fine condiviso di garantire partecipazione e controllo agli interessati, permette di fornire informazioni sulla logica e sull'impatto degli algoritmi sull'individuo e di intervenire con una tutela collettiva a favore dell'interessato, laddove prevista dalla normativa dei singoli Stati, azionabile indipendentemente dal mandato dell'interessato stesso, al fine di proteggerlo in modo efficace.

4. Riflessioni conclusive

Le norme che favoriscono trasparenza e apertura e che promuovono una tutela collettiva accanto a quella individuale tracciano alcune direttrici sulle quali basare la *governance* etica e giuridica dei Big Data.

A questo proposito, sono interessanti e condivisibili le considerazioni delle "Guidelines on the Protection of Individuals with Regard to the Processing of Personal Data in a World of Big Data", adottate il 23 gennaio 2017 dal Comitato previsto dalla Convenzione 108, che evidenziano la centralità della persona e del suo diritto di controllo sui dati nell'era degli algoritmi.

Le linee guida, in modo conforme all'esaminata previsione dell'art. 80 del regolamento europeo, precisano la necessità di un diritto di controllo sui dati non circoscritto all'individuo, ma tale da comprendere una valutazione dei rischi per la collettività e suggeriscono la conseguente considerazione dell'impatto giuridico, sociale ed etico dell'utilizzo dei Big Data sia a livello individuale che collettivo, al fine di prevenire i potenziali effetti negativi dell'utilizzo dei Big Data sulla dignità umana, sulle libertà e sui diritti fondamentali degli individui.

In considerazione del difficile rispetto dei principi del regolamento europeo (minimizzazione dei dati, limitazione delle finalità, correttezza e trasparenza, consenso libero, specifico e informato) nel

contesto dei Big Data, le *guidelines* indicano la necessità di un uso etico, consapevole e socialmente responsabile dei dati, che comporta al momento dell'analisi del rischio la valutazione circa la possibilità di conflitto con altri diritti e valori, soprattutto laddove le informazioni siano impiegate per scopi predittivi nei processi decisionali. Si sottolinea, poi, l'importanza del ruolo dell'intervento umano nei processi decisionali basati sull'analisi dei Big Data, che va preservato nella sua autonomia, deve tenere conto di tutte le circostanze e deve consentire la libertà di non fare affidamento sui risultati, potendo assumere decisioni diverse da quelle consentite dall'analisi dei dati.

Nelle *guidelines* si richiamano la necessità del rispetto del principio di limitazione delle finalità e del principio di trasparenza, in modo da evitare che i dati siano ulteriormente elaborati in modo inaspettato, inappropriato o discutibile per l'interessato. In merito al consenso e al correlato pericolo che non sia efficace nel contesto dei Big Data, le linee guida suggeriscono di agevolare la comprensione delle operazioni per mezzo dell'utilizzo di interfacce grafiche, che simulino l'utilizzo dei dati e il potenziale impatto sull'interessato, ribadendo che il consenso non è da intendersi liberamente reso in condizioni di chiaro squilibrio di potere, atto a influenzare le decisioni dell'interessato: significativamente l'onere della prova al riguardo spetta al titolare.

Anche l'aspetto problematico dell'anonimizzazione è preso in esame dalle *guidelines*, che suggeriscono in proposito una valutazione del rischio di re-identificazione tenendo conto del tempo, degli sforzi e delle risorse necessarie alla luce della natura dei dati, del contesto, delle tecnologie e dei costi. Anche in tal caso la prova sull'adeguatezza delle misure di anonimizzazione spetta ai titolari, mostrando la rilevanza di *accountability* e responsabilizzazione del titolare nella tutela dell'interessato.

A tutto questo le linee guida accompagnano la necessità di cultura digitale, istruzione, informazione e formazione, abilità educative essenziali degli individui, da sviluppare al fine di far maturare una consapevolezza diffusa al riguardo e la correlata comprensione delle implicazioni sottese all'utilizzo dei Big Data.

Alla luce dell'analisi compiuta, nel difficile rapporto tra *data governance* e *data protection* è importante, infine, prestare attenzione alle finalità dell'utilizzo dei Big Data, che possono essere legate alla tutela di interessi generali, ma altresì a motivazioni economiche.

Sotto tale profilo, in considerazione del fatto che la protezione dei dati personali è funzionale ai diritti fondamentali dell'uomo, alla dignità e allo sviluppo della persona, anche se il regolamento europeo non traccia una gerarchia esplicita dei valori in gioco, non risulta congruo che tali diritti siano compressi per mere ragioni di profitto o motivazioni legate esclusivamente al mercato: per tale direzione il rischio è quello di smarrire la persona e i valori delle nostre società[45].

[45] Cfr. M.F. De Tullio, *La* privacy *e i* big data *verso una dimensione costituzionale collettiva*, in *Politica del diritto*, 2016, fasc. 4, 671 ss.

Manipolazione commerciale e privacy mentale all'ombra del GDPR

Gianclaudio Malgieri

Sommario: 1. Introduzione: privacy mentale e marketing manipolativo nel GDPR – 2. Articolo 22: manipolazione come "effetti analogamente significativi"? – 3. Vulnerabilità nel GDPR – 4. La Direttiva sulle Pratiche Commerciali Scorrette e la distorsione della libertà di scelta del consumatore – 5. Il problema del "consumatore medio" e dei gruppi vulnerabili "chiaramente individuabili" – 6. Manipolazione mentale come pratica commerciale "aggressiva"? – 7. Conclusioni: confrontando la tutela del GDPR con quella della direttiva sulle pratiche commerciali scorrette: mezzi v. effetti

1. Introduzione: privacy mentale e marketing manipolativo nel GDPR

Nel mercato digitale, la manipolazione commerciale online è una realtà crescente: le pubblicità comportamentali online sono una delle principali pratiche nell'economia delle piattaforme online.

Il GDPR non affronta esplicitamente il tema della pubblicità comportamentale e del marketing manipolativo. Ciononostante, ci sono diverse disposizioni in esso che meritano di essere considerate.

Innanzitutto, occorre notare che tra i principi per il trattamento dei dati personali all'art. 5 spicca il principio della "correttezza" al paragrafo 1, lettera a). Pare necessario comprendere l'esatto signifi-

cato di "correttezza"[1] in questo contesto per poter stabilire se la pubblicità manipolativa online possa essere considerata una violazione di quel principio.

È stato sostenuto in dottrina che la Corte di Giustizia dell'Unione Europea (CGUE) ha interpretato "correttezza" come protezione contro l'intrinseca asimmetria nel rapporto tra interessato e titolare del trattamento e dunque contro le possibili conseguenze negative del trattamento dei dati per gli interessati anche a prescindere da qualsiasi intento di trarre in errore gli interessati da parte del soggetto titolare[2].

In altri termini, il test di "correttezza" dovrebbe mirare a verificare il "corretto equilibrio" (fair balance) nell'applicazione dei requisiti contenuti nel GDPR: I dati non dovrebbero essere trattati in un modo da violare sproporzionatamente I diritti fondamentali e le libertà degli interessati e in particolare, il loro diritto alla privacy e alla protezione dei dati personali[3].

In realtà, dal momento che il marketing non può essere generalmente considerato una vera violazione di diritti fondamentali dei soggetti interessati, occorre trovare la linea di confine tra il marketing legittimo e l'illecita manipolazione dei consumatori/cittadini/soggetti interessati.

In altri termini, occorre determinare la distinzione normative tra ciò che Baldwin considerava "nudging" positivo ("enhancing rational thinking") e nudging negativo ("behavioural manipulation")[4].

[1] D. Clifford, *Citizen-consumers in a personalised Galaxy: Emotion influenced decision-making, a true path to the dark side?*, in *CiTiP Working Paper*, 31/2017, KU Leuven Centre for IT & IP Law, 17.

[2] Cfr., College van burgemeester en wethouders van Rotterdam v MEE Rijkeboer [2009] Court of Justice of the European Union C-553/07 and X [2013] Court of Justice of the European Union C-486/12; in relation to the balancing of different fundamental rights see Google Spain SL, Google Inc v Agencia Española de Protección de Datos (AEPD), Mario Costeja González [2014] Court of Justice of the European Union C-131/12; Promusicae v Telefónica [2008] Court of Justice of the EU C-275/06, Curia.

[3] D. Clifford-J. Ausloos, *Data Protection and the Role of Fairness*, in *CiTiP Working Paper Series*, 31/2017. Available at SSRN: https://ssrn.com/abstract=3037425, 14.

[4] R. Baldwin, *From Regulation to Behaviour Change: Giving Nudge the Third Degree*, in *The Modern Law Review*, 77, 2014, 831.

Un'altra disposizione che va presa in considerazione è l'articolo 6, sulla liceità del trattamento. In base a tale disposizione, qualsiasi trattamento di dati personali necessita di una chiara base giuridica tra quelle elencate all'articolo 6, par. 1 (consenso, necessità per adempimento di un contratto, obbligo di legge, interesse pubblico, legittimo interesse, interesse vitale)[5].

Dunque resta da capire se le pubblicità comportamentali online possono considerarsi basate su un legittimo interesse (art. 6, lett. e) o se necessitino sempre del consenso espresso del soggetto interessato.

Il Gruppo di lavoro Articolo 29 (WP29) nel 2010[6] si era già espresso sul punto, affermando che alla luce della previgente normative 95/46/EC, le pubblicità comportamentali online necessitano sempre, come base giuridica, del consenso del soggetto interessato.

In realtà, il GDPR presenta oggi una interessante novità: il considerando 47 afferma che «può essere considerato *legittimo interesse* trattare dati personali per *finalità di marketing diretto*»[7], rigettando apparentemente la summenzionata opinione del WP29.

Comunque, tale discussione non costituisce l'oggetto specifico di tale capitolo e non può adeguatamente essere affrontata qui[8].

Un altro tema problematico è la liceità del trattamento di eventuali dati sensibili (categorie particolari di dati personali) coinvolti nelle pubblicità comportamentali. Infatti, in base all'art. 9 GDPR, se i dati sono tra le categorie particolari (rivelano, cioè, opinioni politiche, filosofiche, religiose, sindacali, stato di salute, vita sessuale od orientamento sessuale, sono dati genetici o biometrici tesi ad identificare univocamente il soggetto interessato), le basi giuridiche per tale trattamento sono maggiormente limitate (ad es., consenso esplicito, interesse vitale, dati resi manifestamen-

[5] Sul punto vedere P. De Hert-I. Kamara, *Understanding the balancing act behind the legitimate interest of the controller ground: a pragmatic approach*, in E. Selinger-J. Polonetsky-O. Tene, *Cambridge Handbook of Consumer Privacy*, Cambridge, Cambridge University Press, 2017.

[6] Article 29 Working Party, Opinion 2/2010 on online behavioural advertising, WP 171.

[7] Enfasi aggiunta.

[8] Per maggiori dettagli, cfr. D. Clifford, *Citizen-consumers in a personalised Galaxy*, cit., 17-20.

te pubblici, interesse pubblico rilevante, medicina preventiva, medicina del lavoro). Inoltre, in tal caso, se questi dati sensibili sono trattati su larga scala potrebbe essere necessario adottare altre cautele per i soggetti interessati (come l'effettuazione di una Valutazione d'Impatto sul trattamento dei dati personali ai sensi dell'art. 35, par. 3 del GDPR oppure l'obbligo di dotarsi di un Responsabile del Trattamento dei dati personali ai sensi dell'art. 37, par. 1, lett. c)

Potremmo chiederci se l'art. 9 del GDPR si applichi anche a modalità particolarmente intrusive di pubblicità comportamentale: la domanda è, dunque, se i dati comportamentali possono essere considerati "sensibili". In realtà, non si può fornire una risposta generale: dipende dallo specifico tipo di dati comportamentali in oggetto (ad es. se rivelano la vita sessuale, la salute, le opinioni del soggetto interessato) oppure sul modo in cui i dati sono raccolti (ad es., tramite dispositivi di "eye tracking" oppure riconoscimento facciale, i quali possono ben essere considerati una raccolta di "dati biometrici intesi a identificare in modo univoco una persona fisica"; al contrario di altre forme di raccolta di dati comportamentali, come l'inferenza testuale o da cronologia web)[9].

Pertanto, occorre investigare se altre parti del GDPR possano tutelare l'integrità mentale dei soggetti interessati contro le diverse forme di manipolazione commerciale online.

2. Articolo 22: manipolazione come "effetti analogamente significativi"?

Un'altra disposizione meritevole di considerazione è l'art. 22, il "diritto a non essere soggetti a decisioni automatizzate". Al paragrafo 1, l'art. 22 stabilisce che «l'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o *che incida in modo analogo significativamente sulla sua persona*»[10].

[9] Cfr. D. Clifford, *Citizen-consumers in a personalised Galaxy*, cit., 22.

[10] Enfasi aggiunta.

In realtà, la *ratio* dell'articolo 22 non è già la prevenzione di *effetti* negativi sui soggetti interessati, ma porre dei limiti alle decisioni automatizzate che impiegano dati personali dei soggetti[11].

In altre parole, anche considerando lo scopo del GDPR, l'articolo 22 si occupa dei "mezzi" decisionali (*come* la decisione è raggiunta) piuttosto che degli "effetti" della decisione (ad es., manipolazione dei consumatori).

Considerando che la pubblicità comportamentale è generalmente basata su profilazione automatizzata, ci dovremmo chiedere se gli effetti che essa produce (manipolazione commerciale) possa essere considerata nell'ambito degli "effetti giuridici o analogamente significativi" di cui all'art. 22, par. 1.

Il Gruppo di Lavoro art. 29 ha recentemente rilasciato delle linee guida sulla profilazione ai sensi del GDPR[12]. Nell'interpretare gli "effetti giuridici o analogamente significativi", WP29 spiega che «un trattamento di dati per avere effetti significativi deve comportare effetti sufficientemente significativi ed importanti da essere meritevoli di attenzione»[13].

Di conseguenza, WP29 ha elencato tre fattori alternativi che possono aiutare a determinare se l'effetto è significativo: «la decisione deve avere il potenziale per:

- Influenzare significativamente le circostanze, il comportamento o le scelte del soggetto interessato;
- Avere effetti prolungati o permanenti sul soggetto; oppure
- In casi estremi, condurre all'esclusione o alla discriminazione di alcuni soggetti»[14].

[11] Cfr. in generale Article 29 Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, WP251rev.01, adopted on 3 October 2017, as last revised and adopted on 6 february 2018.

[12] Article 29 Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, WP251rev.01, 21.

[13] «For data processing to significantly affect someone the effects of the processing must be sufficiently great or important to be worthy of attention».

[14] «The decision must have the potential to: significantly affect the circumstances, behaviour or choices of the individuals concerned; have a prolonged or permanent impact on the data subject; or at its most extreme, lead to the exclusion or discrimination of individuals».

In altre parole, questi parametri si riferiscono a: effetti *interni* (influenzare comportamento/scelte), *durata* degli effetti (impatto prolungato/permanente) ed effetti *esterni* (esclusione/discriminazione). È interessante notare che, sebbene in dottrina questa ampia interpretazione di WP29 degli "effetti significativi" sia stata considerata in violazione del testo stesso dell'art. 22, sembra chiaro che il primo criterio («influenzare significativamente [...] il comportamento o le scelte del soggetto interessato») si riferisca esplicitamente alla manipolazione.

Infatti, il marketing comportamentale e la manipolazione online chiaramente influenzano significativamente il comportamento e la libertà di scelta dei consumatori/utenti.

In realtà, WP29 menziona esplicitamente il caso del marketing online: «ciò ci porta al problema delle pubblicità online, che sono sempre più basate su mezzi automatici e riguardano decisioni individuali totalmente automatizzate»[15].

WP29 chiarisce, tuttavia, che in molti casi tipici la decisione di presentare pubblicità mirata basata sulla profilazione «non ha effetti significativi sugli individui». In particolare, si fa un esempio emblematico: «la pubblicità per un outlet di moda di successo online basata su un semplice profilo demografico, del tipo: 'le donne nella regione di Brussels tra i 25 e i 35 anni sono più inclini ad essere interessate alla moda e in certi prodotti di vestiario[16]»

Questo esempio si riferisce chiaramente al "targeting", piuttosto che al *microtargeting* personalizzato: se sono impiegate poche e approssimative variabili (sesso, età approssimativa e regione di provenienza) la pubblicità non dovrebbe considerarsi procurare effetti significativi ai consumatori. Al contrario, nel caso del *microtargeting*, cioè *targeting* basato su una profilazione comportamentale dettagliata, la pubblicità può ben provocare effetti significativi (come la manipolazione).

[15] Article 29 Working Party, *Guidelines on Automated individual decision-making*, 22: «this brings us also to the issue of *online advertising*, *which increasingly relies on automated tools and involves solely automated individual decision-making*». Enfasi aggiunta.

[16] *Ibidem*: «the advertisement for a mainstream online fashion outlet based on a simple demographic profile: "women in the Brussels region aged between 25 and 35 who are likely to be interested in fashion and certain clothing items"».

È interessante notare che il WP29 ha anche indicato una lista di parametri specifici che dovrebbero essere presi in considerazione per determinare se le pratiche di marketing sono considerabili rilevanti ai sensi dell'art. 22, par. 1 del GDPR:

- l'intrusività del processo di profilazione, per esempio il tracciamento dei soggetti attraverso differenti siti, dispositivi e servizi;
- le aspettative e i desideri dei soggetti interessati;
- il modo in cui la pubblicità è presentata al soggetto;
- l'utilizzo di conoscenze sulle vulnerabilità dei soggetti profilati[17].

In altre parole, ciò che è considerato rilevante per valutare gli effetti manipolativi della pubblicità comportamentale è: l'intrusività delle tecniche di raccolta dei dati personali; le peculiarità del contesto del consumatore; la pratica pubblicitaria adoperata e lo sfruttamento di vulnerabilità individuali.

Tale chiarimento pare fornire dei parametri fondamentali per determinare il confine tra legittima ed illegittima manipolazione[18].

WP29 spiega che tali parametri sono stati scelti perché gli "effetti" del marketing dipendono fortemente dalle peculiarità dei soggetti profilati e dalle specifiche pratiche pubblicitarie adoperate: «il trattamento che potrebbe avere un trascurabile impatto su alcuni soggetti potrebbe in realtà avere effetti significativi su *alcuni gruppi sociali*, come ad esempio minoranze o adulti vulnerabili. Per esempio qualcuno noto per avere difficoltà economiche che riceve regolarmente pubblicità con prestiti ad alto interesse potrebbe accettare tali offerte che potenzialmente potrebbe procurare maggiori debiti al soggetto stesso»[19].

[17] «The intrusiveness of the profiling process, including the tracking of individuals across different websites, devices and services; the expectations and wishes of the individuals concerned; the way the advert is delivered; or using knowledge of the vulnerabilities of the data subjects targeted».

[18] Vd. M. Veale-L. Edwards, *Clarity, surprises, and further questions*, cit.

[19] «Processing that might have little impact on individuals generally may in fact have a significant effect for *certain groups of society*, such as minority groups or *vulnerable adults*. For example, someone known or likely to be in financial difficulties who is regularly targeted with adverts for high interest loans may sign up for these offers and potentially incur further debt». Enfasi aggiunta. WP29

3. Vulnerabilità nel GDPR

Il riferimento agli "adulti vulnerabili" è particolarmente interessante. La manipolazione è soprattutto basata sullo sfruttamento di vulnerabilità individuali[20], ma al tempo dei Big Data e del data mining, le vulnerabilità sono spesso nascoste, sottili o addirittura sconosciute al soggetto stesso.

Ciò che è interessante è che non c'è alcuna menzione del concetto di "vulnerabilità" nell'articolato del GDPR, se non in un fugace passaggio al considerando 75 sui rischi rilevanti da prendere in considerazione quando si effettua una Valutazione d'Impatto sul Trattamento dei Dati ai sensi dell'art. 35 (se sono trattati dati personali di *persone fisiche vulnerabili*, in particolare minori). In quel caso, il GDPR menziona "persone fisiche vulnerabili", con uno specifico esempio di vulnerabilità: i minori. Ciò rende ancora più interessante l'espressione "adulti vulnerabili" adoperata da WP29: essa si riferisce a tutti gli altri tipi di vulnerabilità che non sono menzionabili nel GDPR, né probabilmente determinabili a priori.

Spiegheremo più giù che un altro paradigma giuridico che affronta il tema delle vulnerabilità è quello delle pratiche commerciali scorrette.

Un'ultima domanda che può sorgere dal GDPR è se la manipolazione può essere considerate un "rischio per I diritti e le libertà delle persone fisiche" sotto la definizione dello scopo materiale della Valutazione d'Impatto *ex* art. 35.

Il considerando 75 spiega che tali rischi «possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale». Menziona, inoltre, una serie di casi problematici che dovrebbero essere considerati: discriminazione, furto d'identità, rivelazione di dati sensibili, *scoring*, gran numero di soggetti interessati coinvolti e, tra l'altro, come già riferito poco

aggiunge anche: «Automated decision-making that results in differential pricing based on personal data or personal characteristics could also have a significant effect if, for example, prohibitively high prices effectively ban someone from certain goods or services».

[20] R. Calo, *Digital Market Manipulation*, in *The George Washington Law Review*, vol. 82:995, 1031-1033.

sopra, il trattamento di dati di "persone fisiche vulnerabili, in particolare minori".

Il WP29 nelle sue linee guida sulla Valutazione d'Impatto[21] spiega che la vulnerabilità non può essere limitata soltanto ai minori, ma dovrebbe comprendere anche i lavoratori dipendenti (rispetto al loro datore di lavoro), ma anche segmenti vulnerabili di popolazione che richiedono una speciale protezione, come ad esempio, le persone con patologie mentali, i richiedenti asilo, gli anziani, i pazienti o qualsiasi caso in cui si può identificare uno sbilanciamento tra la posizione dei soggetti interessati e il titolare del trattamento[22].

Anche se WP29 non menziona i "consumatori" tra le categorie vulnerabili, si chiarisce che ciò che determina la vulnerabilità è lo "squilibrio" tra soggetti interessati e titolari del trattamento[23]. La nozione di "squilibrio", peraltro, è spesso utilizzata anche in ambito di diritto dei consumatori[24] e può dunque essere applicata almeno alla gran parte delle relazioni c.d. B2C.

In particolare, la relazione tra i soggetti e i titolari del trattamento che effettuano pubblicità comportamentali online (utilizzando informazioni sulle vulnerabilità, utilizzando tecniche di data mining

[21] Article 29 Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, WP248, 4 aprile 2017.

[22] Article 29 Working Party, Guidelines on Data Protection Impact Assessment (DPIA), 9: «vulnerable segment of the population requiring special protection, such as, for example, the mentally ill, asylum seekers, or the elderly, a patient or in any case where an imbalance in the relationship between the position of the data subject and the controller can be identified».

[23] Article 29 Working Party, *Guidelines on Automated individual decision-making*, 9: «For example, employees would often meet serious difficulties to oppose to the processing performed by their employer, when it is linked to human resources management. Similarly, children can be considered as not able to knowingly and thoughtfully oppose or consent to the processing of their data. This also concerns more vulnerable segment of the population requiring special protection, such as, for example, the mentally ill, asylum seekers, or the elderly, a patient, or in any case where an imbalance in the relationship between the position of the data subject and the controller can be identified».

[24] Cfr. Council Directive 93/13/EEC of 5 april 1993 on unfair terms in consumer contracts, art. 2(a).

intrusive e/o violando le aspettative dei soggetti interessati) appare chiaramente basata su uno squilibrio significativo.

Di conseguenza, la manipolazione commercial può ben essere considerate, nei limiti sopra detti, un "rischio per i diritti e le libertà delle persone fisiche" che dovrebbe essere limitato e preso in considerazione almeno attraverso la Valutazione d'Impatto sul trattamento dei dati.

Comunque, come è già stato ricordato sopra, la sola esplicita categoria di "vulnerabile" menzionata nel GDPR è quella dei minori (considerando 75). In effetti, tale categoria è la più facilmente riconoscibile, poiché si basa su un parametro oggettivo (l'età), facilmente verificabile. Di conseguenza, per i titolari del trattamento può risultare più semplice proteggere la sola categoria esplicitamente menzionata tra quelle vulnerabili nel GDPR piuttosto che altre categorie di soggetti vulnerabili.

È interessante citare qui l'esempio di Facebook, che ha adottato misure specifiche per proteggere quel tipo di vulnerabilità. In particolare, in base ai nuovi Termini di Servizio, per i minori: a) le categorie di pubblicità sono più limitate; b) il riconoscimento facciale è disabilitato per chiunque sotto i 18 anni; c) è necessario il consenso dei genitori per abilitare le pubblicità basate sui dati raccolti dai partner commerciali di Facebook e che possano includere informazioni su interessi religiosi o politici del minore.

In pratica, tali minori vedranno una versione di Facebook meno personalizzata con una condivisione di dati ristretta e pubblicità meno rilevanti finché non sarà prestato il consenso parentale alla fruizione di tutti gli aspetti del social network[25].

[25] Facebook, Terms of Services: «We've built many special protections into Facebook for all teens, regardless of location. For example, advertising categories for teens are more limited, and their default audience options for posts do not include "public". We also keep face recognition off for anyone under age 18 and limit who can see or search specific information teens have shared, like hometown or birthday. Later this year we'll introduce a new global online resource center specifically for teens, and more education about their most common privacy questions.

Under GDPR, people between the ages of 13 and 15 in some EU countries need permission from a parent or guardian to allow some features on Facebook – seeing ads based on data from partners and including religious and political views or

La cosa interessante è che, per proteggere la sola categoria esplicitamente vulnerabile, Facebook sta limitando la pubblicità comportamentale, le tecniche di rilevazione delle emozioni (e.g. riconoscimento facciale, *eye tracking*, ecc.) e l'uso di dati sensibili provenienti da partner commerciali. Implicitamente tali misure rilevano il cuore della manipolazione online: lo scambio di dati con partner commerciali, l'utilizzo di informazioni sulle vulnerabilità individuali (dati sensibili, mezzi di rilevazione emozionale) che vanno a costituire dettagliati *microtargeting*.

Questo insieme di funzionalità che Facebook limita per i minori sembra riferirsi curiosamente richiamare la lista di parametri menzionati dal WP29 come rivela la Tabella 1.

Tabella 1. Comparazione tra i parametri del WP29 che descrivono la manipolazione commerciale e specifiche salvaguardie proposte da Facebook per una maggiore tutela dei minori sul social network

Parametri del WP29 che descrivono la manipolazione commerciale	*Salvaguardie proposte da Facebook per una maggiore tutela dei minori*
Intrusività delle tecniche di raccolta dei dati	Limitare la condivisione dei dati con partner o rendere i dati dei minori non accessibili pubblicamente
Le peculiarità del contesto del consumatore	Implicito (servizio riservato ai minori)
La pratica pubblicitaria impiegata	Limitare le pubblicità commerciali personalizzate sulla pagina Facebook
Lo sfruttamento di dati sulle vulnerabilità individuali	Limitare l'uso di dati sensibili e riconoscimento facciale

"interested in" on your profile. These teens will see a less personalized version of Facebook with restricted sharing and less relevant ads until they get permission from a parent or guardian to use all aspects of Facebook. Even where the law doesn't require this, we'll ask every teen if they want to see ads based on data from partners and whether they want to include personal information in their profiles».

4. La Direttiva sulle Pratiche Commerciali Scorrette e la distorsione della libertà di scelta del consumatore

Oltre al diritto sulla protezione dei dati personali, ciò che può essere d'aiuto per determinare il confine tra "nudging" accettato e manipolazione illecita alla luce del diritto UE è anche la Direttiva sulle pratiche commerciali scorrette.[26]

È interessante innanzitutto notare che il considerando 6 di detta Direttiva suggerisce proprio questo confine: «La presente direttiva lascia altresì impregiudicate pratiche pubblicitarie e di marketing generalmente ammesse, quali il product placement consentito, la differenziazione del marchio o l'offerta di incentivi in grado di incidere legittimamente sulla percezione dei prodotti da parte dei consumatori e di influenzarne il comportamento senza però limitarne la capacità di prendere una decisione consapevole».

Di conseguenza, "incidere sulla percezione" o "influenzare i comportamenti" dei consumatori appare legittimo, mentre "limitare la capacità di prendere una decisione consapevole" non lo è.

In altre parole, già da questa primissima disposizione, sembra che possiamo tracciare la linea di confine tra marketing accettato e manipolazione illecita nella "limitazione della capacità di scelta". Quindi, ciò che sembra rilevare come bene giuridico protetto è l'integrità mentale, la continuità psicologica e/o la libertà cognitiva del consumatore consapevole e ben informato. Questi valori possono ben essere considerati parte di un più ampio diritto alla "privacy mentale" di cui anche parla recente dottrina[27].

Ma cosa vuol dire in concreto "effetti limitative della capacità di scelta? Come possiamo distinguere la mera influenza ("nudging"

[26] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive').

[27] M. Ienca-R. Adorno, *Towards new human rights in the age of neuroscience and neurotechnology*, in *Life Sciences, Society and Policy*, 13, 2017, 5.

c.d. positivo) dalla limitazione mentale (manipolazione) ai sensi della Direttiva sulle Pratiche Commerciali Scorrette?

Una possibile risposta può essere trovata all'art. 5, par. 2, ovvero la definizione generale di pratica commerciale "scorretta": «Una pratica commerciale è sleale se: a) è contraria alle norme di diligenza professionale, e b) *falsa o è idonea a falsare in misura rilevante il comportamento economico*, in relazione al prodotto, *del consumatore medio* che raggiunge o al quale è diretta o *del membro medio di un gruppo* qualora la pratica commerciale sia diretta a un determinato gruppo di consumatori»[28].

In altre parole, il parametro è quello del "consumatore medio" (o del membro medio di un particolare gruppo di consumatori) e gli effetti limitativi sembrano significare una materiale distorsione del comportamento economico del consumatore da un parametro medio.

5. Il problema del "consumatore medio" e dei gruppi vulnerabili "chiaramente individuabili"

Comunque, appare interessante che anche nella Direttiva sulle pratiche commerciali scorrette il parametro "medio" non è un parametro assoluto, ma è relativo al "particolare gruppo di consumatori" a cui la pratica commerciale è diretta.

L'art. 5, par. 3 chiarisce che «Le pratiche commerciali che possono falsare in misura rilevante il comportamento economico solo di *un gruppo di consumatori chiaramente individuabile*, particolarmente *vulnerabili* alla pratica o al prodotto cui essa si riferisce a motivo della loro infermità mentale o fisica, della loro età o ingenuità, *in un modo che il professionista può ragionevolmente prevedere* sono valutate nell'ottica del membro medio di tale gruppo»[29].

È interessante notare che la sola deroga dalla "finzione" del consumatore medio razionale è basata sul "gruppo chiaramente identificabile di consumatori", in particolare è basata sull'infermità mentale o fisica, sull'età o sull'ingenuità

[28] Enfasi aggiunta.
[29] Enfasi aggiunta.

Se confrontiamo i gruppi vulnerabili giuridicamente riconosciuti dal GDPR (sia nel testo che nelle summenzionate linee guida del WP29 sulla Valutazione d'Impatto[30]) con quelli riconosciuti dalla ora citata disposizione troviamo somiglianze interessanti come mostrato nella Tabella 2.

Tabella 2. Confronto tra esempi di categorie giuridicamente riconosciute come vulnerabili alla luce del GDPR e della Direttiva 2005/29/CE

Gruppi vulnerabili alla luce del GDPR	*Gruppi Vulnerabili alla luce della Direttiva sulle pratiche commerciali scorrette*
'Persone con patologia psichica', 'pazienti' (WP29)	'Infermità mentale e psichica' (art. 5(3))
'Bambini' (considerando 75), 'anziani' (WP29)	'Età' (art. 5(3))
	'Ingenuità' (art. 5(3))
'Richiedenti asilo' (WP29)	
'Qualsiasi volta in cui ci sia uno squilibrio nelle relazioni' (WP29)	

Mentre l'età e le condizioni di salute mentale e fisica sono punti in comune, la maggiore differenza tra i due modelli è che alla luce dell'interpretazione che ha fornito WP29 del GDPR c'è una clausola aperta che può meglio proteggere i gruppi vulnerabili non individuabili a priori (vulnerabilità come squilibrio), mentre ai sensi della Direttiva 2005/29/EC troviamo una categoria intermedia e trasversale di "ingenuità". Ovviamente "ingenuità" e "squilibrio nelle relazioni" sono concetti diversi, ma forse ampi abbastanza da includere anche situazioni non prevedibili a priori dal legislatore.

Infatti, nella società dei Big Data, la vulnerabilità non è meramente basata su gruppi pre-individuabili di adulti vulnerabili, come invece sembra riferire la Direttiva sulle pratiche commerciali scorrette.

[30] Article 29 Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*, Adopted on 4 april 2017 as last revised and adopted on 4 october 2017, 10.

Tale Direttiva fu approvata nel 2005, quando il *microtargeting* e le pubblicità comportamentali non avevano raggiunto il livello di sviluppo tecnologico che hanno oggi. Di conseguenza, il concetto di "consumatore medio" era ancora considerato un parametro valido. Oggi, invece, l'idea di consumatore medio è messa fortemente in crisi per via dello sfruttamento personalizzato delle vulnerabilità individuali. L'idea del consumatore razionale è stata considerata in dottrina una "functional fiction" (finzione funzionale)[31], ma oggi – anche considerando lo sviluppo e la consapevolezza dell'economia comportamentale – tal finzione è sempre meno "funzionale" e sempre più considerabile "disfunzionale"[32].

L'idea del consumatore "medio", "razionale" e consapevole ha infatti dimostrato di essere una illusione: ogni consumatore è relativamente irrazionale e vulnerabile in alcune specifiche circostanze. [33] In altri termini, la vulnerabilità è oggi considerata graduale, contestuale e non limitata a "gruppi" legalmente riconosciuti[34].

Pertanto, non solo l'idea di considerare le vulnerabilità (come deviazioni dal consumatore medio) in gruppi specifici "chiaramente individuabili" è anacronistica ma lo stesso fatto di considerare il "membro medio" di questi gruppi vulnerabili può apparire una maldestra riproduzione della finzione dis/funzionale[35] del consumatore razionale in più piccolo gruppi "non-medi".

[31] A. Rouvroy, *The end(s) of critique: data-behaviourism vs. due-process*, in *Privacy, Due Process and the Computational Turn. Philosophers of Law Meet Philosophers of Technology*, M. Hildebrandt-E. De Vries (eds.), Routledge, 2012, 157-158.

[32] D. Clifford, *Citizen-consumers in a personalised Galaxy: Emotion influenced decision-making, a true path to the dark side?*, cit., 30.

[33] Cfr., e.g., F. Luna, *Elucidating the Concept of Vulnerability: Layers Not Labels*, in *Int'l J. Feminist Approaches to Bioethics*, spring 2009, at 121, 129 («A way for understanding this proposal is not by thinking that someone is vulnerable, but by considering a particular situation that makes or renders someone vulnerable»). See also R. Calo, *Digital Market Manipulation*, cit., 1033.

[34] *Ibidem*.

[35] Cfr. più ampiamente D. Clifford, *Citizen-consumers in a personalised Galaxy: Emotion influenced decision-making, a true path to the dark side?*, cit., 30. See also A. Rouvroy, *The end(s) of critique: data-behaviourism vs. due-process*, in *Privacy, Due Process and the Computational Turn. Philosophers of Law Meet Philosophers of Technology*, M. Hildebrandt-E. De Vries (eds.), Routledge, 2012, 157-158.

6. Manipolazione mentale come pratica commerciale "aggressiva"?

A parte la definizione generale di "pratiche commerciali scorrette", la Direttiva fornisce anche due sotto-definizioni: pratiche aggressive e pratiche ingannevoli.

Tralasciando la definizione di pratiche ingannevoli (articolo 6) che sembra fuoriuscire dai confini di tale capitolo, ci concentreremo sulla definizione di "pratica aggressiva".

Si definisce aggressiva (articolo 8) una «pratica commerciale che, nella fattispecie concreta, tenuto conto di tutte le caratteristiche e circostanze del caso, mediante molestie, coercizione, compreso il ricorso alla forza fisica, o *indebito condizionamento*, limiti o sia idonea a *limitare considerevolmente la libertà di scelta o di comportamento* del consumatore medio in relazione al prodotto e, pertanto, lo induca o sia idonea ad indurlo ad assumere una decisione di natura commerciale che non avrebbe altrimenti preso» [36].

È interessante rilevare anche all'articolo 8 lo stesso riferimento alla limitazione della libertà di scelta summenzionata in merito al considerando 6. Inoltre, la sola possibile condotta che sembra rilevante per scolpire il fenomeno della manipolazione digitale non è certo la forza fisica, ma più probabilmente l'"indebito condizionamento".

Nonostante l'ampio significato di tale espressione, l'art. 2, lett. j definiscono meglio l'indebito condizionamento come «lo sfruttamento di una *posizione di potere* rispetto al consumatore per esercitare una pressione, anche senza il ricorso alla forza fisica o la minaccia di tale ricorso, in modo da *limitare notevolmente la capacità del consumatore di prendere una decisione consapevole*» [37].

Il riferimento alla "posizione di potere", peraltro, sembra molto simile all'«aumentato squilibrio di potere tra il soggetto interessato e il titolare», oggetto dell'ampia definizione di vulnerabilità ai sensi delle succitate linee guida del WP29[38].

[36] Enfasi aggiunta.

[37] Enfasi aggiunta.

[38] Questo riferimento può anche essere trovato al considerando 43 del GDPR sulla libertà di consenso. La menzione allo "squilibrio" è anche un elemento central nella definizione di termini contrattuali abusive nella Direttiva 93/13/

Da ultimo, occorre aggiungere che l'Annesso I della Direttiva 2005/29/EC fornisce una specifica lista nera delle pratiche commerciali scorrette vietate sempre. Ebbene, in tale annesso non c'è alcuna menzione della manipolazione online basata sulla profilazione comportamentale. In quella lista è possibile trovare soltanto una lista di casi molto specifici di pratiche aggressive o ingannevoli[39].

7. Conclusioni: confrontando la tutela del GDPR con quella della direttiva sulle pratiche commerciali scorrette: mezzi v. effetti

Se confrontiamo i due diversi approcci summenzionati (del GDPR e della direttiva sulle pratiche commerciali scorrette) possiamo trovare diversi parametri per distinguere marketing legittimo da manipolazione illecita (vedere Tabella 3 a pagina seguente).

La differenza tra questi due paradigmi si basa sulle diverse prospettive considerate: il GDPR si focalizza sulle fonti delle pubblicità comportamentali online (i dati personali appunti) o, meglio, sui "mezzi" della manipolazione. D'altro canto, la Direttiva 2005/29/EC è basata sulla protezione contro gli effetti (economici) delle pubblicità comportamentali.

Probabilmente solo una combinazione di questi due diversi paradigmi può aiutare a scolpire i confini del diritto alla privacy mentale contro la manipolazione commerciale.

Infatti, un punto in comune ad entrambi i paradigmi concerne gli effetti "interni" sugli individui: effetti significativi in base a aspettative, vulnerabilità e intrusività dei mezzi di raccolta dei dati ai sensi dell'art. 22 GDPR; limitazione della libertà mentale ai sensi dell'art. 8 della Direttiva 2005/29/EC.

CEE del Consiglio, del 5 aprile 1993, concernente le clausole abusive nei contratti stipulati con i consumatori all'art. 3(1) («1. Una clausola contrattuale, che non è stata oggetto di negoziato individuale, si considera abusiva se, malgrado il requisito della buona fede, determina, a danno del consumatore, un *significativo squilibrio* dei diritti e degli obblighi delle parti derivanti dal contratto». Enfasi aggiunta).

[39] Vedi Direttiva 2005/29/EC, Annesso I.

Tabella 3. Confronto tra l'approccio del GDPR e quello della Direttiva 2005/29/EC alla pubblicità manipolativa

WP29 su art. 22, GDPR	*Art. 8, Direttiva sulle pratiche commerciali scorrette*
La pubblicità online ha effetti significativi sui soggetti ai sensi dell'art. 22, prendendo in considerazione: • l'intrusività del processo di profilazione, per esempio il tracciamento dei soggetti attraverso differenti siti, dispositivi e servizi; • le aspettative e i desideri dei soggetti interessati; • il modo in cui la pubblicità è presentata al soggetto; • l'utilizzo di conoscenze sulle vulnerabilità dei soggetti profilati".	Una pratica commerciale [anche pubblicitaria online] è scorretta e, in particolare, aggressive se: • attraverso indebita influenza, • limiti o sia idonea a *limitare considerevolmente la libertà di scelta o di comportamento* del consumatore medio e • lo induca o sia idonea ad indurlo ad assumere una decisione di natura commerciale che non avrebbe altrimenti preso

È interessante fare riferimento al lavoro di Ryan Calo in tema di manipolazione online, in cui egli ha provato a determinare i "danni" della manipolazione commerciale sui consumatori. In particolare ha sottolineato tre diversi tipi di danno: il danno economico, il danno alla privacy e "la vulnerabilità come danno". [40]

In realtà, pare chiaro che il danno alla privacy rappresenti il "mezzo" della pubblicità manipolativa, mentre il danno economico rappresenti gli effetti "esterni" e, la vulnerabilità-danno riguardi invece gli effetti (mentali) interni.

Possiamo, dunque, provare a coniugare i due summenzionati diversi paradigmi e provare a sintetizzare le tre variabili necessarie per distinguere il marketing permesso dalla manipolazione illecita:

Le caratteristiche del trattamento dei dati personali effettuato (l'utilizzo di informazioni sulle vulnerabilità, il contesto del consumatore, l'intrusività dei mezzi di raccolta), cioè che Calo definisce il danno alla privacy;

Effetti interni, ovvero effetti mentali (manipolazione, distorsione), che è ciò che Calo definisce danno-vulnerabilità;

[40] R. Calo, *Digital Market Manipulation*, cit., 1025-1034.

Effetti esterni, ovvero gli effetti economici (azioni e scelte che non si sarebbero altrimenti prese), ciò che Calo definisce danno economico.

Firme grafometriche e trattamento dei dati biometrici alla luce del GDPR

Aurora Cavo

Sommario: 1. La firma grafometrica: in particolare, la firma grafometrica avanzata come firma biometrica – 2. Gli obblighi a carico dei soggetti proponenti le soluzioni di firma biometrica a confronto con il GDPR – 3. Uso di nuove tecnologie nelle firme biometriche: legge di bilancio 2018 e spunti di riflessione – 4. Conclusioni

1. La firma grafometrica: in particolare, la firma grafometrica avanzata come firma biometrica

Tra le firme elettroniche maggiormente diffuse per la sottoscrizione di documenti informatici e ai fini di identificazione ed autenticazione, in particolare in ambito bancario ed assicurativo, la firma grafometrica occupa un posto di rilievo.

Tale tipo di firma, consistente in concreto nella sottoscrizione autografa apposta per lo più su *tablet* informatico, può diversamente qualificarsi sotto il profilo giuridico a seconda della tecnologia prescelta dal soggetto proponente: mentre l'apposizione di una firma grafometrica tramite l'utilizzo di dispositivi *tablet* è una costante, il processo all'interno del quale detta firma si inserisce deve essere distinto in base alla soluzione effettivamente adottata.

È possibile così ricondurre la firma grafometrica sotto l'alveo delle mere firme elettroniche, allorquando sia assente uno *specimen* di firma a confronto, precedentemente depositato dal

medesimo soggetto firmatario, ovvero delle firme elettroniche avanzate[1].

A seguito delle modifiche di cui al d.lgs. 26 agosto 2016, n. 179, recante modifiche ed integrazioni al Codice dell'Amministrazione Digitale[2] (in seguito, CAD) per conformare l'ordinamento giuridico italiano al Regolamento europeo EIDAS[3] in materia di identificazione elettronica, il novellato art. 1-*bis* del CAD prevede che le definizioni normative delle firme elettroniche cui occorre fare riferimento sono quelle di cui all'art. 3 del citato Regolamento.

Ciò premesso, una firma grafometrica che sia connessa univocamente al firmatario, idonea a identificare il firmatario, creata mediante dati per la creazione di una firma elettronica che il firmatario può utilizzare sotto il proprio esclusivo controllo e collegata ai dati sottoscritti in modo da consentire l'identificazione di ogni successiva modifica di tali dati, è qualificata giuridicamente come firma elettronica avanzata[4].

Il processo di firma grafometrica avanzata, che dovrebbe essere unico e irreversibile, dal punto di vista tecnico consiste nella creazione di un algoritmo di *HASH* integrato al documento informatico sottoscritto, che confronta automaticamente la firma apposta con la firma grafometrica depositata in precedenza (*matching* con lo *specimen*) dal medesimo soggetto.

La firma grafometrica avanzata è una firma biometrica: tipicamente, durante il predetto processo, vengono raccolti e registrati dati biometrici del firmatario quali, a titolo esemplificativo, la velocità di scrittura, la pressione esercitata nell'apposizione, l'angolo di inclinazione della penna, l'accelerazione del movimento e il numero delle volte che la penna viene sollevata dal *device* utilizzato.

Alla fase di raccolta di tali informazioni, segue la creazione del *template* biometrico e l'invio dei dati al *biometric server* per l'immediata conversione attraverso l'algoritmo sopra citato, integrato al documento informatico in una sequenza di caratteri tendenzialmente immodificabile e irreversibile.

1 F. Buffa, *Firme elettroniche e grafometriche*, Milano, Editore Key, 2016, 47 ss.

2 D.lgs. 7 marzo 2005, n. 82.

3 Reg. UE 23 luglio 2014, n. 910.

4 Reg. UE n. 910/2014, art. 26.

Il Regolamento europeo GDPR[5] definisce in modo innovativo i dati biometrici, rientranti nelle categorie particolari di dati personali di cui all'art. 9, par. 1, ottenuti da un trattamento specifico, e corrispondenti a caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca[6].

È possibile evincere, da tale definizione, che gli elementi connotanti i dati personali raccolti tramite le firme grafometriche avanzate che rendono gli stessi biometrici ai sensi del GDPR, sono: la funzione di identificazione esclusiva dei dati raccolti attraverso la firma; la funzione di identificazione ed autenticazione svolta da detti dati (si pensi, tra gli altri, ai rapporti bancari ed assicurativi); l'estrapolazione dei dati personali da caratteristiche fisiche, fisiologiche o comportamentali di una persona.

2. Gli obblighi a carico dei soggetti proponenti le soluzioni di firma biometrica a confronto con il GDPR[7]

Il Garante per la protezione dei dati personali (in seguito, Garante), con provvedimento prescrittivo generale n. 513 del 12 novembre 2014, aveva individuato alcune tipologie di trattamento di dati biometrici che, qualora poste in essere nel rispetto delle misure e limitazioni ivi stabilite, non necessitavano più della verifica preliminare *ex* art. 17, Codice della Privacy[8], prima di procedere al trattamento.

[5] Reg. UE 27 aprile 2016, n. 679.

[6] Reg. UE n. 679/2016, art. 4, n. 14.

[7] Il decreto legislativo 10 agosto 2018, n. 101, recante disposizioni per l'adeguamento della normativa nazionale al GDPR, in attuazione di quanto ivi previsto all'art. 9, par. 4 («Gli Stati membri possono mantenere o introdurre ulteriori condizioni, comprese limitazioni, con riguardo al trattamento [...] di dati biometrici»), inserisce, all'interno del d.lgs. n. 196/2003, l'art. 2-*septies* il quale stabilisce che il Garante per la protezione dei dati personali dovrà adottare un provvedimento, con cadenza almeno biennale, al fine di disporre misure di garanzia ulteriori adeguate a protezione, in particolare, dei dati biometrici. Si evidenzia soprattutto quanto precisato dal comma V° dell'art. 2-*septies*, laddove dette misure di garanzie possono individuare ulteriori condizioni sulla base delle quali il trattamento dei dati, nello specifico biometrici, è consentito: tale norma permetterebbe di argomentare in favore della permanenza, *post* GDPR, delle autorizzazioni generali del Garante.

[8] D.lgs. 30 giugno 2003, n. 196.

Le operazioni su dati biometrici costituiti da informazioni dinamiche associate all'apposizione a mano libera di una firma autografa avvalendosi di specifici dispositivi *hardware*, erano incluse tra detti trattamenti autorizzati ed esonerati dalla richiesta di verifica preliminare, a condizione, in particolare, che si utilizzassero esclusivamente sistemi di firma grafometrica posti a base di una soluzione di firma elettronica avanzata, e sempre che non si prevedesse la conservazione centralizzata di dati biometrici.

Da una lettura combinata del provvedimento del Garante e delle disposizioni del GDPR applicabili in materia, le prescrizioni anzidette risultano rivisitate ed aggiornate nei termini che seguono.

Per quanto concerne l'utilizzo di tecniche crittografiche, per cui i dati biometrici vengono memorizzati all'interno del documento informatico in forma cifrata tramite sistemi di crittografia a chiave pubblica e certificato digitale emesso da un certificatore accreditato *ex* art. 29, CAD, il collegamento con il contenuto dell'art. 32 GDPR, laddove prevede la cifratura dei dati personali tra le misure tecniche ed organizzative adottabili per garantire un livello di sicurezza adeguato al rischio per i diritti e le libertà delle persone fisiche, risulta di tutta evidenza.

Anche la protezione dei sistemi informatici utilizzati, sia a livello di *hardware* che *software*, contro l'azione di *malware*, e l'adozione di sistemi di *firewall* contro i tentativi di accesso abusivo ai dati biometrici trattati, sono misure tecniche di sicurezza dei dati da ricomprendersi nell'analisi dei rischi *ex* art. 32 GDPR, a prevenzione dei pericoli derivanti dalla «divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati»

L'informativa sul trattamento dei dati biometrici – aggiornata ai sensi dell'art. 13 GDPR –, oltre all'informativa sull'utilizzo della firma biometrica sottoscritta dal firmatario prima dell'attivazione del servizio[9], e la raccolta del consenso espresso dall'interessato all'atto di adesione al sistema di firma biometrica – *esplicito ex* art. 9, par. 2, lett. a) e revocabile – permangono, a monte, quali presupposti di legittimità delle operazioni effettuate su detti dati.

I precetti e le limitazioni del Garante sulla conservazione dei dati biometrici grafometrici negli strumenti utilizzati per la raccolta e

[9] D.p.c.m. 22 febbraio 2013, art. 57.

memorizzazione all'interno dei documenti informatici sottoscritti in forma cifrata, concernono inoltre i tempi, ossia conservazione per il tempo strettamente necessario a realizzare le finalità del sistema biometrico, e le modalità, con conservazione disgiunta dei dati biometrici dai dati identificativi degli interessati.

Tale ultimo assunto non può che essere ricondotto a quella misura tecnica di protezione dei dati, introdotta esplicitamente dal GDPR, della pseudonimizzazione, quale trattamento di dati personali tale per cui le informazioni aggiuntive per l'attribuzione dei dati biometrici a un interessato specifico vengono conservate separatamente.

Un particolare adempimento di *compliance* di tipo documentale avviato dal GDPR, sussistente in capo alle realtà adottanti sistemi di firma biometrica, si esplica nella tenuta di un registro, in forma scritta, che illustri i trattamenti effettuati per macrotipologie, tra i quali quello dei dati biometrici raccolti e registrati, ed il ciclo di vita di tali dati, in formato "mappatura".

Il soggetto proponente la soluzione di firma biometrica, nella sua qualità di Titolare del trattamento, deve invero descrivere «le categorie di destinatari a cui i dati sono stati o saranno comunicati» (art. 30, GDPR), nominati anche Responsabili del trattamento (si pensi ai soggetti terzi fiduciari coinvolti nel processo di firma grafometrica avanzata, che conservano le chiavi private di accesso ai dati biometrici).

Nel caso di specie, l'obbligatorietà della redazione ed aggiornamento nel tempo del registro delle attività di trattamento per le realtà aziendali che erogano sistemi di firma biometrica si ricava dal comma 5 dell'art. 30, GDPR: al di là del numero dei dipendenti, le società offerenti una firma biometrica rientrano *in toto* nella platea dei Titolari di trattamenti di categorie particolari di dati personali, occasionali o meno.

Infine, giova rammentare che, oltre all'introduzione dell'obbligo di notifica della violazione dei dati personali (*data breach*) all'autorità di controllo[10], il Titolare del trattamento deve anche comunicare tale violazione all'interessato quando essa possa potenzialmente «presentare un rischio elevato per i diritti e le libertà delle persone fisiche»[11].

[10] Reg. UE n. 679/2016, art. 33.

[11] Reg. UE n. 679/2016, art. 34.

È indubbio che da una gestione illecita o inaccorta dei dati biometrici raccolti da firme grafometriche, nei vari settori ove dette soluzioni di firma sono state concretamente implementate, possono derivare pregiudizi alla riservatezza e qualsiasi altro danno economico o sociale significativo, al di là della perdita del controllo dei dati personali, del furto o usurpazione d'identità, delle perdite finanziarie, e della decifratura non autorizzata della pseudonimizzazione, quali conseguenze di una violazione informatica[12].

Tuttavia, ai sensi dell'art. 34, par. 3, GDPR, la comunicazione all'interessato non è richiesta in particolare allorquando il Titolare del trattamento abbia adottato le misure tecniche e organizzative di sicurezza ritenute adeguate a protezione dei dati trattati, e che al momento della violazione tali misure erano state applicate: il riferimento espresso alla cifratura quale misura tecnica volta a rendere oscuri ai soggetti non autorizzati all'accesso i dati trattati, consentirebbe di escludere, nel caso di trattamenti di dati biometrici raccolti tramite firme grafometriche, tale ulteriore adempimento.

Infatti, il processo di firma biometrica, anche in base alle prescrizioni del Garante, comprende l'impiego di tecniche crittografiche da una parte, e la cifratura dei dati identificativi con conservazione separata degli stessi rispetto ai dati biometrici (pseudonimizzazione) dall'altra, di tal che la comunicazione all'interessato risulterebbe pleonastica, naturalmente a patto che, all'avverarsi della *data breach*, dette misure di sicurezza siano state correttamente applicate dal Titolare del trattamento.

Le Linee Guida del Gruppo di lavoro ex art. 29 (WP29), Direttiva CE 95/46, in materia di notifica delle *data breach*[13], specificano che le misure tecniche a protezione dei dati la cui presenza esonererebbe il Titolare dall'obbligo della comunicazione anzidetta, includono ad esempio «...*state-of-the-art encryption*, *or by tokenization*»: il Titolare del trattamento dei dati biometrici dovrebbe pertanto monitorare costantemente lo stato di avanzamento delle tecnologie, e proteggere i dati in una prospettiva dinamica ed evolutiva.

[12] Reg. UE n. 679/2016, considerando 85.

[13] WP29, *Guidelines on Personal data breach notification under Regulation 2016/679*, 6 febbraio 2018.

Qualora il Titolare del trattamento decida di non dover procedere alla comunicazione all'interessato di una *data breach* avente ad oggetto dati raccolti tramite firme biometriche, le citate Linee Guida insistono sulla capacità del medesimo di dimostrare la legittimità delle determinazioni assunte, nel rispetto del principio di *accountability* che permea complessivamente l'intero modello organizzativo sulla *Data Protection* inaugurato dal Regolamento.

Allo stato attuale occorre dunque considerare, con riguardo al trattamento dei dati biometrici nella materia *de qua*: che la verifica preliminare *ex* art. 17 del Codice della Privacy[14] e la notificazione *ex* art. 37 del medesimo Codice al Garante, da effettuarsi da parte del Titolare prima di procedere al trattamento dei dati biometrici, non sono istituti contemplati nel GDPR; il dato biometrico è diventato, secondo il linguaggio adottato dal Codice della Privacy, un dato "sensibile" a tutti gli effetti, rientrante in quelle rinnovate categorie particolari di dati personali di cui all'art. 9, GDPR; cambia completamente l'approccio alla *cybersecurity*.

3. Uso di nuove tecnologie nelle firme biometriche: legge di bilancio 2018[15] e spunti di riflessione

La legge di bilancio 2018, al comma 1022 dell'art. 1, prevede, qualora il Titolare effettui un trattamento di dati personali fondato sull'interesse legittimo comportante l'uso di nuove tecnologie o di strumenti automatizzati, che venga data tempestiva comunicazione al Garante, attraverso l'invio di un'informativa descrittiva dell'oggetto, delle finalità e del contesto del trattamento considerato, prima di procedere al medesimo.

Una volta inviata l'informativa al Garante, e trascorsi quindici giorni lavorativi dall'inoltro, alla mancanza di riscontro da parte dell'Autorità consegue un nullaosta implicito all'esecuzione del trattamento.

Tale meccanismo di silenzio-assenso contrasta *ictu oculi* con l'obbligo, in capo al Titolare del trattamento e prima di procedervi,

[14] D.lgs. 196/2003, art. 17.

[15] L. 27 dicembre 2017, n. 205.

di effettuazione di una *Data Protection Impact Assessment* (Valutazione d'impatto sulla protezione dei dati, in seguito DPIA) *ex* art. 35 GDPR laddove il trattamento possa «presentare un rischio elevato per i diritti e le libertà delle persone fisiche» e allorché preveda «in particolare l'uso di nuove tecnologie».

Uno specifico trattamento di dati biometrici, basato sull'utilizzo di strumenti di firma grafometrica implicanti l'uso di nuove tecnologie, rientrerebbe nella casistica descritta nel suddetto articolo circa l'obbligatorietà di attuazione di una DPIA.

Posta dunque la correlazione tra strumenti del trattamento dalla portata tecnologica innovativa e il derivante criterio generale di svolgimento della DPIA[16], a prescindere dai mezzi con cui i trattamenti vengono effettuati, in ogni caso, se il trattamento dei dati biometrici raccolti tramite il sistema di firma grafometrica è effettuato su larga scala, poiché tali dati sono ricompresi in quelle categorie particolari di cui all'art. 9, par. 1, GDPR, l'adempimento della DPIA permane.

Il contrasto normativo sussiste altresì con riguardo all'obbligo, eventuale e successivo alla DPIA, in capo al Titolare del trattamento, sempre *ex ante*, di consultare il Garante qualora all'esito della DPIA risulti che il trattamento presenterebbe un rischio elevato e vi sia l'impossibilità oggettiva di attenuazione del rischio tramite adozione di misure di sicurezza adeguate, per mancanza di una tecnologia disponibile o per gli elevati costi di attuazione[17] (art. 36 GDPR).

Ricevuta la richiesta di parere, è stabilito che l'autorità di controllo fornisca, entro otto settimane dal ricevimento, un parere scritto al Titolare ove ritenga che il trattamento presenti il suddetto rischio elevato; ed il considerando 94 del GDPR prevede espressamente che la mancanza di reazione dell'autorità di controllo entro il termine anzidetto, «dovrebbe far salvo ogni intervento della stessa nell'ambito dei suoi compiti e pareri previsti dal presente regolamento, compreso il potere di vietare i trattamenti».

Risulta visibilmente un vero e proprio conflitto tra norme, che si risolve, come noto, nella prevalenza del Regolamento a discapito

[16] L. Bolognini-E. Pelino-C. Bistolfi, *Il Regolamento Privacy europeo*, Varese, Giuffrè, 2016.

[17] Reg. UE n. 679/2016, considerando 94.

della legislazione nazionale: pertanto, un Titolare del trattamento di dati biometrici nell'ambito di un sistema di firma grafometrica che comprenda l'utilizzo di tecnologie all'avanguardia dovrebbe, in prima battuta, effettuare una DPIA; se, a esito della stessa, il Titolare è del parere che il rischio elevato per i diritti e le libertà delle persone fisiche non possa essere ragionevolmente attenuato con i mezzi in sua disponibilità, allora procederà alla consultazione, *ex ante* rispetto all'esecuzione del trattamento, del Garante.

Nel caso in cui il Garante non renda un parere nel termine previsto, non vi è margine di concessione di un silenzio-assenso: l'autorità di controllo mantiene integro il proprio potere inibitorio sul trattamento considerato.

4. Conclusioni

Il GDPR, nell'estendere il raggio di azione delle disposizioni del Codice della Privacy per i trattamenti di dati personali che presentano rischi specifici per i diritti e le libertà fondamentali degli interessati, conferisce una nuova dignità ai dati biometrici in modo tale che, nella logica della prevenzione di qualsivoglia evento accidentale o illecito, compromettente la sicurezza dei dati biometrici trattati dai vari soggetti che hanno implementato la firma grafometrica quale modalità di sottoscrizione di un documento alternativa a quella cartacea, che si possa in ipotesi verificare, gli adempimenti richiesti dalla normativa europea a protezione di detti dati si sono resi ancor più stringenti.

In effetti, con particolare riguardo ai trattamenti di dati biometrici raccolti attraverso una firma grafometrica che comporti l'uso di nuove tecnologie, la mancata predisposizione delle misure di prevenzione e sicurezza adeguate, rilevanti per la *cybersecurity*, i rischi elevati per i diritti e le libertà degli interessati sottesi alla falsificazione o clonazione della sottoscrizione elettronicamente apposta sono latenti.

È proprio grazie alla realizzazione, ad opera del GDPR, di un sistema di protezione dei dati personali, ancor più se particolari, strutturato già prima che i dati vengano raccolti, che le operazioni compiute sui medesimi e la corrispondente circolazione si prestano ad una messa all'opera più proficua.

Per tali motivi, il Regolamento Generale sulla protezione dei dati, con riguardo alle categorie particolari di dati personali tra cui i dati biometrici, si preoccupa di creare un quadro uniforme di cautele procedurali, che trova la sua naturale collocazione nella valutazione d'impatto sulla protezione dei dati (DPIA), nella consultazione preventiva in via eventuale, e nella tenuta del registro delle attività di trattamento.

Non di meno, il Titolare del trattamento considerato deve mettere in atto una procedura di valutazione regolare volta ad analizzare costantemente l'efficacia e l'adeguatezza delle misure di sicurezza, con particolare riguardo alle specifiche informatiche, anche attraverso *audit* periodici con la debita collaborazione del personale autorizzato e dei Responsabili, interni ed esterni all'organizzazione del Titolare, del trattamento dei dati biometrici appositamente nominati: l'invio sistematico di report circa lo stato di conservazione delle chiavi private, di cui al sistema di crittografia dei modelli biometrici concretamente applicato, da parte del soggetto terzo fiduciario detentore esclusivo delle medesime potrebbe rappresentare in tal senso una *best practice*.

Sulla base delle nominate procedure, ai soggetti offerenti soluzioni di firma grafometrica avanzata, una volta ottemperati i vari obblighi previsti a baluardo del diritto fondamentale alla protezione del dato, è consentito procedere alle operazioni di trattamento sul dato biometrico, quale esemplare di dato particolare la cui utilità è decisamente fruttuosa.

Processo mediatico e diritto all'oblio. Il possibile gioco di sponda tra UE e CEDU

Edoardo Mazzanti

Sommario: 1. L'oblio nella dialettica tra processo penale e mass media – 2. I diritti della "vittima mediatica" – 3. La tutela multilivello – 4. Le declinazioni dell'oblio nel sistema CEDU e la possibile influenza della legislazione UE – 5. Il futuro del "diritto umano all'oblio"

1. L'oblio nella dialettica tra processo penale e mass media

Storicamente connesso all'istituto della prescrizione quale delimitazione temporale del potere punitivo[1], il tema dell'oblio – o, più in generale, del decorso *qualificato* del tempo – erompe, oggi, anche in altri àmbiti del dibattito penalistico; fra di essi, spicca senz'altro l'interazione tra sistema penale, internet e nuovi mezzi di comunicazione[2]. Va premesso che il rapporto tra processo penale e mass

[1] Sul riconoscimento espresso del diritto all'oblio quale fondamento della prescrizione, nella giurisprudenza costituzionale, Corte cost. sent. n. 23/2013; Corte cost. sent. n. 143/2014.

[2] In proposito, si è detto che il tema dell'oblio in rete, oltre a coinvolgere questioni attinenti ai profili di responsabilità del fornitore di un servizio nella società dell'informazione, tocca anche i «profili distopici che talvolta si vogliono attribuire a Internet, proprio quale "*wild web*"' della globalizzazione del crimine, portato a estremi apocalittici» (R. Flor, *La giustizia penale nella rete? Tutela della riservatezza* versus *interesse all'accertamento e alla prevenzione dei reati nella recente giurisprudenza della Corte di Giustizia dell'Unione Europea*, in R. Flor-D. Falcinelli-S.

media può essere osservato in due diverse chiavi: approfondendo le ripercussioni della cronaca giudiziaria sulle vicende processuali (c.d. informazione sul processo), per un verso; analizzando il modo in cui gli stessi *media* "si fanno aula giudiziaria" (c.d. processo mediatico), per l'altro. Ai fini del presente lavoro, conviene concentrarci sul secondo aspetto.

L'inarrestabile ascesa dei nuovi mezzi di comunicazione di massa ha intensificato la dialettica tra processo penale e c.d. processo mediatico[3]: sebbene «entrambi esplicativi della (di una) realtà sociale»[4], i due sistemi presentano, in effetti, divergenze quantitative, qualitative, contenutistiche e, non per ultimo, modali. Decisiva, in quest'ultimo senso, la loro diversa relazione col tempo: alla diacronia del processo, è stato fatto notare, si contrappone la sincronia dei *media*; nel c.d. processo mediatico, in altre parole, il momento di reale afflittività si consuma pressoché istantaneamente, di solito all'inizio – e soltanto all'inizio – del procedimento vero e proprio.

Questa tensione si fa drammaticamente elevata quando il canale mediatico di riferimento è internet, il cui avvento ha mutato il ruolo giocato dal fattore temporale nell'economia dell'oblio: non più riferimento al solo tempo trascorso tra due eventi puntuali – una notizia e la sua ripubblicazione – ma anche – verrebbe da dire: soprattutto – alla *permanenza* di una determinata informazione[5].

Marcolini (a cura di), *La giustizia penale 'nella rete'. Le nuove sfide della società dell'informazione nell'epoca di Internet*, DipLaP, 2015, 154).

[3] Nella ricca letteratura, M. Bertolino, *Privato e pubblico nella rappresentazione mediatica del reato*, in *Riv. dir. pen. proc.*, 2003, 4, 1070; Ead., *Giustizia narrata o giustizia tradita?*, in G. Forti-C. Mazzucato-A. Visconti (a cura di), *Giustizia e letteratura*, vol. I, Milano, Vita e pensiero, 2012, 610; G. Giostra, *Processo penale e mass media*, in *Criminalia*, 2007, 57; F. Palazzo, *Mezzi di comunicazione e giustizia penale*, in *Pol. dir.*, 2009, 2, 193; C.E. Paliero, *La maschera e il volto (percezione sociale del crimine ed 'effetti penali' dei media)*, in *Riv. dir. pen. proc.*, 2006, 2, 467; T. Padovani, *Informazione e giustizia penale: dolenti note*, in *Dir. pen. proc.*, 2008, 6, 689.

[4] C.E. Paliero, *La maschera e il volto*, cit., 469.

[5] G. Finocchiaro, *Il diritto all'oblio nel quadro dei diritti della personalità*, in *Dir. inf.*, 2014, 4/5, 591; più di recente, R. Pardolesi, *L'ombra del tempo e (il diritto al) l'oblio*, in *Quest. giust.*, 2017, 1, 85, che sottolinea come la diffusione di informazioni, nell'era di internet, «sia contraddistinta da una latenza passiva che però dilata la sfera della disponibilità virtuale».

Calata nella realtà della cronaca giudiziaria[6], questa svolta ha un impatto decisivo: la straordinaria capacità di conservazione della rete, in effetti, fa sì che le *notitiæ* (non necessariamente *criminis*) non soltanto permangano, ma permangano, come opportunamente precisato, «solo nelle premesse»[7], senza che agli eventuali successivi sviluppi (archiviazione, assoluzione, dissequestro ecc.) sia spesso dato adeguato peso. La memoria di internet[8], insomma, presenta un'accentuata "resistenza selettiva", in grado di cristallizzare le (sole) fasi iniziali di una determinata vicenda penale, con conseguente distorsione del quadro complessivo e, in ultimo, dell'immagine dei soggetti coinvolti.

2. I diritti della "vittima mediatica"

La mediatizzazione giudiziaria aggiunge una pena *pubblica* – intesa come "di pubblico" – alla pena del processo, relegando definitivamente nell'ombra le dinamiche della pena vera e propria[9]. Questa «catabasi mediatica», è stato acutamente scritto, modella la sagoma d'una nuova vittima: la vittima, per l'appunto, *mediatica*[10]. In

[6] In proposito, con particolare attenzione alle distorsioni tipiche delle grandi inchieste, V. Pezzella, *La diffamazione*, Torino, Utet, 2016, 679 ss; in prospettiva difensiva, *L'informazione giudiziaria in Italia. Libro bianco sul rapporto tra mezzi di comunicazione e processo penale*, a cura dell'Osservatorio sull'informazione giudiziaria dell'Unione Camere Penali Italiane, Pisa, Pacini, 2016, part. 85 ss.

[7] A. Marandola, *La tutela dell'identità personale (informatica), anche del soggetto coinvolto in un processo penale*, in *Proc. pen. giust.*, 2017, 3, 373.

[8] Descritta come «immensa, universale, densa, disorganizzata, volatile e persistente», S. Martinelli, *Diritto all'oblio e motori di ricerca: il bilanciamento tra memoria e oblio in internet e le problematiche poste dalla de-indicizzazione*, in *Dir. inf.*, 2017, 3, 566.

[9] Sul progressivo spostamento dell'attenzione dalla pena *stricto sensu* alla «pena "pubblica"» amplificata dai *media*, F. Palazzo, *Mezzi di comunicazione e giustizia penale*, cit., 205 s.

[10] V. Manes, *La 'vittima' del 'processo mediatico': misure di carattere rimediale*, in *Dir. pen. cont. - Riv. trim*, 2017, 3, 117; secondo R. Aprati, *Riflessioni intorno alla 'vittima del processo'*, in *Cass. pen.*, 2017, 3, 980, l'esposizione mediatica rientrerebbe fra i pregiudizi *eventuali* della c.d. vittima da processo penale.

sostanza, colui che nel processo penale riveste il ruolo di indagato/imputato, per eterogenesi dei ruoli, nel c.d. processo mediatico diventa egli stesso vittima, titolare di "nuovi" diritti che la resistenza selettiva di internet finisce per mettere a dura prova.

Fra le prerogative che la c.d. vittima mediatica rischia di vedere sacrificate, figurano, in particolare, sia i diritti globalmente connessi alla personalità individuale (art. 2 Cost.), sia, trattandosi di possibili coinvolgimenti criminali, la presunzione di non colpevolezza (art. 27 co. 2 Cost.): nella sua accezione di "regola di trattamento", difatti, quest'ultima assume «una valenza anche "extra-processuale", quale fondamentale criterio di orientamento culturale»[11], che conferisce all'interessato il diritto a non essere illegittimamente *mostrato* come colpevole[12]. Intesa in questo senso, peraltro, si ritiene che la presunzione d'innocenza tenda ad avvicinarsi molto alla reputazione[13]; per tale via, viene a delinearsi un più ampio "diritto all'identità personale mediatica", che mira a «mantenere il rapporto tra la persona e il suo "corpo digitale"»[14] e inspessisce quel fitto groviglio di valori facenti globalmente capo al concetto di "dignità"[15].

Questo macro-diritto, sul piano temporale, opera in due direzioni: in chiave *ex-ante*, tutelando l'individuo dalla prematura diffusione di notizie colpevoliste; in chiave *ex-post*, imponendo l'aggiornamento e inibendo la riproposizione di notizie superate da nuovi fatti procedimentali (ad esempio, un'archiviazione). Al cospetto delle istanze tipiche del c.d. processo mediatico, dunque, a venire in gioco non sono tanto l'oblio o la riservatezza nei loro significati tradizionali, quanto la completezza e la corretta collocazione stori-

[11] P.P. Paulesu, voce *Presunzione di non colpevolezza*, in *Dig. disc. pen.*, Torino, 1995, 678.

[12] Per un primo riconoscimento, Corte cost., sent. n. 18/1966.

[13] F. Palazzo, *Note sintetiche sul rapporto tra giustizia penale e informazione giudiziaria*, in *Dir. pen. cont. - Riv. trim.*, 2017, 3, 145.

[14] S. Martinelli, *Diritto all'oblio e motori di ricerca*, cit., 568.

[15] Sulla *dignità* intesa come «qualificazione normativa dell'essere umano», da adoperare – con cautela e in prospettiva complementare – come contro-interesse della libertà di manifestazione del pensiero, F. Bacco, *Dalla dignità all'eguale rispetto: libertà di espressione e limiti penalistici*, in *Quad. cost.*, 2013, 4, 823, e bibliografia ivi contenuta.

ca di un determinato episodio[16]; note, quest'ultime, espressive del diritto di ciascuno a non subire i danni derivanti dall'indeterminata esposizione mediatica della propria posizione processuale.

Per quanto *fondamentale*[17], non si tratta, ovviamente, di diritto assoluto, dovendo esso essere contemperato con i contrapposti diritti di cronaca/critica in senso stretto – laddove il "recupero" di una notizia passata sia funzionale a corroborare una notizia attuale – ovvero di cronaca/critica storica – laddove la notizia potenzialmente lesiva sia conservata in un archivio *web*. Le indicazioni generali su come bilanciare i due poli sono state tracciate dal Working Party Article 29 (WP 29, oggi *European Data Protection Board*) sulla scorta della cruciale sentenza *Google Spain*[18]. Oltre a delineare una griglia di criteri cui le autorità nazionali per la protezione dei dati personali debbono ispirarsi nell'opera di bilanciamento[19], ai nostri fini, è utile segnalare che il WP 29: *(i)* esclude che il mero decorso temporale sia di per sé risolutivo, rilevando, piuttosto, se il dato – leggasi: la notizia – sia o meno aggiornato, e se esso sia stato reso accessibile per un tempo congruo rispetto alla finalità del trattamento (n. 7); *(ii)* in materia penale, distingue tra reati lievi risalenti e reati gravi recenti, suggerendo la de-indicizzazione del dato nel primo caso ed escludendola nel secondo (n. 13).

[16] A. Marandola, *La tutela dell'identità personale*, cit., 375; nello stesso senso, da ultimo, F. Agnino, *Il diritto all'oblio e diritto all'informazione: quali condizioni per il dialogo?*, in *Danno resp.*, 2018, 1, 105. R. Pardolesi, *L'ombra del tempo e (il diritto al) l'oblio*, cit., 76, offre una ricostruzione critica ed elegante delle "due anime" del diritto all'oblio, distinguendo tra "oblio euronitario" – fondamentalmente incentrato sulla *removal of visibility* – e "oblio domestico" – incentrato sulla rimozione forzata del dato.

[17] Sulle difficoltà a configurare il diritto all'oblio come diritto "fondamentale", E. Stradella, *Cancellazione e oblio: come la rimozione del passato, in bilico tra tutela dell'identità personale e protezione dei dati, si impone anche nella rete, quali anticorpi si possono sviluppare e, infine,* cui prodest*?*, in *Riv. AIC*, 2016, 4, 26ss.

[18] Corte GUE, *Google Spain SL e Google Inc.* c. *AEPD e Mario Costeja Gonzáles*, 13.5.2014, C-131/12.

[19] Art. 29 Data Protection Working Party, *Guidelines on the Implementation of the Court of Justice of the European Union Judgement on 'Google Spain and Inc. v. Agencia Espanola de Protección de Datos (AEPD) and Mario Costeja González' C-131/12*.

3. La tutela multilivello

La lesione del diritto come sopra ricostruito può essere fatta valere in varie sedi[20].

A livello nazionale, il tema s'inscrive nel processo di c.d. privatizzazione dei conflitti, favorendo il potenziale coinvolgimento – e la potenziale sovrapposizione – di svariate branche dell'ordinamento giuridico[21]. In dettaglio, le soluzioni spaziano dalle istanze rivolte all'Autorità Garante[22], alle azioni in sede civile[23] per arrivare alle contestazioni penali, imperniate principalmente – sebbene non esclusivamente – sul delitto di diffamazione[24].

Ai nostri fini, merita spostare lo sguardo oltralpe, per valutare se e in che misura la "vittimizzazione mediatica" possa trovare protezione ai sensi della Convenzione europea dei diritti dell'uomo (CEDU). In proposito, s'è condivisibilmente evidenziato che la teoria

[20] Per una panoramica, V. Pezzella, *La diffamazione*, cit., 883 ss.

[21] Sulle interrelazioni tra penale e civile, specie sul piano sanzionatorio, C. Piergallini, '*Civile*' *e* '*penale*' *a perenne confronto: l'appuntamento di inizio millennio*, in V. Roppo-P. Sirena (a cura di), *Il diritto civile, e gli altri*, Milano, Giuffrè, 2012, 112, part. 132 ss.

[22] In materia di de-indicizzazione di notizie relative a vecchi procedimenti penali, fra le più recenti, accolgono il ricorso Provv. n. 280 del 15.6.2017; Provv. n. 156 del 23.3.2017; dichiara il non luogo a provvedere per spontanea attivazione del sito e del motore di ricerca Provv. n. 21 del 18.1.2018; rigettano il ricorso in ragione del persistente interesse pubblico alla conoscenza dell'informazione Provv. n. 344 del 22.5.2018; Provv. n. 286 del 9.5.2018; Provv. n. 63 del 1.2.2018.

[23] Da ultimo, recepisce i criteri elaborati dalla giurisprudenza sovranazionale in punto di bilanciamento tra interessi del singolo e interessi della collettività Cass. civ. sez. I, sent. 20.3.2018 n. 6919; in precedenza, Cass. civ. sez. I, sent. 24.6.2016 n. 13161; Cass. civ. sez. I, sent. 5.4.2012 n. 5525. Nella giurisprudenza di merito, T. Milano sez. I, sent. 4.1.2017 n. 12623; T. Milano sez. I, sent. 28.9.2016 n. 10374; con specifico riferimento a pregresse vicende penali T. Mantova, sent. 28.10.2016.

[24] In linea generale, in materia di diffamazione, la Cassazione si mostra oltremodo cauta nel riconoscere prevalenza al diritto all'oblio: in materia di vecchi fatti di cronaca nera riesumati durante un *talk-show*, Cass. pen. sez. V, sent. 17.7.2009 n. 45051; *contra*, negano la sussistenza del fatto Cass. pen. sez. V, sent. 22.6.2017 n. 38747; Cass. pen. sez V, sent. 7.10.2010 n. 38096. In materia di abuso d'ufficio, ritiene che la violazione del diritto all'oblio possa rientrare nella nozione di "danno ingiusto" Cass. pen. sez. VI, sent. 7.7.2016 n. 39452.

dei cc.dd. obblighi positivi sviluppata in seno alla giurisprudenza di Strasburgo[25] implica una *corresponsabilizzazione* dello Stato per violazioni dovute alla mediatizzazione del procedimento penale[26]: a fronte di violazioni che appaiono spesso strutturali, lo Stato può essere chiamato a rispondere sia della mancata predisposizione di meccanismi che limitino l'esposizione mediatica dell'accusato, sia della mancata previsione di specifiche misure che garantiscano a quest'ultimo una qualche forma di riparazione o compensazione. In favore della rilevanza convenzionale della permanenza in rete di notizie pregiudizievoli, militano anche taluni passi della sentenza *Google Spain*, la quale, da un lato, richiama espressamente l'art. 8 CEDU (cons. 10)[27]; dall'altro, orienta la soluzione finale alla luce degli artt. 7-8 della Carta di Nizza (§§ 68s), che della disposizione CEDU costituiscono, di fatto, la versione progredita e attualizzata[28].

4. Le declinazioni dell'oblio nel sistema CEDU e la possibile influenza della legislazione UE

Sebbene la Corte di Strasburgo abbia esplicitamente riconosciuto il problema della permanenza online di contenuti diffamatori o comunque illegittimi[29], la giurisprudenza convenzionale in materia di

[25] Per un inquadramento, J.F. Akandji-Kombe, *Positive obligations under the European Convention on Human Rights*, CoE, 2007.

[26] V. Manes, *La 'vittima' del 'processo mediatico'*, cit., 118 s.

[27] Stigmatizza la ritrosia della Corte ad "affidarsi" alla giurisprudenza di Strasburgo, definendo quest'ultima, nell'economia della sentenza, «un cane che non ha abbaiato», E. Frantziou, *Further Developments in the Right to be Forgotten: the European Court of Justice's Judgment in Case C-131/12*, Google Spain SL, Google Inc. c. Agenzia Espanola de Proteçion de Datos, in *Hum. Rig. Law Rev.*, 2014, 14, 772 ss.

[28] Per una critica al ruolo eccessivo attribuito gli artt. 7-8 CDFUE, 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, 4/5, 569, il quale sottolinea, tra le altre, le differenze nei meccanismi di bilanciamento tra interessi contrapposti operati, rispettivamente, da Corte GUE e Corte EDU (577).

[29] Corte EDU (GC), *Delfi AS c. Estonia*, 16.6.2015, ric. n. 64569/09, § 110.

oblio, al momento, appare dormiente[30]. Nondimeno, considerato lo storico impegno della Corte nell'*adeguare* le norme della Convenzione alle nuove tecnologie[31], pensiamo sia possibile immaginare prossimi sviluppi in materia.

Un incentivo, in tal senso, potrebbe senz'altro arrivare dalla recente legislazione di matrice UE. Al di là del complesso dibattito sulla responsabilità statale ai sensi della CEDU per violazione di una norma UE[32], s'è recentemente evidenziato che la Corte di Strasburgo è solita richiamare il *corpus juris* eurounitario sia come parte delle premesse in fatto, sia, soprattutto, come "fonte d'ispirazione" per la soluzione delle controversie. Significativo, in quest'ultimo senso, l'uso del diritto UE – primario e secondario – per corroborare il c.d. *European consensus*, strategia tramite la quale la Corte, dando atto dell'esistenza di consenso generalizzato intorno a un determinato tema, punta, al contempo, a cementare la *ratio decidendi* e rinsaldare la propria legittimazione[33].

Resta da capire, a questo punto, in quale previsione della Convenzione meglio s'inquadrino le pretese delle c.d. vittima mediatica. Si profilano tre ipotesi.

(i) In dottrina, è stato evocato l'art. 3 CEDU[34], *sub specie*, immaginiamo, di divieto di trattamento degradante: la perdurante esposi-

[30] Un esempio è dato da Corte EDU, *Wegryznowski e Smolczewski c. Polonia*, 16.7.2013, ric. n. 33846/07; i ricorrenti si dolevano, in particolare, della decisione della Corte d'appello di Varsavia di non rimuovere le versione online di un articolo che, nella versione cartacea, la stessa Corte aveva già giudicato lesivo della loro reputazione.

[31] In dottrina, T. Murphy-G. Ó Cuinn, *Work in Progress: New Technologies and the European Court of Human Rights*, in *Hum. Rig. Law Rev.*, 2010, 10, 601. Sulla giurisprudenza EDU connessa a internet, si veda l'utile guida *Internet: case-law of the European Court of the Human Rights*, elaborata dalla Divisione Ricerca della Corte medesima (ultimo aggiornamento: luglio 2015).

[32] Il tema s'inscrive nel complesso dibattito sulla c.d. protezione equivalente tra UE e CEDU, che vede il proprio caposaldo nella decisione Corte EDU (GC), *Bosphorus Hava Yollari Turizm ve Ticaret Anonim Sirketi c. Irlanda*, 30.6.2005, ric. n. 45036/98; più di recente, Corte EDU, *Michaud c. Francia*, 6.12.2012, ric. n. 12323/11; Corte EDU (GC), *Avotinš c. Lettonia*, 23.5.2016, ric. n. 17502/07.

[33] T. Lock, *The Influence of EU Law on Strasbourg Doctrines*, in *Edinburgh School of Law Research Paper*, 2017, 3, disponibile su https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2922462, 4 s, 18 ss.

[34] Seppur di sfuggita, A. Marandola, *La tutela dell'identità personale*, cit., 375.

zione mediatica nelle vesti di colpevole, a prima vista, parrebbe poter infondere quel sentimento di «paura, angoscia e inferiorità capace di umiliare e degradare la vittima e, eventualmente, di vincere la sua resistenza fisica o psichica» indispensabile affinché un determinato trattamento rientri nell'àmbito applicativo della previsione[35].

Ci sembra una tesi difficile da sostenere. Sebbene anche l'art. 3, nel suo insieme, ruoti intorno al concetto di "dignità umana" e sebbene il trattamento degradante possa consistere, in effetti, nel solo turbamento psichico dell'interessato[36], la semplice permanenza online di una determinata notizia difetta dei tratti di *materialità* abitualmente associati al concetto di "trattamento". *A contrario*, va anzi rilevato che, nei rari casi di "gogna mediatica" in cui l'art. 3 ha trovato applicazione, la violazione è dipesa da condotte assai diverse, come la videoregistrazione degli imputati all'interno di una gabbia metallica[37]. Occorre, dunque, volgere lo sguardo altrove.

(ii) Trattandosi di vittima da processo penale, la mente corre inevitabilmente alla presunzione d'innocenza (art. 6 §2 CEDU), che, nella giurisprudenza EDU, assume ormai anche una proiezione mediatica[38]. Nello specifico, la Corte di Strasburgo ha più volte chiarito che fuoriesce dal diritto alla libertà d'espressione la diffusione di notizie che riflettano anzitempo il sentimento che un imputato sia colpevole[39]; in astratto, dunque, anche la loro memorizzazione a oltranza parrebbe poter condurre a una violazione dell'art. 6.

Merita rimarcare che la declinazione mediatica della presunzione d'innocenza è stata oggetto, fra le altre, di una Raccomandazione del Consiglio d'Europa[40] e, soprattutto, della recente Dir. (UE) 2016/343 del 9.3.2016, «sul rafforzamento di alcuni aspetti della presunzione

[35] Per tutte, Corte EDU (GC), *Jalloh c. Germania*, 11.7.2006, ric. n. 54810/00, § 68.

[36] In argomento, C. Grabenwarter, *Art. 3*, in Id., *European Convention on Human Rights*, Beck, 2014, 36 ss.

[37] Corte EDU, *Khodorkovskiy c. Russia* e *Ramishvili et al. c. Georgia*, 27.1.2009, ric. n. 1704/06, §§ 96ss.

[38] Corte EDU (GC), *Bédat c. Svizzera*, 20.3.2016, ric. n. 56925/08, §§ 68ss.

[39] Corte EDU, *Rywin c. Polonia*, 18.2.2016, ric. nn. 6091/06, 4047/07 e 4070/07, § 204.

[40] *Raccomandazione (2003) 13 del Comitato dei Ministri del Consiglio d'Europa sull'informazione attraverso i mezzi di comunicazione sui procedimenti penali*, la quale, elencando i principi che devono ispirare l'informazione giudiziaria, al punto n. 2 fissa inequivocabilmente la presunzione d'innocenza.

d'innocenza e del diritto di presenziare al processo nei procedimenti penali». Si tratta di un provvedimento di grande rilevanza che, in base a quanto accennato sopra, potrebbe spiegare i suoi effetti anche in àmbito CEDU[41]. Significativi, in particolar modo, i conss. 17-19 e l'art. 4 ("Riferimenti in pubblico alla colpevolezza"), che, nel complesso, impongono agli Stati di preservare l'immagine dell'imputato impendendo il rilascio di dichiarazioni che lo presentino prematuramente come colpevole[42].

Sennonché, ad uno sguardo più attento, il riferimento all'art. 6 CEDU, in questo specifico settore, non può non suscitare qualche perplessità: se scorriamo la giurisprudenza EDU, in effetti, notiamo che la presunzione d'innocenza, solitamente, riguarda non tanto l'attività giornalistica, quanto le dichiarazioni ufficiali di organi o agenti dello Stato[43]. L'ipotesi paradigmatica in cui viene in gioco l'art. 6 CEDU, a ben vedere, è rappresentata dalle conferenze stampa abitualmente allestite a margine di inchieste, processi e sentenze; situazioni che, pur potendo certamente ledere un diritto fondamentale dell'accusato[44], mal s'attagliano al diritto della c.d. vittima mediatica come sopra tratteggiato. La differenza è stata stigmatizzata dalla stessa Corte, la quale, in tempi recentissimi, ha ribadito che la diffusione di articoli "colpevolisti" sganciati dal processo vero e proprio non dà luogo a violazione dell'art. 6 § 2, potendo rifluire, al più, nel successivo art. 8[45].

(iii) Come precisato nella sentenza appena citata, la previsione più adatta per garantire tutela alla c.d. vittima mediatica appare

[41] F. Pizzetti, *Informazione, presunzione d'innocenza e 'verginità del giudice'. L'Italia e l'Europa*, in *L'informazione giudiziaria in Italia*, cit., 128.

[42] Sul punto, C. Valentini, *La presunzione d'innocenza nella Direttiva n. 2016/343 UE:* per aspera ad astra, in *Proc. pen. giust.*, 2016, 6, 195 ss; *contra*, ritiene che la giurisprudenza EDU vanti uno standard di tutela maggiore rispetto a quello garantito dalla direttiva, n. Canestrini, *La direttiva sul rafforzamento di alcuni aspetti della presunzione d'innocenza e del diritto di presenziare al processo nei procedimenti penali*, in *Cass. pen.*, 2016, 5, 2230 ss.

[43] R. Chenal, *Il rapporto tra processo penale e media nella giurisprudenza della Corte europea dei diritti dell'uomo*, in *Dir. pen. cont. - Riv. trim.*, 2017, 3, 39 ss.

[44] Per tutte, Corte EDU, *Allenet de Ribemont c. Francia*, 10.2.1995, ric. n. 15175/89.

[45] Corte EDU, *Seferi Ylmaz c. Turchia*, 13.2.2018, ric. nn. 61949/08, 38776/09 e 44565/09, §§ 46ss.

quella di cui all'art. 8 CEDU, nella forma di diritto al rispetto della vita privata: portata ampia, formulazione flessibile e natura non assoluta, in effetti, negli anni hanno favorito il suo progressivo sviluppo secondo un modello "ad albero"[46], rendendolo, per quel che qui interessa, il raccordo privilegiato tra Convenzione e nuove tecnologie[47]. La disposizione, per giurisprudenza costante, mira ad assicurare lo sviluppo della personalità di ciascun individuo nelle relazioni con gli altri, impedendo indebite interferenze esterne[48] sia pubbliche che private; essa, fra le altre, offre tutela contro la pubblicazione di qualunque informazione personale che il titolare possa legittimamente aspettarsi non venga diffusa senza consenso o, comunque, senza oggettiva necessità[49]. In virtù della tipica interpretazione evolutiva della Corte, ci pare che anche la permanenza in rete di notizie non aggiornate relative ad una posizione processuale "scomoda" possa rientrare in tale spettro di tutela, previo bilanciamento, naturalmente, con il contrapposto diritto *collettivo* all'informazione[50].

[46] Nel senso che ciascun "ramo" – *i.e.*: diritto – ha favorito la crescita di altri "rami" (M. Burbergs, *How the Right to Respect for Private and Family Life, Home and Correspondence Became the Nursery in Which New Rights Are Born*, in E. Brems-J. Gerards (a cura di), *Shaping Rights in the ECHR. The Role of the European Court of Human Rights in Determining the Scope of Human Rights*, Cambridge, Cambridge University Press, 2014, 315, part. 325 ss).

[47] T. Murphy-G. Ó Cuinn, *Work in Progress*, cit., 617 ss. Utile, al riguardo, la recente *Guide on Article 8 of the European Convention of the Human Rights*, CoE, 2017, ove si sottolinea che «l'approccio generoso nella definizione degli interessi personali ha consentito alla giurisprudenza di svilupparsi in linea coi cambiamenti sociali e tecnologici» (16).

[48] Per pacifica acquisizione, l'art. 8 CEDU assume medesima portata sia se interpretato come divieto d'interferenza, sia se analizzato nel suo ruolo di fonte di obblighi positivi. Di recente, Corte EDU (GC), *Hämäläninen c. Finlandia*, 16.7.2014, ric. n. 3735/09, § 65.

[49] Corte EDU (GC), *Axel Springer AG c. Germania*, 7.2.2012, ric. n. 39954/08, § 83.

[50] La Corte ha a più riprese chiarito che i princìpi elaborati per dirimere il contrasto tra diritto al rispetto della vita privata e diritto alla libertà d'espressione meritano eguale ponderazione, a prescindere che il ricorrente invochi la violazione, rispettivamente, dell'art. 8 ovvero dell'art. 10 CEDU. I criteri-guida sono frutto di giurisprudenza ormai stratificata (Corte EDU (GC), *Von Hannover c. Germania (2)*, 7.2.2012, ric. nn. 40660/08 e 60641/08, §§ 108ss; Corte EDU (GC), *Axel Springer AG*, cit., §§ 89ss; Corte EDU (GC), *Couderc e Hachette Filippachi Associés c. Francia*, 10.11.2015, ric. n. 40454/07, §§ 90ss) e riguardano, fra le altre:

A conferma della compatibilità fra diritto all'oblio in senso lato e art. 8 CEDU, si segnala un caso deciso nel 2017, instaurato su ricorso di un soggetto che si doleva della mancata rimozione dal sito del *New York Times* di un articolo nel quale si adombravano suoi passati legami con organizzazioni criminali[51]. Se, in concreto, la Corte nega la violazione, ritenendo che il tribunale domestico avesse correttamente bilanciato l'interesse del ricorrente con l'interesse della collettività (§§ 35ss) e che non sussistessero «forti ragioni» tali da sovvertire il giudizio (§§ 54s); essa, in astratto, ritiene che la permanenza online di notizie circa passati ipotetici coinvolgimenti criminali – mai sfociati, peraltro, in alcuna condanna – costituisca «un'allegazione sufficientemente grave affinché l'art. 8 possa essere invocato» (§ 30). L'esito negativo del ricorso, in altre parole, sembra dipendere da circostanze fattuali specifiche[52], non certo da una generale inconciliabilità tra oblio e sistema CEDU[53].

(i) il contributo a un dibattito di pubblico interesse e la notorietà della persona coinvolta; *(ii)* la precedente condotta del soggetto; *(iii)* il modo in cui chi diffonde la notizia è venuto in possesso delle informazioni; *(iv)* il contenuto, la forma e la conseguenze della pubblicazione; *(v)* le circostanze in cui la notizia è stata diffusa.

[51] Corte EDU, *Fuchsmann c. Germania*, 19.10.2017, ric. n. 71233/13, su cui S. Bonavita-R. Pardolesi, *La Corte Edu contro il diritto all'oblio?*, in *Danno resp.*, 2018, 2, 149; nonché, volendo, E. Mazzanti, *Vecchio sospetto di reato e diritto all'oblio. A proposito di una recente sentenza della Corte di Strasburgo*, in *Dir. pen. cont.*, 18.4.2018.

[52] I giudici di Strasburgo, fra le altre, sottolineano la mancata richiesta di de-indicizzazione: «considerato che il ricorrente recriminava che l'articolo fosse raggiungibile semplicemente cercando il suo nome in rete», si legge, «la Corte nota che egli non ha fornito alcuna informazione relativa a eventuali tentativi volti a far rimuovere suddetto articolo dai motori di ricerca» (§ 53). Per tale via, la Corte sembra dunque ravvisare nella mancata richiesta di *de-listing* una sorta di atecnico mancato esaurimento delle vie di ricorso interne.

[53] Analogamente, Corte EDU, *Wegryznowski e Smolczewski*, cit., §§ 53ss, che ha parimenti negato la violazione concreta dell'art. 8, salvo decretarne l'astratta applicabilità, specialmente per quanto riguarda la conservazione di materiale online (§ 58). In senso diverso, accoglie con minor entusiasmo il legame tra art. 8 CEDU e diffusione di informazioni commerciali G. Carraro, *Pubblicità commerciale e 'diritto all'oblio' nella prospettiva dei diritti dell'uomo*, in *Nuova giur. civ. comm.*, 2016, 4, 634.

Un apporto significativo *anche* per la giurisprudenza EDU potrebbe arrivare, oggi, dal Regolamento (UE) 679/2016 del 27.4.2016 (c.d. GPDR), che, come noto, all'articolo 17 ha codificato il «diritto alla cancellazione ("diritto all'oblio")». Si potrebbe controbattere che i limiti di tale previsione, approfonditamente scandagliati già prima dell'entrata in vigore del GDPR[54], si riverberino anche sul sistema CEDU: l'equiparazione alla cancellazione, in particolare, parrebbe ridurre l'area applicativa guadagnata negli anni dal "diritto all'oblio", pregiudicando la sua funzione di presidio dell'identità c.d. dinamica dell'interessato[55]. Pur non volendo ridimensionare le falle della nuova disposizione, crediamo che esse, ai nostri limitati fini, siano in qualche misura superabili: nella nostra prospettiva, rileva semplicemente il formale riconoscimento, in seno al contesto europeo, di un'ampia schiera di diritti *globalmente* riconducibili alla tutela dell'identità digitale[56], da leggere, tra l'altro, alla luce del criterio di esattezza/aggiornamento dei dati (art. 5 §1 lett. d GPDR).

5. Il futuro del "diritto umano all'oblio"

Concludendo, si potrebbe dire che la Corte di Strasburgo, al momento, tenga fuori il diritto all'oblio lasciando, tuttavia, la porta socchiusa.

La CEDU continua ad apparire strumento idoneo ad assecondare le istanze di tutela della c.d. vittima mediatica: considerata la relativa novità del tema e la specificità dei pochi casi trattati, crediamo resti intatta la possibilità che, in futuro, uno Stato sia chiamato a rispondere per non aver garantito la massima "neutralizzazione" delle informazioni originariamente colpevoliste,

[54] Per una sintesi, F. Agnino, *Il diritto all'oblio e diritto all'informazione*, cit., 109. Sul significato assunto dal "nuovo" oblio, si veda anche il contributo di G. Rugani contenuto in questo Volume.

[55] F. Di Ciommo, *Il diritto all'oblio (oblito) nel Regolamento UE 2016/679 sul trattamento dei dati personali*, in *Foro it.*, 2017, V, 306.

[56] Non soltanto il diritto alla cancellazione/oblio, ma anche il "diritto di rettifica" (art. 16), il "diritto di limitazione di trattamento" (art. 18) e il "diritto di opposizione" (art. 21).

obbligando chi le ha pubblicate a rimuoverle[57], oscurarle o, quantomeno, rettificarle[58].

Al riguardo, si consideri ancora il caso da ultimo citato. Nell'esaminare il parametro del «contributo ad un dibattito di interesse pubblico», la Corte ha modo di trattare, seppur fugacemente, anche i profili di natura temporale. In tale sede, tuttavia, emerge (se non una contraddizione, quantomeno) una sovrapposizione: da una parte, si afferma che la pubblicazione della notizia dei remoti (e comunque mai definitivamente accertati) coinvolgimenti criminali del ricorrente «fosse divenuta nuovamente rilevante in considerazione dei sospetti di corruzione in capo al candidato sindaco di New York»; dall'altra, si identificano gli archivi online come «un'importante fonte per l'educazione e la ricerca storica, soprattutto perché prontamente accessibili al pubblico e generalmente gratuiti»[59]. L'impressione è che la Corte, nel giustificare la sussistenza dell'interesse pubblico al mantenimento della notizia, saldi due piani temporali distinti, così confondendo anche le rispettive declinazioni del diritto all'informazione: diritto a essere informati su fatti (divenuti nuovamente) attuali, da un lato; diritto "alla Storia", dall'altro.

Ora, a noi sembra che un diritto a essere informati declinato, al contempo, sia in senso *attualizzante* che in senso *storico* rischi di comprimere in modo eccessivo le aspettative di tutela del singolo, che corre così il rischio – tanto più inaccettabile, quanto più le accuse si rivelino infondate – di rimanere per un tempo indeterminato indebitamente esposto alla "gogna virtuale". Non resta che augurarsi che la ventura giurisprudenza della Corte, auspicabilmente corroborata dai *diritti* ora sanciti nella legislazione UE, riesca – senza irragionevolmente comprimere la libertà d'informazione e il diritto alla Storia[60] – a delineare in modo più nitido i contorni del "diritto

[57] Rifiuta questa ipotesi R. Pardolesi, *L'ombra del tempo e (il diritto al) l'oblio*, cit., 83, giudicandola un «rimedio – ineluttabilmente sovradimensionato – [che] travolge tutto e, nel segno dell'oblio violato per qualche (breve) tempo, porta alla condanna definitiva della memoria».

[58] Ancora, V. Manes, *La 'vittima' del 'processo mediatico'*, cit., 124 s.

[59] Corte EDU, *Fuchsmann*, cit., § 36, 39.

[60] Sul rischio che la nuova disciplina sull'oblio mascheri forme di censura generalizzata, S. Bonavita-R. Pardolesi, *GDPR e diritto alla cancellazione (oblio)*, in *Danno resp.*, 2018, 3, 279 ss.

umano all'oblio", specie laddove connesso all'irrinunciabile principio della presunzione d'innocenza.

Scenari applicativi

La successione nei rapporti digitali e la tutela post-mortale dei dati personali

Giorgio Resta

Sommario: 1. L'economia dell'immateriale e la successione nei beni e rapporti digitali – 2. I problemi coinvolti e le soluzioni emergenti – 3. Il modello successorio: l'esperienza tedesca – 4. Il modello personalistico – 4.1. La riforma francese – 4.2. La riforma italiana – 5. Il modello dell'autonomia privata

1. L'economia dell'immateriale e la successione nei beni e rapporti digitali

Il regime dei dati personali e degli altri contenuti digitali nella fase successiva alla morte del soggetto cui essi si riferiscono costituisce uno degli argomenti oggi maggiormente dibattuti nel quadro del diritto dell'economia digitale[1].

Le corti sono spesso chiamate a confrontarsi con controversie attinenti all'accesso o al riuso dei dati, personali e non, conservati nelle piattaforme[2]. A questo tema sono stati dedicati di recente svariati saggi e alcuni volumi monografici, di impronta non soltanto giuridi-

[1] K. Nemeth-J. Morais Carvalho, *Digital Inheritance in the European Union*, in *EuCML*, 2017, 253.

[2] Per un'analisi degli ultimi sviluppi, v. G. Resta, *Personal data and digital assets after death: a comparative law perspective on the BGH* Facebook *ruling*, in *EuCML*, 2018, 4 (in corso di stampa); M.O. Mackenrodt, *Digital Inheritance in Germany*, in *EuCML*, 2018, 41.

ca, ma anche sociologica, economica e antropologica[3]. Le organizzazioni rappresentative delle varie professioni giuridiche hanno pubblicato diversi rapporti e *position papers* di ampio respiro[4]. Lo stesso legislatore è intervenuto in diversi paesi (europei e extraeuropei) per definire un primo quadro di regole applicabili alla successione nei beni e nei rapporti digitali[5].

L'importanza pratica assunta dalle questioni appena evocate è riconducibile a una precisa serie di fattori di natura socio-economica:

i) una porzione preponderante della ricchezza nelle economie contemporanee è oggi costituita da beni immateriali[6]. Di conseguenza, la massa ereditaria è destinata ad attrarre al suo interno in misura sempre crescente *assets* intangibili, rendendo particolarmente importante la definizione di una serie di regole chiare che governino la devoluzione di tali beni[7];

[3] Tra i saggi recenti di più ampio respiro v. M. Bock, *Juristische Implikationen des digitalen Nachlasses*, in *AcP*, 2017, 217, 370; L. Edwards-E. Harbinja, *Protecting Post-Mortem Privacy: Reconsidering the Privacy Interests of the Deceased in a Digital World*, in 32 *Cardozo Arts & Ent. L.J.* 83, 2013; D. McCallig, *Facebook after death: an evolving policy in a social network*, in *Int.'l J. L. & Tech.* 1, 2013; J. Groffe, *La mort numérique*, in *D.*, 2015, chr., n. 28; C. Camardi, *L'eredità digitale. Tra reale e virtuale*, in *Dir. inf.*, 2018, 65; nonché, volendo, G. Resta, *La morte digitale*, in *Dir. inf.*, 2014, 891. Tra i volumi non strettamente giuridici si segnala E.C. Steinhart, *Your Digital Afterlives. Computational Theories of Life After Death*, Basingstoke-New York, Palgrave Macmillan, 2014.

[4] V. ad es. *Stellungnahme des Deutschen Anwaltvereins durch die Ausschüsse Erbrecht, Informationsrecht und Verfassungsrecht zum Digitalen Nachlass*, n. 34/2013, Berlin, 2013; Consiglio Nazionale del Notariato, *Password, credenziali e successioni mortis causa*, Studio n. 6-2007/IG.

[5] V. *infra*, parr. 4-5.

[6] J. Haskal-S. Westlake, *Capitalism Without Capital. The Rise of the Intangible Economy*, Princeton, Princeton University Press, 2017.

[7] In tema cfr. H. Conway-S. Grattan, *The 'New' New Property: Dealing with Digital Assets on Death*, in *Modern Studies in Property Law: volume 9*, edited by H. Conway-R. Hickey, Oxford, Hart Publishing, 2017, 99 ss.; H. Ludyga, *'Digitales Update' fuer das Erbrecht im BGB?*, in *ZEV*, 2018, 1; v. anche A.F. Watkins, *Digital Properties and Death: What Will Your Heirs Have Access to After You Die?*, 62 *Buffalo L. Rev.* 193, 2014; M. Perrone, *What Happens When We Die: Estate Planning of Digital Assets*, 21 *CommLaw Conspectus* 185, 2012; R. Pinch, *Protecting Digital Assets After Death: Issues to Consider in Planning For Your Digital Estate*, 60 *Wayne L. Rev.* 545, 2014; e già A. Zoppini, *Le 'nuove proprietà' nella trasmissione*

ii) le odierne tecnologie dell'informazione e della comunicazione fanno sì che una massa enorme di dati personali persista oltre la vita del soggetto, tendenzialmente per un periodo illimitato di tempo (secondo alcune stime circa 10.000 titolari di account Facebook muoiono ogni giorno; 312.000 ogni mese; il 5% degli account esistenti attengono a "zombie" digitali) [8]; da parte degli utenti della rete si fa sempre più insistente la pretesa al controllo di tali informazioni nella fase post-mortale, quale logico prolungamento del diritto alla protezione dei dati personali[9].

iii) tali dati sono conservati e trattati da intermediari professionali, sicché non soltanto essi esulano dalla disponibilità materiale di eredi e congiunti, ma sono anche fatti oggetto di una riserva contrattuale – che stabilisce sovente espressamente l'intrasmissibilità *mortis causa* – da parte del professionista [10]; tale riserva si trova spesso a confliggere con i principi fondamentali del diritto delle persone e del diritto delle successioni, e di qui il proliferare di controversie.

iv) l'"economia politica della morte" nell'era dell'informazione è connotata dallo sviluppo di una serie di servizi economicamente lucrativi (servizi di messaggeria e gestione delle password; memoriali online; servizi di ricreazione dell'identità del defunto attraverso tecniche di intelligenza artificiale, etc.), i quali hanno determinato una crescente *commodification* dei dati e dell'identità digitale del defunto[11];

v) la cultura della micro-celebrità esaltata dalla rete Internet ha condotto ad una sorta di "democratizzazione" dei conflitti attinenti alla sfera post-mortale: mentre nel passato le con-

ereditaria della ricchezza (note a margine della teoria dei beni), in *Riv. dir. civ.*, 2000, I, 185.

[8] G. Resta, *La morte digitale*, cit., 894.

[9] J.C. Buitelaar, *Post-mortem privacy and informational self-determination*, 19 *Ethics Inf. Technol.*, 129, 2017.

[10] N.M. Banta, *Inherit the Cloud: The Role of Private Contracts in Distributing or Deleting Digital Assets at Death*, 83 *Fordham L. Rev.* 799, 2014.

[11] C. Öhman-L. Floridi, *The Political Economy of Death in the Age of Information: A Critical Approach to the Digital Afterlife Industry*, in 27 *Minds and Machines* 639, 2017.

troversie attenevano quasi esclusivamente alla tutela degli interessi delle persone note (dall'attrice Rachel[12], al Cancelliere Bismarck[13], al Presidente Mitterand[14]), oggi lo sviluppo dell'industria ha reso qualsiasi individuo la fonte di un flusso di dati particolarmente appetibile per il mercato, con l'effetto di una significativa "granularizzazione" delle ipotesi di violazione e tutela giuridicamente rilevanti.

2. I problemi coinvolti e le soluzioni emergenti

Se la sinergia dei suddetti fattori spiega agevolmente perché il tema della "morte digitale" si sia di recente imposto all'attenzione del giurista teorico e pratico, più difficile è stilare un quadro di principi e soluzioni sufficientemente condivisi. Le difficoltà derivano da molteplici ragioni.

Innanzitutto, v'è il dato fenomenologico costituito dalla elevata eterogeneità dei beni e delle situazioni giuridiche coinvolti. La nozione di 'eredità digitale' (e i suoi corrispondenti "digital inheritance" e "Digitaler Nachlass"), come generalmente impiegata in letteratura, è molto ampia e i suoi confini non sono suscettibili di agevole demarcazione[15]. Tra i beni e i rapporti che ad essa vengono più comunemente ascritti si annoverano i seguenti: *a*) documenti digitali offline; *b*) contenuti immessi e conservati nei social media; *c*) messaggi di posta elettronica e comunicazioni chat; *d*) profili online personali e professionali; *e*) *avatars* e dati relativi a giochi virtuali; *f*) accounts;

[12] Trib. civ. Seine, 16-6- 1858, in *D.*, 1858, III, 62.

[13] RG, 28-12-1899, *GRUR*, 1900, 196, con nota di J. Kohler, *Zum Autorrecht und Individualrecht. Der Fall der Bismarckphotographie.*

[14] Cass., 14-12- 1999, in *D.*, 2000, jur., 372, con nota di B. Beignier; Eur. Ct. H. R., 18-5 2004, App. n. 58148/00, Éditions Plon v. France.

[15] Sul punto v. C. Camardi, *L'eredità digitale. Tra reale e virtuale*, cit., 73, la quale riconduce a tale nozione il «fenomeno della successione nelle attività e nelle posizioni del *de cuius* collegate alla produzione e al controllo dei suoi dati personali e delle sue risorse, quanto gli uni e le altre si presentano in formato digitale e/o collegati ad un rapporto giuridico con un fornitore di servizi ascrivibile alla categoria degli Internet Service Providers»; G. Marino, *La 'successione digitale'*, in *ODCC*, 2018, 167 ss., 169.

g) files conservati attraverso servizi di *cloud computing*; *h*) criptovalute; *i*) nomi di dominio[16]. Stante la disomogeneità interna della categoria, si è suggerito di distinguere due principali classi di beni, in funzione della connotazione prevalentemente patrimoniale (come le criptovalute e i contenuti protetti da diritti di proprietà intellettuale) o personale (messaggistica email e chat, profili di social network) delle situazioni coinvolte[17]. In linea astratta, tale demarcazione contribuirebbe ad apportare maggiore chiarezza concettuale e a offrire una griglia ordinata per l'analisi e la soluzione dei problemi applicativi in oggetto. Ne deriverebbe, in particolare, una netta diversificazione di statuto e regole applicabili tra le fattispecie successorie a carattere meramente patrimoniale (come nel caso delle criptovalute e dei beni protetti da diritti di proprietà intellettuale, eccezion fatta per le opere protette dal diritto d'autore) e quelle che coinvolgono beni e rapporti direttamente interferenti con le situazioni della persona, e in primo luogo i dati personali[18].

Tuttavia, è necessario osservare come le suddette categorie possano essere un'effettiva valenza soltanto come idealtipi. Nella realtà, i confini tra le due classi si rivelano ben più permeabili e sovrapponibili di quanto si possa supporre in astratto, da un lato perché la dimensione personale e quella patrimoniale delle informazioni sono sovente inscindibilmente correlate[19], sia perché nella realtà digitale il medesimo contenente può indifferentemente ospitare contenuti patrimoniali e contenuti personali (si pensi soltanto a un account di posta elettronica). Di conseguenza, modelli analitici e soluzioni flessibili appaiono preferibili rispetto a schemi concettuali più lineari e rigorosi, ma spesso incapaci di offrire una valida lente per la comprensione della realtà.

[16] V. in proposito B. Maeschaelck, *Digital Inheritance in Belgium*, in *EuCML*, 2018, 37, 38.

[17] Per il modello teorico v. T. Hoeren, *Der Tod und das Internet - Rechtliche Fragen zur Verwendung von E-Mail- und WWW-Accounts nach dem Tode des Inhabers*, in *NJW*, 2005, 2113; M. Martini, *Der digitale Nachlass und die Herausforderung postmortalen Persönlichkeitsschutzes im Internet*, in *JZ*, 2012, 1145.

[18] V. ad es. C. Camardi, *L'eredità digitale. Tra reale e virtuale*, cit., 75 ss.

[19] Sul punto sia consentito rinviare a G. Resta, *Autonomia privata e diritti della personalità*, Napoli, 2005, 245; e v. ora anche G. Marino, *La 'successione digitale'*, cit., 188.

In secondo luogo, è fonte di non pochi problemi l'attrito che viene inevitabilmente a determinarsi tra la logica regolativa sottesa al funzionamento delle maggiori piattaforme digitali, la quale risponde prevalentemente a esigenze tecnologiche e di business, e il linguaggio e il *modus operandi* del diritto. Per di più, tale frizione è acuita dalla coesistenza tra il carattere transnazionale del mercato, al quale si rivolgono tali piattaforme e l'impronta prettamente locale della relativa struttura organizzativa e regolamentare. È un dato ben noto, infatti, che le maggiori piattaforme digitali hanno sede o origine negli USA, e da tale ordinamento riprendono sia la cultura gestionale, sia la conformazione istituzionale[20]. Da ciò discendono tuttavia numerose ragioni di conflitto, atteso non soltanto che le condizioni generali di contratto contengono sovente clausole incompatibili con norme imperative del diritto europeo (si pensi soltanto alle clausole di scelta del foro competente e della legge applicabile)[21], ma anche che la cultura giuridica nordamericana muove da una visione delle finalità e dei limiti del sistema di tutela della persona molto diversa e sotto vari profili incompatibile con quella stratificatasi nel continente[22].

Per questi ed altri motivi non è facile rispondere al quesito, che occupa il giurista teorico e pratico, su chi sia titolare di un potere di controllo (declinabile secondo le varie forme di appartenenza) su dati personali e contenuti digitali nella fase post-mortale.

3. Il modello successorio: l'esperienza tedesca

All'interrogativo appena fermato sono state offerte diverse risposte, varianti sia in funzione dei formanti coinvolti, sia del loro contenuto. Se in alcuni ordinamenti sono state approntate specifiche discipline volte a governare il fenomeno della successione digitale, in altri il silenzio del legislatore ha rimesso l'iniziativa al formante

[20] In tema, per maggiori approfondimenti, sia consentito rinviare a G. Resta, *Digital Platforms under Italian Law*, in U. Blaurock-M. Schmidt-Kessel-K. Erler (a cura di), *Plattformen: Geschäftsmodell und Verträge*, Baden-Baden, 2018, 99 ss.

[21] V. Zeno-Zencovich-G. Giannone Codiglione, *Ten Legal Perspectives on the 'Big Data Revolution'*, *Concorrenza e mercato*, 2016, 29, 49; M.B. Loos, *Standard terms for the use fo the Apple App Store and the Google Play Store*, *EuCML*, 2016, 10.

[22] V. *infra*, par. 4.

giurisprudenziale. Sia nell'uno sia nell'altro caso, si è fatto ricorso a opzioni regolatorie che combinano in vario modo tre principali modelli: *a*) il modello successorio; *b*) il modello personalistico; *c*) il modello dell'autonomia privata.

Il primo modello muove da una lettura in senso proprietaria dei beni immateriali compresi nel patrimonio del soggetto e si propone di verificare in che modo il diritto delle successioni iscritto nei codici civili classici possa essere adattato alla realtà dell'economia digitale[23]. Un saggio particolarmente istruttivo delle potenzialità – ma anche dei limiti – dell'approccio successorio è offerto da una recente, importante, pronunzia del *Bundesgerichtshof*, che rappresenta la prima decisione di una corte europea di ultima istanza sul tema della morte digitale[24].

Essa ha ad oggetto la richiesta di accesso ai contenuti dell'account Facebook rivolta alla piattaforma da parte dei genitori (ed eredi) di una ragazza minorenne deceduta in seguito a un tragico incidente nella metropolitana di Berlino, dovuto probabilmente a suicidio. I genitori intendevano prendere cognizione dei contenuti presenti nell'account della figlia, al fine di comprendere meglio la natura dell'incidente e precostituire alcuni strumenti di prova nell'ipotesi di un'azione di responsabilità promossa nei loro confronti da parte del conducente del treno, il quale lamentava uno shock nervoso sofferto in conseguenza dell'evento. Tuttavia l'account era stato "memorializzato" in seguito alla notifica della scomparsa della donna, e pertanto, ad avviso di Facebook, non sarebbe stato più possibile modificarlo, né accedervi.

Convenuta in giudizio di fronte al *Landgericht* di Berlino, Facebook si difendeva sostenendo che: *a*) l'account non era suscettibile di trasmissione *mortis causa* in base alle *policy* aziendali, nonché alle condizioni generali di contratto alle quali l'utente aveva spontaneamente aderito al momento dell'attivazione del servizio; *b*) in ogni caso Facebook non avrebbe potuto rivelare i contenuti delle comunicazioni, essendo tenuta a uno specifico obbligo di non divulgazione sulla base della legge tedesca sui media telematici; *c*) la tutela postuma della personalità del defunto, così come il dovere di rispetto della confidenzialità delle informazioni imposto dalla normativa sul trat-

[23] Cfr. H. Ludyga, '*Digitales Update*' *fuer das Erbrecht im BGB?*, in *ZEV*, 2018, 1.

[24] BGH, 12-7-2018, III ZR 183/17, in *ZIP*, 2018, 1881; in *WM*, 2018, 1606.

tamento dei dati personali, avrebbero impedito divulgazione a terzi dei dati conservati nel profilo utente del social network.

La richiesta dei genitori, accolta in primo grado con una pronunzia coerente e ben motivata del *Landgericht* di Berlino[25], è stata respinta in grado di appello dal *Kammergericht*[26], che ha insistito soprattutto sull'effetto di vincolo derivante dalla legge tedesca sui media telematici. Con una pronunzia resa nel luglio 2018, il *Bundesgerichtshof* ha cassato la pronunzia di appello, facendo rivivere la decisione di primo grado e pertanto affermando il diritto degli eredi ad ottenere l'accesso all'account Facebook della figlia defunta[27].

Rinviando per un'analisi di dettaglio alle varie note di commento già apparse nelle riviste tedesche ed europee[28], converrà limitarsi a segnalare i tre punti fondamentali del ragionamento della Corte.

In primo luogo, la soluzione adottata dalla corte è prevalentemente basata sulle regole in materia di successioni *mortis causa* e non sulla disciplina dei diritti della personalità o dei dati personali. Ciascuno di tali aspetti è debitamente preso in considerazione e discusso nelle sue implicazioni, ma non rappresenta il fondamento ultimo del rimedio accordato agli attori. La Suprema Corte tedesca muove dall'assunto per cui i rapporti giuridici relativi a beni immateriali pertengono al patrimonio del *de cuius* e sono suscettibili di trasmissione ereditaria[29]. In particolare, dal principio di universalità della successione (§ 1922 BGB) si fa discendere la conseguenza che un account di social network, al pari di tutte le altre posizioni contrattuali, è suscettibile di devoluzione e acquisto *mortis causa*[30]. Nessuna

[25] LG Berlin, 17-12-2015, in *DNotZ* 2016, 537, con nota di S. Gloser; in *ZEV* 2016, 189.

[26] KG Berlin, 31-5-2017, A.Z. 21 U 9/16, in *FamRZ*, 2017, 1348.

[27] BGH, 12-7-2018, cit.

[28] V. in particolare L. Wusthöf, *Germany's Supreme Court Rules in Favour of "Digital Inheritance"*, in *EuCML*, 2018, 5 (in corso di stampa); K.N. Peifer, *Zugang für die Erben gesichert, aber viele Fragen offen: Das BGH-Urteil zu Hinterlassenschaften*, in *https://verfassungsblog.de/zugang-fuer-die-erben-gesichert-aber-viele-fragen-offen-das-bgh-urteil-zu-digitalen-hinterlassenschaften/.*

[29] BGH, 12-7-2018, par. 18.

[30] BGH, 12-7-2018, par. 22. Circa la trasmissibilità *mortis causa* delle posizioni contrattuali si veda F. Padovini, *Le posizioni contrattuali*, in G. Bonilini (a cura di), *Trattato di diritto delle successioni e donazioni*, I, *La successione ereditaria*, Milano, Giuffrè, 2009, 525 ss.

valida obiezione può essere desunta dalla particolare natura dei beni coinvolti, che includono dati personali e non[31]. In contrasto con la posizione assunta da una parte minoritaria della dottrina tedesca[32], la Corte esclude che dati e informazioni di natura personale siano sottratti a successione e destinatari di una tutela indiretta a carattere fiduciario da parte dei prossimi congiunti (come nel caso delle norme in materia di tutela post-mortale dell'immagine). A riprova, vengono espressamente richiamate le disposizioni del *BGB* concernenti l'acquisto dell'eredità (§§ 2373 e 2047), dalle quali si evince chiaramente che le carte e i ricordi di famiglia ricadono nella massa ereditaria, nonostante il loro carattere eminentemente personale[33]. Di conseguenza, i genitori della ragazza hanno diritto ad ottenere l'accesso al complesso delle comunicazioni racchiuse nell'account della figlia, in quanto successori nell'integralità dei rapporti attivi e passivi della donna, e dunque anche nel contratto atipico di utilizzazione del social network, e non invece quali legittimati *iure proprio* o su base fiduciaria alla tutela della personalità della figlia[34].

In secondo luogo, la Corte mostra piena consapevolezza dei limiti intrinseci di una soluzione di stampo prettamente successorio, ed in particolare della sua permeabilità agli atti abdicativi. Difatti, è comunemente ammesso che i contraenti possano liberamente escludere la trasmissibilità delle pretese contrattuali[35]. Ciò risponde sovente all'interesse di entrambe le parti. Tuttavia, nel campo dei rapporti digitali, dove sussiste una forte asimmetria di potere negoziale tra le piattaforme e gli utenti, v'è un serio rischio che, ammettendo il libero gioco dell'autonomia privata, si realizzi la prospettiva di una generalizzata "intrasmissibilità contrattua-

[31] Sul punto M. Bock, *Juristische Implikationen des digitalen Nachlasses*, cit., 393.

[32] Tra gli altri v. T. Hoeren, *Der Tod und das Internet - Rechtliche Fragen zur Verwendung von E-Mail- und WWW-Accounts nach dem Tode des Inhabers*, in *NJW*, 2005, 2113; M. Martini, *Der digitale Nachlass und die Herausforderung postmortalen Persönlichkeitsschutzes im Internet*, in *JZ*, 2012, 1145.

[33] BGH, 12-7-2018, par. 49.

[34] Circa le differenti alternative teoriche, v. G. Resta, *Autonomia privata e diritti della personalità*, cit., 375-389.

[35] M. Bock, *Juristische Implikationen des digitalen Nachlasses*, cit., 384; BGH, 12-7-2018, par. 24.

le"[36]. In altri termini, è reale il pericolo che i fornitori dei servizi on line si assicurino, per il tramite dell'accordo contrattuale formalmente condiviso da entrambe le parti, una preziosa miniera di dati e contenuti digitali, liberamente sfruttabili dopo la morte del soggetto[37]. Pertanto, non si può che salutare con favore il rigore osservato dalla Corte Suprema nel sindacare la validità delle rinunzie contrattuali. Non soltanto si richiede la prova che tali clausole siano effettivamente confluite nel perimetro del programma negoziale sottoscritto dalle parti; il che nel caso in esame era dubbio, atteso che la *policy* di "memorializzazione" non era esplicitata nelle condizioni generali di contratto, bensì nella *help section* del sito in oggetto[38]. Soprattutto, esse devono riflettere un'equa distribuzione dei diritti e degli obblighi e, in particolare, non debbono avvantaggiare unilateralmente una parte a detrimento dell'altra. Nella specie, le clausole in oggetto non riescono a superare il vaglio contenutistico operato dalla Corte alla stregua del § 307, par. 1 e 2, *BGB*[39]. Difatti, la *policy* di memorializzazione svantaggia l'utente in maniera sproporzionata, in quanto determina una modifica retroattiva del piano degli obblighi contrattuali gravanti sul professionista e preclude agli eredi l'accesso all'account, con ciò neutralizzando il principio di universalità della successione (§ 1922 BGB) [40]. Per di più, la *policy* in oggetto risulta in contrasto con il § 307, par. 2, n. 2 BGB, in quanto impedisce il perseguimento delle finalità del contratto[41] e implica la creazione di una sorta di "cimitero dei dati" (*Datenfriedhof*) [42].

In terzo luogo, la divulgazione delle comunicazioni personali conservate nell'account Facebook non è in contrasto con l'art. 88, par. 3, della legge tedesca sulle telecomunicazioni, né con il GDPR.

[36] D. Horton, *Contractual Indescendibility*, 66 *Hastings L.J.* 1047, 2015.

[37] Su questo punto si vedano anche le considerazioni di G. Marino, *La 'successione digitale'*, cit., 176.

[38] BGH, 12-7-2018, par. 27.

[39] BGH, 12-7-2018, par. 29.

[40] BGH, 12-7-2018, par. 29.

[41] BGH, 12-7-2018, par. 30.

[42] BGH, 12-7-2018, par. 29.

Quanto alla prima disposizione, che vieta al fornitore di servizi di telecomunicazione di rivelare il contenuto delle comunicazioni a "terze persone", essa non è opponibile agli eredi. Difatti, costoro succedono nell'intera posizione giuridica di una delle parti della conversazione, e pertanto non possono essere considerati "terzi" ai sensi di legge (art. 88, par. 3 TKG) [43]. Quanto al Regolamento generale sulla protezione dei dati, la Corte ricorda innanzitutto che esso non si applica ai dati di una persona defunta. Pertanto, i problemi in punto di tutela dei dati si pongono unicamente in relazione al partner di una comunicazione con il defunto[44]. Per superare l'obiezione avanzata da Facebook, secondo cui la piattaforma sarebbe tenuta a un dovere di riserbo, la Corte ha fatto ricorso a due distinti argomenti. Innanzitutto, essa ha invocato il disposto dell'art. 6, par. 1, lett. b) del Regolamento 2016/679, che ammette il trattamento dei dati qualora questo sia necessario all'esecuzione di un rapporto contrattuale di cui sia parte l'interessato. Assumendo che il contratto di accesso al social network sia stato validamente trasmesso agli eredi, può agevolmente concludersi che la comunicazione delle informazioni conservate nell'account è lecita, poiché strumentale all'effettivo trasferimento della posizione contrattuale e all'esecuzione delle obbligazioni primarie della piattaforma (fornitura del servizio, conservazione e accesso ai contenuti)[45]. In secondo luogo, la Corte ha richiamato l'art. 6, par. 1, lett. f) del Regolamento 2016/679, il quale autorizza il trattamento dei dati personali necessario per il "perseguimento del legittimo interesse" del titolare o di terzi. Atteso che gli eredi, nonché genitori, della donna intendevano accedere all'account al fine di apprendere elementi utili a chiarire l'esistenza di un possibile progetto di suicidio della figlia, come pure a dotarsi di prove spendibili in una possibile causa di risarcimento dei danni, la divulgazione delle informazioni avrebbe dovuto ritenersi legittima[46].

[43] BGH, 12-7-2018, par. 56; sul punto v. M. Bock, *Juristische Implikationen des digitalen Nachlasses*, cit., 407.

[44] BGH, 12-7-2018, par. 67.

[45] BGH, 12-7-2018, par. 72.

[46] BGH, 12-7-2018, pars. 80-81.

4. Il modello personalistico

Distinto, ma non necessariamente alternativo al modello successorio, è quello personalistico. Per convenzione, intendo con quest'espressione sia l'approccio strettamente fondato sui diritti della personalità, sia quello sui dati personali, non ignorando però che sulla *ratio* della tutela dei dati personali sussistano opinioni difformi.

Come si accennava in apertura del presente scritto, una delle maggiori difficoltà insite nel governo delle fattispecie successorie aventi ad oggetto contenuti digitali è costituita dal fatto che le piattaforme più importanti sono regolate in maniera conforme alla cultura giuridica e ai vincoli istituzionali posti dal sistema statunitense, trovando queste in prevalenza la loro sede o la loro origine negli USA.

Il primo aspetto su cui è opportuno ragionare, in quest'ottica, è rappresentato dal diverso livello di protezione accordato alla privacy postuma dall'uno e dall'altro lato dell'Atlantico. Come si è avuto modo di chiarire più diffusamente in altra sede[47], nel diritto USA gode ancora di ampio credito la tesi per cui *actio personalis moritur cum persona*; sicché le azioni a tutela della privacy si estinguono – come espressamente prevede il *Restatement Second of Torts*[48] – con la morte del soggetto. Di conseguenza, eredi e congiunti non possono trovare nel sistema di tutela civile della personalità (*rectius*, della privacy, quando si discorra del modello USA)[49] un valido appiglio da cui desumere un set di rimedi inibitori e risarcitori a fini della protezione postuma degli interessi del defunto. Né ad esiti diversi conduce l'analisi della disciplina in materia di protezione dei dati personali. Difatti, a livello costituzionale, il Quarto e il Quattordicesimo Emendamento sono stati ritenuti non applica-

[47] G. Resta, *La morte digitale*, cit., 899-900.

[48] § 652, *Restatement of Torts 2nd* (1977): «except for the appropriation of one's name or likeness, an action for invasion of privacy can be maintained only by a living individual whose privacy is invaded».

[49] V. G. Resta, *Personnalité, Persönlichkeit, Personality: Comparative Perspectives on the Protection of Identity in Private Law*, in *European Journal of Comparative Law & Governance*, 2014, 1, 215.

bili alla posizione del defunto[50]; il *Freedom of Information Act* e il *Privacy Act* del 1974 sono stati interpretati dalle corti nel senso di escludere che l'interesse alla privacy sia meritevole di tutela nella fase post-mortale[51]. Chiaramente ciò implica che, nell'ottica di una piattaforma, il controllo sui dati personali del *de cuius* non trova un limite negli altrui diritti della persona e può essere assunto come "dotazione" dell'impresa, a meno che l'accordo contrattuale non disponga diversamente.

Diverso, invece, è il punto di partenza degli ordinamenti europei, i quali in larga parte muovono dalla tesi della persistenza di interessi giuridicamente tutelabili in capo ai prossimi congiunti[52]. I modelli divergono quanto alla prospettazione dogmatica della legittimazione di tali soggetti, nonché – sia pure in minore misura – alla natura dei rimedi esperibili. I sistemi area germanica propendono per una legittimazione fiduciaria dei congiunti, che si spiega in ragione di una *Fortwirkung* dei diritti della persona e segnatamente del dovere di rispetto della dignità del defunto[53]. I sistemi di matrice francese, tra cui quello italiano, optano invece per un meccanismo di acquisto *iure proprio* di un diritto nuovo, fondato sul legame familiare con lo scomparso[54]. Queste differenze, notevoli se osservate nell'ottica del giurista municipale, scolorano quando vengano poste a confronto con il diverso approccio condiviso dai sistemi di *common law*. Qui, come si è detto, si muove dall'assunto dell'estinzione pressoché completa dei rimedi posti a tutela della personalità del defunto; per contro, i sistemi continentali realizzano tutti, pur dando a tale effetto una diversa veste dogmatica, una proiezione dell'apparato rimediale oltre il momento della morte.

Ciò implica, per il tema in oggetto, che gli strumenti di protezione della personalità appaiono astrattamente in grado di assicurare una

[50] N.M. Banta, *Death and Privacy in the Digital Age*, 94 *North Carol. L. Rev.* 927 (2016), alla p. 940 (anche per i necessari riferimenti giurisprudenziali).

[51] N.M. Banta, *Death and Privacy in the Digital Age*, cit., 941-942.

[52] G. Resta, *L'oggetto della successione: i diritti della personalità*, in *Trattato di diritto delle successioni e donazioni*, diretto da G. Bonilini, cit., 729 ss.

[53] G. Resta, *L'oggetto della successione: i diritti della personalità*, cit., 736.

[54] G. Resta, *L'oggetto della successione: i diritti della personalità*, cit., 735.

prima forma di controllo sull'identità digitale postuma. A riprova potrebbe citarsi una interessante pronunzia brasiliana, che ha riconosciuto su questa base il diritto di ottenere la cancellazione del profilo "memoriale" del defunto[55].

Strettamente correlato al discorso della tutela della personalità è quello relativo all'applicazione della disciplina in materia di protezione dei dati personali. In proposito le soluzioni adottate dagli ordinamenti europei sono maggiormente differenziate: la soluzione più restrittiva coesiste con una tendenza, che gode di consensi crescenti, a ricomprendere i dati del defunto all'interno della disciplina del trattamento dei dati personali.

A tal riguardo mette conto rapidamente ricordare che la direttiva 95/46 si applicava soltanto ai dati relativi alle "persone fisiche" e non contemplava espressamente la situazione del defunto. Come chiarito dal Gruppo art. 29, nell'Opinione 4/2007, l'informazione relativa a persone defunte non avrebbe dovuto ritenersi, ai sensi della direttiva 95/46, un dato personale[56]. Il GDPR si sofferma espressamente su tale questione, stabilendo al Considerando 27 che il Regolamento non è applicabile ai dati personali di una persona defunta e che gli stati membri hanno la discrezionalità di introdurre norme relativamente a tale fattispecie[57].

A livello nazionale, sono accolte diverse soluzioni. Guardando alla fase successiva all'introduzione della direttiva 95/46, sono tre i principali modelli regolatori che emergono dall'osservazione comparatistica[58].

Innanzitutto vi sono ordinamenti che escludono espressamente l'applicabilità della normativa in materia di tutela dei dati personali alle informazioni relative a defunti (cfr. ad esempio l'art. 3

[55] Trib. Campo Grande (Juiz. Esp. Cent., 1 vara), 2-3-2013, *Dolores Pereira Ribeiro Coutinho c. Facebook*, accessibile all'indirizzo www.migalhas.com.br/arquivo_artigo/art20130424-12.pdf

[56] Art. 29 Data Protection Working Party, Opinion 4/2007, *On the concept of personal data*, 01248/07/EN WP 136, alla p. 22.

[57] Cfr. i *Considerando* nn. 27, 158, 160.

[58] Per un panorama dettagliato, v. E. Harbinja, *Post-mortem privacy 2.0: theory, law, and technology*, 31 *International Review of Law, Computers & Technology* 26 (2017), alla p. 33.

della legge svedese[59]; l'art. 1(1) della legge inglese[60]; l'art. 2 (iv) della legge irlandese[61]).

In secondo luogo, vi sono ordinamenti che si astengono dal dettare – a livello legislativo – una soluzione chiara in un senso o nell'altro. In questa prospettiva è rilevante l'esempio tedesco: il *Bundesdatenschutzgesetz* non contempla la fattispecie, ma la dottrina e la giurisprudenza hanno in prevalenza optato per la tesi dell'applicabilità di tale disciplina unicamente ai dati delle persone viventi[62].

Infine, un terzo gruppo di ordinamenti propende per un'estensione della tutela, attribuendo ai congiunti, agli eredi o ad altri soggetti il potere di esercitare i diritti dell'interessato dopo la sua morte. In questa categoria si colloca, tra gli altri paesi, l'Italia; mentre la legge francese riconosce agli eredi soltanto il diritto di domandare al titolare del trattamento l'aggiornamento e l'integrazione dei dati, in modo tale da riflettere l'intervenuto decesso dell'interessato[63].

4.1. La riforma francese

Se si prende in considerazione la fase successiva, ed in particolare la normativa di implementazione del Regolamento 2016/679, è agevole constatare che il tema della tutela postuma dei dati ha ricevuto una accresciuta attenzione.

L'esempio indubbiamente più significativo è costituito dalla Francia, che ha recentemente approvato una disciplina dettagliata delle "direttive anticipate di trattamento". Come si è pocanzi accennato, l'art. 40, c. 6, della legge *Informatique et libertés* del 1978, come emendata dalla legge n. 2004-801 del 6 agosto 2004, si limitava a prevedere

[59] Ove si definiscono come "dati personali": «all kinds of information that directly or indirectly may be referable to a natural person who is alive».

[60] UK Data Protection Act, Sect. 1(1) (e), secondo cui sono dati personali i dati «which relate to a living individual».

[61] Secondo la Sect. 2 (iv) dell'Irish Data Protection (Amendment) Act, si definiscono dati personali «data relating to a living individual».

[62] In proposito v. M. Bock, *Juristische Implikationen des digitalen Nachlasses*, cit., 398-399; H. Ludyga, *'Digitales Update' fuer das Erbrecht im BGB?*, in *ZEV*, 2018, 1; e per una posizione meno restrittiva M.J. Heinemann-D. Heinemann, *Postmortaler Datenschutz*, in *DuD*, 4, 2013, 242.

[63] V. *infra*, par. 4.1.

il diritto dei congiunti a richiedere un aggiornamento dei dati del defunto[64]. In costanza di tale assetto normativo, le corti hanno affermato in diverse occasioni che i diritti dell'interessato hanno natura personale e, pertanto, si estinguono al momento della morte[65]. Di riflesso, i congiunti risultavano sprovvisti di alcun effettivo strumento di tutela dell'identità digitale del defunto, a meno che non fossero in grado di dimostrare che il trattamento interferiva direttamente con la propria sfera personale. Al fine di colmare le lacune lasciate aperte da tale assetto regolatorio[66], il legislatore è intervenuto nel 2016, nel contesto della più generale legge sulla *République numérique*[67]. Si è quindi introdotta un'articolata disciplina della "morte digitale" [68], racchiusa in un nuovo art. 40-1 aggiunto alla legge *Informatique et libertés* ed informata ai seguenti principi:

i) i diritti dell'interessato si estinguono di regola con la morte (art. 40-1, c. 1);
ii) tuttavia, ciascun individuo può stabilire direttive generali o speciali concernenti il trattamento dei propri dati personali *post mortem* (art. 40-1, c. 2);
iii) le direttive generali di trattamento concernono l'insieme dei dati personali e possono essere depositate presso un *trusted third party* certificato dalla CNIL e rese conoscibili attraverso un apposito registro;

[64] Art. 40, c. 6: «Les héritiers d'une personne décédée justifiant de leur identité peuvent, si des éléments portés à leur connaissance leur laissent présumer que les données à caractère personnel la concernant faisant l'objet d'un traitement n'ont pas été actualisées, exiger du responsable de ce traitement qu'il prenne en considération le décès et procède aux mises à jour qui doivent en être la conséquence. Lorsque les héritiers en font la demande, le responsable du traitement doit justifier, sans frais pour le demandeur, qu'il a procédé aux opérations exigées en vertu de l'alinéa précédent». In tema v. N. Metallinos, *Accès des héritiers: distinction entre personne intéressée et personne concernée*, in *Comm. Comm. Électr.*, 2016, comm. 74.

[65] CE, 8-6-2016, n° 386525, *RGD on line*, 2016, n° 23948, con nota di P. Cossalter; CE, 7-6-2017, n° 399446, M. A. B. c/ CNIL, *CCE*, Oct. 2017, comm. 84, con nota di n. Metallinos, *Conditions de l'extension de la notion de personne concernée aux héritiers*.

[66] Su cui si veda J. Groffe, *La mort numérique*, *D.*, 2015, chr., n. 28.

[67] Art. 63, par. 2, Law 7-10-2016, n. 2016-1321 *pour une République numérique*.

[68] C. Pérès, *Les données à caractère personnel et la mort. Observations relatives au projet de loi pour une République Numérique*, *D.*, 2016, 90.

iv) le direttive particolari concernono soltanto le tipologie dati a cui si riferiscono, sono depositate presso il titolare del trattamento coinvolto, e sono efficaci se espresse attraverso un consenso specifico della persona, non potendo in ogni caso risultare dalla sottoscrizione di condizioni generali di contratto;
v) tali direttive sono sempre revocabili e possono contenere la designazione di un fiduciario incaricato della loro esecuzione;
vi) qualsiasi clausola contenuta in condizioni generali di contratto che limiti o escluda le prerogative riconosciute all'interessato in ordine al governo postumo della propria identità digitale si ha per non scritta;
vii) in assenza di direttive anticipate, gli eredi possono esercitare i diritti dell'interessato al fine: *a*) di dar corso alla vicenda successoria, ed in particolare ottenere le informazioni utili alla ricostruzione del relitto, nonché tutte le comunicazioni e i contenuti oggetto di trasmissione per causa di morte; *b*) di regolare gli effetti della morte sul rapporto negoziale inerente ai social network, e in particolare disporre la sua prosecuzione o definitiva risoluzione.

4.2. La riforma italiana

La disciplina francese, ancora priva di riscontri giurisprudenziali, costituisce uno dei primi esempi di regolamentazione in via legislativa del problema della morte digitale. L'adeguamento degli ordinamenti nazionali al Regolamento 2016/679 ha offerto l'occasione per rimeditare la questione e elaborare analoghi modelli di disciplina, ritagliati sul sistema della protezione dei dati personali. Particolarmente istruttiva, a tal proposito, è la scelta compiuta dal legislatore italiano.

Il decreto legislativo 10 agosto 2018, n. 101, ha dedicato una specifica disposizione, l'art. 2-*terdecies*, al tema della tutela post-mortale e dell'accesso ai dati personali del defunto[69]. Essa si colloca in un'e-

[69] Per ragioni di trasparenza è opportuno chiarire che l'autore di queste pagine ha partecipato al Gruppo di Lavoro costituito presso il Ministero della Giustizia e incaricato della predisposizione del decreto legislativo finalizzato all'adeguamento dell'ordinamento interno al Regolamento 2016/679.

vidente – anche sul piano lessicale – linea di continuità con la disciplina previgente, e in particolare con l'art. 9, c. 3, del d.lgs. 196/2003[70]. Al contempo sono presenti forti elementi di novità, che denotano l'intento del legislatore di modernizzarne i contenuti, adeguandone il portato alla realtà del mondo digitale. Se ne illustreranno di seguito i principali.

Innanzitutto, il primo comma della disposizione citata riprende la struttura testuale dell'art. 9, c. 3, del Codice della protezione dei dati personali, prevedendo un ampio spettro di legittimati attivi all'esercizio post-mortale dei diritti dell'interessato. Come già nel previgente Codice, anche qui il legislatore non entra nel merito della vicenda acquisitiva, chiarendo se si tratti di un vero e proprio acquisto *mortis causa* (almeno in alcuni casi) o di una semplice legittimazione *iure proprio*[71]. Ci si limita, invece, a prefigurare una sorta di persistenza (*Fortwirkung*) dei diritti in questione oltre la vita della persona fisica, rilevante soprattutto a livello remediale[72]. Le medesime questioni sollevate dalla dottrina in margine all'art. 9, c. 3 (e prima ancora all'analoga norma della l. 675/1996) si ripropongono, dunque, sostanzialmente invariate. La scelta di fondo di non alterare l'assetto normativo previgente – una scelta che appare ragionevole, anche in considerazione dell'esigenza di non intaccare la ricca esperienza applicativa stratificatasi, soprattutto nei settori bancario e sanitario[73], anche a costo di riprodurre una norma non priva di difetti sul piano testuale e su quello concettuale – non è tuttavia assoluta.

[70] Tale disposizione prevedeva che: «i diritti di cui all'articolo 7 riferiti a dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato o per ragioni familiari meritevoli di protezione».

[71] In tema v. A. Zoppini, *Le 'nuove proprietà' nella trasmissione ereditaria della ricchezza (note a margine della teoria dei beni)*, in *Riv. dir. civ.*, 2000, I, 185 ss., 231; A. Nervi, *I diritti dell'interessato*, in V. Cuffaro-R. D'Orazio-V. Ricciuto (a cura di), *Il codice del trattamento dei dati personali*, Torino, Giappichelli, 2007, 61 ss., 73; S. Pardini, *sub art. 13*, II, in C.M. Bianca-F.D. Busnelli (a cura di), *Tutela della privacy. Commentario alla l. 31 dicembre 1996, n. 675*, in *Nuove leggi civ. comm.*, 1999, 417-420.

[72] Cfr. C. Camardi, *L'eredità digitale. Tra reale e virtuale*, cit., 81.

[73] Per un'elencazione dei principali provvedimenti e pronunzie in materia v. G. Resta, *La morte digitale*, cit., 914-915, note 114, 115 e 116.

Difatti, vi sono due elementi particolarmente innovativi che meritano di essere specificamente segnalati. Il primo consiste nell'estensione del novero dei diritti suscettibili di esercizio post-mortale: la novella include, infatti, anche il diritto alla portabilità dei dati, che a sua volta rappresenta una delle più importanti novità del Regolamento 2016/679 (art. 20). Tale estensione si spiega non soltanto con considerazioni di ordine sistematico, ma anche con l'esigenza di far sì che l'intero pacchetto di dati originariamente oggetto di trattamento possa essere riacquisito – anche dopo la morte del soggetto – al patrimonio del dante causa e non rimanga indefinitamente nella disponibilità del titolare[74]. Un'esigenza, quest'ultima, che trova un duplice fondamento, sia nel diritto al controllo sulla circolazione dei dati personali, sia nella logica del mercato concorrenziale, che presuppone il contrasto all'effetto di *lock in* conseguente all'impossibilità di recuperare il proprio pacchetto di dati, eventualmente al fine di trasferirlo ad altri titolari[75]. Se questa è la *ratio* della norma in oggetto, si dovrebbe logicamente limitare in via interpretativa la cerchia dei soggetti legittimati all'esercizio del diritto alla portabilità, restringendola soltanto a chi agisca «a tutela dell'interessato, in qualità di suo mandatario, o per ragioni familiari meritevoli di protezione». Sarebbe cioè ragionevole escludere che tale situazione soggettiva possa essere esercitata – a differenza dell'accesso, o dell'integrazione, ad esempio – da parte di chi "ha un interesse proprio" e la cui pretesa non sia fondata su un legame, di natura successoria, familiare o fiduciaria, con il *de cuius*. In tal caso non potrebbe infatti ravvisarsi alcuna valida ragione che giustifichi l'acquisto non soltanto di un "diritto a ricevere" i dati personali riferibili al defunto, ma soprattutto di un "diritto di trasmettere tali dati a un altro titolare del trattamento"; un diritto, questo, che disvela un vero e proprio "contenuto attributivo" (nel senso di *Zuweisungsgehalt*) tale da far presupporre una vera e propria vicenda successoria o quanto meno

[74] Per un simile ordine di considerazioni, sia pure in un differente contesto, M.O. Mackenrodt, *Digital Inheritance in Germany*, cit.

[75] Per una siffatta lettura del diritto alla portabilità dei dati, v. R. Janal, *Data Portability – A Tale of Two Concepts*, in 8 *JIPITEC* 59 (2017); B.P. Paal-D.A. Pauly, *Datenschutz-Grundverordnung*, München, 2017, sub § 20, Rn. 4; n. Metallinos, *La protection des données au service de l'émancipation du consommateur*, in *CCÉ*, 2, 2017, comm. 17.

una legittimazione fiduciaria che tragga origine da un'espressa manifestazione di volontà del *de cuius*[76]. Per quanto osservato, dovrebbe dunque logicamente ritenersi che l'esercizio post-mortale del diritto alla portabilità sia riservato agli eredi e/o ai prossimi congiunti (secondo il modello degli artt. 93 e 96 l.d.a.)[77], nonché ai fiduciari del defunto, mentre esso rimane precluso a chi invochi un mero "interesse proprio".

Tale conclusione permette di evidenziare il secondo elemento di novità della norma, e segnatamente il riferimento, che era assente nella disposizione previgente, al "mandatario" quale soggetto legittimato all'esercizio dei diritti dell'interessato. Un lettore frettoloso o poco avvertito potrebbe ravvisare in tale inciso una svista del legislatore italiano. Così non è. Il legislatore ha preso atto dell'esistenza di una prassi ormai consolidata nel campo dei rapporti online, in ragione della quale i soggetti "affidano", generalmente attraverso apposite piattaforme, o sezioni dedicate all'interno dei maggiori social networks, le proprie credenziali di accesso, oppure l'intera gestione della propria identità digitale a soggetti di propria fiducia, come amici, parenti o professionisti[78]. Tale prassi non è parsa, alla dottrina prevalente, confliggere con i principi ordinatori del nostro diritto delle successioni, almeno nei limiti in cui attraverso questi schemi non si provveda all'attribuzione di diritti patrimoniali, poiché altrimenti si incorrerebbe nella violazione del divieto dei patti successori (art. 458 c.c.), ma si appresti unicamente un regolamento per i rapporti afferenti alla sfera della personalità[79]. Tecnicamente, gli atti con i quali il *de cuius* provveda ad incaricare un terzo affinché costui compia per suo conto, dopo la morte, determinati atti giuridici, sono riconducibili alla fattispecie del mandato *post mortem exequendum*[80] (o secondo un'altra ricostruzione, non differente nella sostanza, ad un negozio unilaterale atipico, con funzione autoriz-

[76] Sull'ipotesi della legittimazione fiduciaria basata sul mandato *post mortem exequendum* v. *infra*.

[77] Su cui v. G. Resta, *Autonomia privata e diritti della personalità*, cit., 396 ss.

[78] G. Resta, *La morte digitale*, cit., 916 ss.

[79] C. Camardi, *L'eredità digitale. Tra reale e virtuale*, cit., 84, 91-92; e già G. Resta, *La morte digitale*, cit., 919.

[80] *Ibid*.

zatoria ed efficacia *post mortem*)[81]. Una fattispecie, quest'ultima, di prevalente matrice dottrinale[82], ma che riceve ora dal d.lgs. 101/2018 un espresso suggello normativo, candidando tale schema negoziale a porsi come alternativa efficace alla – pur sempre possibile[83] – nomina di un esecutore testamentario.

Completamente nuovi sono invece i commi successivi. Essi perseguono l'obiettivo di valorizzare l'autonomia privata, e segnatamente l'autodeterminazione informativa della persona, bilanciandola con l'interesse dei successori e dei terzi. Se il primo comma fissa la regola di *default* – ricavata, come si è detto, dalla normativa previgente – per cui i diritti dell'interessato non si estinguono, ma sono suscettibili di esercizio *post mortem*, il secondo comma introduce opportunamente un duplice limite, costituito rispettivamente dalla norma di legge e dalla contraria intenzione del *de cuius*. Recita il secondo comma: «L'esercizio dei diritti di cui al comma 1 non è ammesso nei casi previsti dalla legge o quando, limitatamente all'offerta diretta di servizi della società dell'informazione, l'interessato lo ha espressamente vietato con dichiarazione scritta presentata al titolare del trattamento o a quest'ultimo comunicata». Se il rinvio alla norma di legge si giustifica con il rilievo che l'ordinamento volta per volta attribuisca a interessi contrastanti con quelli sottesi all'esercizio dei diritti dell'interessato, la valorizzazione della volontà del *de cuius* si rivela opportuna, perché colma una lacuna della disciplina previgente e soddisfa un'istanza chiaramente emersa nella prassi e valorizzata dalla dottrina[84].

[81] Così G. Marino, *La 'successione digitale'*, cit., 197.

[82] Cfr. ad es. G. Bonilini, *Concetto, e fondamento, della successione* mortis causa, in G. Bonilini (a cura di), *Trattato di diritto delle successioni e donazioni*, I, cit., 27; N. Di Staso, *Il mandato* post mortem exequendum, in *Fam. pers. succ.*, 2011, 685.

[83] Sul punto v. C. Camardi, *L'eredità digitale. Tra reale e virtuale*, cit., 73, la quale riconduce a tale nozione il «fenomeno della successione nelle attività e nelle posizioni del *de cuius* collegate alla produzione e al controllo dei suoi dati personali e delle sue risorse, quanto gli uni e le altre si presentano in formato digitale e/o collegati ad un rapporto giuridico con un fornitore di servizi ascrivibile alla categoria degli Internet Service Providers».

[84] V. M. Martini, *Der digitale Nachlass und die Herausforderung postmortalen Persönlichkeitsschutzes im Internet*, cit., 1147 ss.

Nel campo dei servizi della società dell'informazione, al quale la norma è destinata, il ricorso agli strumenti della comunicazione elettronica determina la produzione di una massa di dati che, considerati in via aggregata, possono rivelare i dettagli più intimi e riservati della sfera personale. Pertanto si è avvertita la necessità, riflessa in alcuni casi giurisprudenziali, di lasciare all'individuo stesso la scelta se lasciare agli eredi e ai superstiti legittimati la facoltà di accedere ai propri dati personali e esercitare tutti (o parte) dei diritti dell'interessato, oppure sottrarre tali informazioni all'accesso e alla cognizione di terzi. Una valorizzazione dell'autonomia che, sia detto per inciso, fa sorgere naturale il parallelo con la disciplina delle direttive anticipate di trattamento – la coincidenza terminologica merita di essere sottolineata – nell'ambito della gestione del corpo (legge 22 dicembre 2017, n. 219)[85].

Si noti, a questo riguardo, la divergenza degli itinerari percorsi rispettivamente dalla riforma francese e da quella italiana. La prima, muovendo dall'idea dell'automatica estinzione dei diritti dell'interessato al momento della morte (art. 40-1, c. 1, legge *Informatique et libertés*), dedica ampio spazio alle direttive anticipate di trattamento, garantendo al soggetto la possibilità di preservare, attraverso positiva manifestazione di volontà, l'esercizio di tali diritti nella fase post-mortale (art. 40-1, c. 2). La seconda, invece, muove dall'opposta regola della persistenza dei diritti dell'interessato (art. 2-*terdecies*, c. 1, d.lgs. 101/2018) e perciò imprime alla volontà del soggetto un contenuto prevalentemente negativo, nel senso di escludere o conformare l'esercizio dei diritti di cui agli artt. 15-22 del Regolamento dopo la morte del disponente. L'autodeterminazione informativa, proiettata nella fase post-mortale, può dunque avere un contenuto positivo, là dove prefissi condizioni e modalità di governo dell'identità digitale, ma anche negativo, qualora si esprima nel divieto di accesso e intervento modificativo sui dati personali[86].

[85] Circa tale parallelo non può non richiamarsi il pensiero di Stefano Rodotà, che a più riprese ha rilevato la crescente convergenza di problemi sottesi rispettivamente al governo del "corpo fisico" e del "corpo elettronico" (v. ad es. S. Rodotà, *Variazioni sulla libertà personale*, in *Studi in onore di Gianni Ferrara*, III, 2005, 363 ss.).

[86] In generale v. J.C. Buitelaar, *Post-mortem privacy and informational self-determination*, cit.

Il terzo comma riflette la consapevolezza dei rischi che una delega in bianco all'autonomia privata può produrre nel mondo digitale. Come si è ricordato in precedenza, il rapporto con le piattaforme soffre di strutturali asimmetrie informative e di potere negoziale, sicché è opportuno che l'esercizio dell'autonomia privata sia attentamente vagliato e controllato dall'ordinamento perché questo non si traduca in una mera mistificazione[87]. L'opzione seguita dal legislatore italiano è convergente nella sostanza con quella adottata in Francia, dove si sono posti fermi limiti all'utilizzazione delle condizioni generali di contratto; essa ne diverge, però, per la tecnica prescelta. Il decreto legislativo prescrive, infatti, che «la volontà dell'interessato di vietare l'esercizio dei diritti di cui al comma 1 deve risultare in modo non equivoco e deve essere specifica, libera e informata». Non può sfuggire come il lessico impiegato sia ricalcato sul disposto dell'art. 4, c. 1, n. 11) del Regolamento 2016/679; ciò tradisce l'intento del legislatore di sottoporre la manifestazione di volontà proibitiva ai medesimi requisiti sostanziali e formali prescritti dal GDPR in relazione al consenso dell'interessato. In particolare, i presupposti della specificità e della libertà del consenso possono operare in funzione di salvaguardia, escludendo che il divieto di esercizio dei diritti dell'interessato sia desumibile dalla semplice sottoscrizione di condizioni generali di contratto e da clausole di rinunzia predisposte unilateralmente dal fornitore del servizio. Su questo, ovviamente, sarà la prassi delle Corti e del Garante a stabilire con precisione i limiti di ammissibilità della contrattazione standardizzata, come già sperimentato, negli ultimi vent'anni, in relazione al consenso dell'interessato[88].

Infine, mentre il quarto comma precisa opportunamente che la volontà espressa dall'interessato è sempre suscettibile di revoca o modifica, il quinto comma chiarisce che il divieto in oggetto «non può produrre effetti pregiudizievoli per l'esercizio da parte dei ter-

[87] Cfr. *supra*, parr. 1 e 2.

[88] Su cui v. in particolare l'indagine di S. Thobani, *I requisiti del consenso al trattamento dei dati personali*, Santarcangelo di Romagna, Maggioli, 2016; Id., *La libertà del consenso al trattamento dei dati personali e lo sfruttamento economico dei diritti della personalità*, in *Eur. dir. priv.*, 2016, 513 ss.; nonché, volendo, G. Resta-V. Zeno-Zencovich, *Volontà e consenso nella fruizione dei servizi in rete*, in *Riv. trim. dir. proc. civ.*, 2018, 411 ss., spec. 426.

zi dei diritti patrimoniali che derivano dalla morte dell'interessato nonché del diritto di difendere in giudizio i propri interessi». Si tratta di un ragionevole bilanciamento delle posizioni coinvolte (si pensi ad esempio alla posizione di un legittimario pretermesso che intenda esercitare l'azione di riduzione, e al pregiudizio che costui ricaverebbe dall'impossibilità di avere accesso ai dati bancari del *de cuius*), il quale riflette le soluzioni già emerse in sede di applicazione della legge 675/1996 e del Codice della protezione dei dati personali.

5. Il modello dell'autonomia privata

Il terzo modello, quello dell'autonomia privata, è quello che riscuote il maggior credito sia presso gli operatori del settore, sia presso il legislatore nordamericano. V'è, infatti, una tendenza emergente a sviluppare, anche per ragioni di business, interfacce informatiche che agevolino una scelta consapevole del soggetto in ordine alla destinazione delle proprie "tracce" digitali per il tempo successivo alla morte[89]. Di alcuni dei più diffusi strumenti si è offerta una descrizione dettagliata in altra sede e non è pertanto necessario ripetere quanto già scritto[90]. È, invece, opportuno segnalare che negli Stati Uniti è stata approntata una legge-modello (la quale è priva, com'è noto, di valore vincolante sino a che non venga trasposta nel diritto dei singoli Stati), la quale ravvisa nella designazione volontaria di un fiduciario lo strumento principale di risoluzione dei conflitti inerenti l'amministrazione dell'eredità digitale[91]. Analoga scelta è stata compiuta nel 2016 in Canada[92].

Secondo il suddetto schema legislativo, l'utente ha facoltà di nominare un fiduciario, attribuendogli il compito di amministrare,

[89] S. Guillemot-A. Gourmelen, *Quand les entreprises s'emparent de la mort numérique, qui sont les consommateurs potentiels?*, in *Rev. fr. gest.*, 2017, 123 ss.; C. Öhman-L. Floridi, *The Political Economy of Death in the Age of Information: A Critical Approach to the Digital Afterlife Industry*, cit.

[90] G. Resta, *La morte digitale*, cit., 917 ss.

[91] Si tratta del *Revised Uniform Fiduciary Access to Digital Assets Act*, approvato dalla *National Conference of Commissioners on Uniform State Laws* nel 2015.

[92] Uniform Law Conference of Canada, *Uniform Access to Digital Assets by Fiduciary Act* (2016).

disporre, divulgare o eliminare i dati, contenuti digitali e comunicazioni personali riferibili al *de cuius* per la fase successiva alla sua morte[93]. Non siamo molto distanti dalla figura del mandato *post mortem*, evocata dal d.lgs. 101/2018, se non fosse per due importanti profili di disciplina che connotano questo testo. Il primo consiste nella previsione espressa per cui, in caso di contrasto tra la designazione fiduciaria effettuata attraverso un *online tool* – il quale assicuri la costante modificabilità e revocabilità della dichiarazione – e quella contenuta in un testamento, in un atto istitutivo di *trust* o altro documento scritto, la prima è destinata a prevalere (Sect., 4, lett. a)[94]. Il secondo è dato dalla regola per cui, in assenza di una specifica manifestazione di volontà del *de cuius*, la sorte dei dati e dei contenuti digitali è regolata dalle condizioni generali di prestazione del servizio online (Sect. 5)[95].

Siamo ben distanti, dunque, dall'approccio successorio o da quello personalistico, per ciò che la regola contrattuale non trova un limite esterno nelle norme imperative desunte dal diritto delle successioni o dal diritto della protezione dei dati personali. Il che è coerente con le coordinate di fondo del sistema di riferimento, ma non necessariamente in linea con le esigenze di controllo contenutistico dell'autonomia privata segnalate dall'osservazione della prassi e riflesse nella già citata pronunzia della Suprema Corte tedesca[96].

[93] Per un'analisi approfondita della legge-modello, v. H. Conway-S. Grattan, *The 'New' New Property: Dealing with Digital Assets on Death*, cit., 112-114; G. Marino, *La 'successione digitale'*, cit., 198 ss.

[94] Sul punto v. G. Marino, *La 'successione digitale'*, cit., 200.

[95] *Ibid*.

[96] *Supra*, par. 3.

La tutela dei dati personali nel rapporto di lavoro

Roberto D'Orazio

Sommario: 1. Un benchmarking delle regole di tutela dei dati personali – 2. I controlli sul lavoratore – 3. La giurisprudenza della Corte EDU – 4. Il Regolamento 2016/679 e la sua attuazione in Italia e in Spagna – 5. Note conclusive

1. Un benchmarking delle regole di tutela dei dati personali

La tematica riferita alla protezione dei dati personali nel rapporto di lavoro è d'interesse evidentemente non limitato alla prospettiva specifica del giuslavorista, poiché per una pluralità di aspetti essa investe il piano dei diritti fondamentali e si offre quale "banco di prova" – tra i più significativi – del bilanciamento degli interessi messi in gioco dal trattamento di dati a carattere personale.

Il motivo dell'attrattiva interdisciplinare della materia è ancor più palese se si rammenta come nella cultura giuridica italiana il diritto alla riservatezza abbia cominciato a prendere forma anche attraverso la lente rivolta agli indici normativi della tutela dei lavoratori. Evocare questa originaria e indifferenziata matrice – il diritto alla riservatezza – non pare qui ridondante, ove si consideri che l'intreccio tra protezione dei dati personali e tutela della persona trova chiara impronta nel Regolamento UE 2016/679, in cui il solo riferimento diretto alla "dignità umana" (da tutelare in uno con i "diritti fondamentali e gli interessi legittimi dei lavoratori") è dedicato alla protezione dei dati nel contesto lavorativo (art. 88).

La misura del tempo trascorso da quelle prime riflessioni è data tuttavia dalla profondità di implicazioni che il medesimo tema viene rivestendo oggi, a contatto con le incisive e radicali trasformazioni dell'organizzazione produttiva nell'economia globalizzata; implicazioni che vanno ben oltre l'ambito settoriale di riferimento poiché toccano, e mettono anzi in risonanza, corde fondamentali del sistema normativo della protezione dei dati qual è ora delineato dal Regolamento.

Ciò per una serie di motivi, di cui i più evidenti si collegano, per un verso, all'embricarsi dello stato di soggezione giuridica in cui versa il lavoratore dipendente con il potere di controllo che il datore di lavoro è in grado di esercitare su di lui attraverso il trattamento dei suoi dati; dati che sono oggetto di raccolta e di elaborazione non soltanto in relazione ad isolati momenti o vicende del rapporto di lavoro (come l'assunzione o il licenziamento), ma hanno origine dalla stessa prestazione lavorativa quando le sue modalità di svolgimento consentano, in modo costante e dinamico, di ricavarne informazioni di carattere personale sul soggetto che la effettua; e si comprende che il fenomeno possa oggi assumere una densità tale da giustificarne la rappresentazione da alcuni già resa in termini di "work datafication".

Per altro verso, l'interesse suscitato dal tema in esame non può che riferirsi all'incidenza dell'evoluzione tecnologica sull'organizzazione del lavoro e alla pervasività sociale dei nuovi dispositivi tecnologici. Tali fattori tendono ad attenuare, se non talvolta ad elidere – senza più differenza di tempo e di luogo – il confine tra l'uso che di tali strumenti viene fatto per effettuare la prestazione lavorativa e le diverse utilizzazioni poste in essere dal lavoratore nella dimensione privata; con il rischio che il carattere di subordinazione che informa il rapporto di lavoro possa così estendersi, di fatto, ad ambiti a questo estranei. E si comprende allora che in alcuni Paesi, come la Francia, il Belgio e più recentemente il nostro (con la legge 81/2017), si sia cercato di presidiare la separatezza dei contesti mediante la previsione di un "diritto alla disconnessione" in cui in certa misura riecheggia il classico "right to be let alone"[1].

[1] Sul "diritto alla disconnessione", v., per tutti, D. Poletti, *Sul c.d. diritto alla disconnessione nel contesto dei diritti digitali*, in *Resp. civ. prev*., 2017, 1, 8.

Per contro, un elemento mantenutosi costante nella riflessione svolta su tali temi attiene al rapporto che si configura tra la specialità della materia lavoristica e l'applicazione dei principi generali in relazione alla tutela della riservatezza e alla protezione dei dati personali. Tale specificità è stata riconosciuta dal legislatore, il quale nel dettare regole per il trattamento e la protezione dei dati ha tenuto ferme le disposizioni dello Statuto dei lavoratori sul controllo a distanza, intese come preminenti in ragione della speciale materia che ne è oggetto rispetto alle norme generali sulla protezione dei dati. Da ciò è derivata un'intersezione dei piani normativi su cui non sempre è facile orientarsi. Il mosaico che si è così formato non pare tuttavia statico né immutabile, poiché i principi generali ricevono aggiornate applicazioni giurisprudenziali nel "laboratorio" della tutela multilivello dei diritti, rivelando talora implicazioni che potrebbero mettere tra loro in tensione il *genus* e la *species* della disciplina del trattamento dei dati.

2. I controlli sul lavoratore

Nello scenario appena tratteggiato, il confronto tra le esigenze dell'impresa e i diritti del lavoratore sollecita bilanciamenti il cui assetto postula una rinnovata definizione della portata e dei limiti dello stesso controllo esercitabile dal datore di lavoro.

È ben vero che il controllo datoriale si ramifica in una varietà tipologica di dispositivi diversi per caratteristiche tecniche, modalità ed ambiti di potenziale esplicazione, oppure per l'eventuale abilitazione dell'utente a poterne selezionare o disattivare le funzioni. La configurazione dei sistemi, le finalità effettivamente perseguite per loro tramite, l'informazione resa all'interessato circa la loro operatività sono elementi sulla cui base deve valutarsi la legittimità del controllo e se ne siano state ragionevoli e proporzionate le modalità di esercizio.

È tuttavia un dato di comune osservazione che le relazioni di lavoro siano esposte agli effetti caratteristici della diffusione nella vita quotidiana di dispositivi tecnologici (di comunicazione interpersonale, di geolocalizzazione) in grado di produrre una mole di informazioni su chi ne faccia uso; talché un datore di lavoro, avendovi accesso, sarebbe nella condizione non soltanto di poter sottoporre a più intensa verifica l'adempimento della prestazione lavorativa, ma

anche di acquisire sul soggetto che la effettua una conoscenza notevolmente accresciuta in senso qualitativo e quantitativo, benché non necessariamente esatta o veritiera.

Inoltre tale conoscenza – lo si è anticipato – non si limita al tempo o al luogo di lavoro o ad una singola attività (come avrebbero prescritto le classiche "unità aristoteliche", se è lecito il paradosso), ma può attingere dai social networks, fonte continuativa di una caleidoscopica varietà di informazioni personali che, all'insaputa dell'interessato, potrebbero fornire materia per condotte discriminatorie poste in essere nei suoi confronti, se non anche essere utilizzate a detrimento della trasparenza della contrattazione di cui egli sia parte. In altri termini, lo stesso "ambiente" tecnologico in cui si trovi ad operare il lavoratore può incorporare il controllo, esponendolo ad una sorveglianza che può cumularsi con quella subita in veste di utente "ordinario" dei medesimi o di altri strumenti tecnologici utilizzati per le proprie private finalità: ciò potrebbe mettere in dubbio l'idea stessa di una *workplace privacy* da tutelarsi mediante apposite norme[2].

La portata dei controlli che possono esercitarsi sul lavoratore, e la messe delle informazioni che in tal modo possono essere raccolte su di lui, impongono dunque un ordine di garanzie che possa fare riferimento tanto alla protezione dei dati personali, intesa come liceità e correttezza delle attività di trattamento, quanto alla tutela della privacy, ossia alla salvaguardia della sfera privata, implicando entrambi i termini del tradizionale binomio cui corrispondono le tutele codificate dagli art. 7 ed 8 della Carta di Nizza.

Al riguardo può notarsi che mentre la Direttiva europea 95/46/CE (ora abrogata) non prevedeva alcuna disciplina specifica per il trattamento di dati personali di lavoratori dipendenti, il Regolamento ne persegue la relativa tutela in entrambe le direzioni appena richiamate; ciò in coerenza con l'elaborazione giurisprudenziale che, svoltasi nel "dialogo tra le Corti", ha evidenziato in un'ampia casistica la necessità di una tutela della persona, non riducibile alla soggettività del lavoratore nel quadro del rapporto che lo vincola.

[2] Nondimeno, devono tenersi presenti le indicazioni del Consiglio d'Europa rivolte a contestualizzare i principi generali di tutela dei dati con riferimento al rapporto di lavoro: Raccomandazione CM/Rec (2015) 5 del Comitato dei Ministri agli Stati membri sul trattamento di dati personali nel contesto occupazionale.

Si tratta di un'impostazione, peraltro, che può rivelarsi idonea ad "agganciare" la tutela dei dati ai mutamenti dell'organizzazione produttiva che tendono oggi a moltiplicare le figure atipiche in un quadro di complessiva debolezza del lavoratore.

Ne sono esempio i moduli organizzativi peculiari della "gig economy", su cui si impernia il dilemma qualificatorio del lavoratore *app-driven*, intensamente "geolocalizzato" (sebbene autonomo, secondo la qualificazione resa recentemente dai giudici di merito) e per il quale, tra il controllo effettuato sulla sua prestazione e la flessibilità della stessa, si giocano le sorti di una soggezione ai poteri datoriali intesa come porta d'ingresso alle più forti tutele garantite dalla legge[3]. Oppure, si pensi al "telelavoro" o al "lavoro agile", dove la prestazione lavorativa del dipendente è scissa dai luoghi tradizionalmente deputati al suo svolgimento e può comportare l'esercizio di controlli a distanza da parte del datore. Ed ancora – salva la problematicità dell'adattamento della disciplina del lavoro subordinato alle nuove forme di emergenti di lavoro –, questioni inerenti alla tutela dei dati personali possono proporsi in relazione ad attività che fanno leva sulla reputazione del lavoratore operante nei mercati digitali, richiedendosi in tale ipotesi il bilanciamento tra la tutela dei suoi dati e l'esigenza della piattaforma digitale di acquisire informazioni sull'adeguatezza dei prestatori rispetto all'attività che sono chiamati a svolgere, affinché sia garantita la sicurezza dei fruitori dei servizi[4].

L'attitudine delle tutele apprestate dal Regolamento a ramificarsi in relazione alla varietà delle forme occupazionali, d'altra parte, è incentivata dalla previsione che (ancora all'art. 88) riconosce agli Stati membri la facoltà di dettare norme più specifiche in materia di "trattamento dei dati nell'ambito dei rapporti di lavoro". Il motivo di questo margine di intervento rimesso ai legislatori nazionali riposa non tanto sulla peculiarità di tale trattamento, quanto sulle diversità culturali che in questo campo sussistono tra gli Stati membri e vi ispirano criteri differenziati di bilanciamento degli interessi coinvolti; basti pensare alla variegata esperienza delle relazioni in-

[3] Per un esame delle questioni relative al fenomeno, v. G. Balandi, *Concetti lavoristici impigliati nella Rete*, in *Riv. trim. dir. proc, civ*., 2018, 461.

[4] Su tali profili v. A. Toso, Automatic management, *reputazione del lavoratore e tutela della riservatezza*, in *Lavoro e diritto*, 2018, 454.

dustriali nei diversi paesi, al differente peso politico delle organizzazioni portatrici di interessi e alla diversa struttura della contrattazione collettiva, che il Regolamento espressamente include tra le fonti normative idonee a specificare la propria disciplina[5].

In effetti, il rinvio alle legislazioni statali e lo spazio rimesso a specificazioni normative potrebbero introdurre elementi di differenziazione suscettibili di affievolire l'uniformità della tutela dei dati personali in uno dei suoi ambiti maggiormente qualificanti. È da presumere, tuttavia, che vi si possa raggiungere un elevato grado di omogeneità attraverso la tipizzazione delle forme legittime di controllo datoriale da parte della giurisprudenza, finora complessivamente caratterizzata, nelle sue componenti integrate nel sistema di tutela multilivello dei diritti, dalla ricerca di una costante aderenza ai mutamenti tecnico-economici e alle correlate prassi organizzative. Su questo piano viene in risalto la particolare "vitalità" dell'art. 8 Cedu, che in ambito lavoristico ha trovato innovativa applicazione declinandovi, in coerenza con le attuali dinamiche tecnologiche, i canoni di dignità e di libertà, posti ad argine del controllo arbitrario cui venga sottoposto il lavoratore[6].

3. La giurisprudenza della Corte EDU

Il repertorio delle decisioni pronunciate dai giudici di Strasburgo annovera una casistica indicativa sia della tipologia dei controlli

[5] Peraltro, la scelta di agevolare una specificazione della tutela dei dati nell'ambito lavoristico è in linea con quanto sosteneva anni addietro Spiros Simitis, il quale metteva in guardia dai rischi connessi all'adozione di regolazioni *omnibus* inidonee, per il loro carattere di generalità e astrattezza, ad assicurare «un'adeguata protezione della persona in ogni contesto in cui vengono trattati i relativi dati personali», e addirittura delineava un rapporto di proporzionalità inversa tra l'ampiezza del margine di interpretazione delle norme dettate a tale scopo e la loro efficacia: S. Simitis, *Il contesto giuridico e politico della tutela della privacy*, in *Rivista critica del diritto privato*, 1997, 563.

[6] Nella vastissima dottrina, v. A. Trojsi, *Il diritto del lavoratore alla protezione dei dati personali*, Torino, Giappichelli, 2013; P. Tullini (a cura di), *Controlli a distanza e tutela dei dati personali del lavoratore*, Torino, Giappichelli, 2017; C. Colapietro, *Tutela della dignità e riservatezza del lavoratore nell'uso delle tecnologie digitali per finalità di lavoro*, in *Giorn. dir. lav. rel. ind*., 2017, 439; A. Sitzia, *Il diritto alla "privatezza" nel rapporto di lavoro tra fonti comunitarie e nazionali*, Padova, Cedam, 2013.

datoriali sia degli equilibri che, in applicazione del canone della proporzionalità, devono definirsi al fine di tracciare la linea di separatezza tra la vita privata, presidiata nella sua intangibilità, e la dimensione soggettiva esposta ai doveri e alle interazioni derivanti dal rapporto di lavoro.

Tre decisioni, in particolare, fanno stato dei più recenti orientamenti dalla Corte, e da diverse angolazioni riguardano l'accessibilità al datore di lavoro di informazioni non professionali conservate dal dipendente sui dispostivi aziendali assegnatigli in dotazione; possiamo qui richiamarle solo per sommi capi, riservando al successivo paragrafo l'esame di un'ulteriore pronuncia.

In un caso di notevole risonanza (*Bârbulescu*)[7], la Corte è giunta a prospettare in via indiretta, constatando la violazione del diritto alla tutela della "vita privata", l'illegittimità convenzionale del licenziamento disciplinare del lavoratore quale conseguenza di indebite intrusioni ed interferenze poste in essere nei suoi confronti dal datore di lavoro. Dopo un primo rigetto del ricorso nel 2016[8], la Corte ha affermato, in sede di riesame dinanzi alla Grande Camera, che il diritto alla tutela della vita privata del ricorrente fosse violato dall'accesso ai messaggi presenti nella sua casella aziendale di posta elettronica da parte del datore di lavoro (benché motivato dall'esigenza gestionale di rilevare, mediante il monitoraggio delle comunicazioni personali, le infrazioni al divieto di utilizzare a fini privati le risorse aziendali).

In tale occasione i giudici hanno ricondotto al perimetro della "vita privata" l'aspettativa dell'individuo al suo sviluppo personale e a condurre una "vita sociale adeguata", ossia la possibilità di

[7] Corte EDU (Grande Camera), *Bârbulescu c. Romania*, 5 settembre 2017 (ricorso n. 61496/08). Per un commento della decisione v., *e multis*, C. Calomme, *Monitoring of Employees' Communications: ECtHR Spells Out Positive Obligations to Protect Employees' Privacy*, in *Eur. Data Prot. Law*, 4/2017, 545; J. Eichenofer, *Internet Privacy at Work – the ECtHR Bârbulescu Judgment*, ivi, 2/2016, 266; A. Sitzia, *I limiti del controllo della posta elettronica del lavoratore: una chiara presa di posizione della Corte eur. dir. uomo*, in *NGCC*, n. 12/2017, 1656; G. Bronzini-S. Giubboni, *La tutela della privacy dei lavoratori e la Corte di Strasburgo, oltre il Jobs Act*, in *Riv. crit. dir. priv.*, 2018, 155; J. Hörnle, *European Court of Human Rights on Finding the Right Balance in Respect of Employer Email Monitoring – An Opportunity Missed!*, in *Scripted*, 2017, 1, 100.

[8] Corte EDU, *Bârbulescu c. Romania*, 12 gennaio 2016 (ricorso n. 61496/08).

sviluppare un'identità sociale la cui espressione, poiché integra certamente la sfera soggettiva tutelata, non solamente deve essere lasciata immune da interferenze arbitrarie dell'autorità pubblica, ma pone sugli Stati contraenti obblighi positivi affinché sia garantito un effettivo rispetto dei diritti tutelati nelle dinamiche sociali e nelle relazioni instaurate tra privati. I rapporti di lavoro non derogano a tali obblighi, poiché nonostante l'ampio margine di valutazione concesso agli Stati in materia, compete a questi disciplinare le condizioni (principalmente di trasparenza, correttezza, proporzionalità, non eccedenza) in base alle quali un datore di lavoro può regolamentare, senza incorrere in abusi o dare corso ad iniziative arbitrarie, le comunicazioni elettroniche effettuate dai propri dipendenti sul posto di lavoro per finalità non professionali[9].

Interessa qui notare come la stessa esistenza di un regolamento interno (in prima battuta valorizzata dalla Corte, nella prima pronuncia resa nel caso di specie, per argomentare l'esclusione una violazione dell'art. 8), sia stata ritenuta (dalla Grande Camera investita del caso) irrilevante ai fini della tutela della vita privata del dipendente, giacché la *policy* adottata dal datore di lavoro non avrebbe potuto valere ad annichilire la vita sociale del dipendente e a violarne la riservatezza della corrispondenza[10].

[9] È degno di nota che nel caso *Bârbulescu* la Corte abbia formulato un "test di compatibilità", enumerando i criteri a cui i giudici nazionali devono attenersi nel valutare la legittimità delle misure adottate e individuare l'indebita interferenza che queste possano eventualmente rappresentare per la sfera personale del lavoratore. Tali criteri, in sintesi, riguardano la previa notifica e descrizione del monitoraggio che la parte datoriale voglia effettuare; l'entità e la durata del monitoraggio, facendo distinzione tra il controllo sul flusso delle comunicazioni del dipendente e quello sul loro contenuto; la sussistenza di motivi fondati e legittimi per effettuare controlli contenutistici; il possibile ricorso a misure di controllo meno intrusive, e la valutazione delle conseguenze del monitoraggio sul dipendente interessato.

[10] Una traiettoria analoga ha seguito la giurisprudenza italiana con una decisione della Cassazione (I sez. civ., 19 settembre 2016, n. 18302), con cui il giudice di legittimità ha confutato una "lettura" orientata a ritenere che l'adozione di un qualunque regolamento aziendale potesse di per sé suffragare il rispetto dei diritti fondamentali nel contesto lavorativo.

In un secondo caso (*Antovic*)[11], la Corte si è pronunciata sulla installazione di videocamere di sorveglianza in un'aula universitaria dove i ricorrenti, due docenti universitari, tenevano le proprie lezioni. In tale occasione essa ha estensivamente ricompreso nella nozione di "vita privata" ogni manifestazione di attività idonea a consentire lo sviluppo delle interazioni sociali, comprese quelle poste in essere in ambito professionale o condotte in luogo pubblico; e ha argomentato che, in mancanza di un controllo dell'insegnamento stabilito per legge, l'installazione di impianti di videosorveglianza in luoghi di lavoro può essere lecita, e non costituire un'indebita ingerenza nella sfera privata, solo in quanto costituisca una misura necessaria e proporzionata in relazione a specifiche esigenze di sicurezza, da soddisfare altrimenti con mezzi meno invasivi.

Per converso, in un ultimo caso recente (*Libert*)[12] , la Corte ha ritenuto il medesimo parametro non violato dall'accesso del datore ai *files* che il dipendente, contravvenendo al codice deontologico aziendale, aveva archiviato sull'*hard disk* del computer aziendale in sua dotazione, in quanto i documenti oggetto di accesso non erano stati da questo memorizzati o denominati in modo da attestarne inequivocabilmente il carattere "privato".

L'esame delle tre decisioni, seppure sommario[13], vale almeno a individuare un punto fermo: l'ambito della "vita privata" si caratterizza, nell'interpretazione della Corte, per una latitudine che ingloba le attività di natura non professionale svolte sul luogo di lavoro, e comporta immancabilmente l'applicazione del criterio di proporzionalità ad ogni restrizione posta alla relativa tutela.

[11] Corte EDU, *Antovic e Mircovic c. Montenegro*, 28 novembre 2017 (ricorso n. 70838/13).

[12] Corte EDU, *Libert c. Francia*, 22 febbraio 2018 (ricorso. n. 588/13), in relazione al licenziamento di un dipendente della SNCF per violazione del codice deontologico dell'azienda avendo questi utilizzato il pc in sua dotazione professionale per memorizzare propri documenti (contrassegnati, peraltro, come "personali" anziché come "privati").

[13] Sulle sentenze *Bârbulescu* e *Libert* v. il commento di B. Dabosville, *Communication personnelle en entreprise et surveillance patronale:* new deal *ou* status quo*?*, in *Droit social*, 5/2018, 455.

4. Il Regolamento 2016/679 e la sua attuazione in Italia e in Spagna

In questa prospettiva può essere utile il raffronto – suggerito dal titolo di questo Convegno – tra l'esperienza italiana e quella spagnola, accomunate da affinità culturali che permettono di considerare tra loro omogenei il diritto alla riservatezza, consolidatosi in Italia a partire dalla sua origine giurisprudenziale e dottrinale, e il *derecho a la intimidad personal y familiar*, consacrato dalla Carta fondamentale del 1978 (art. 18.1) e compreso nel novero dei diritti tutelabili attraverso il *recurso de amparo*. Comporre in binomio la riservatezza e la *intimidad* è operazione non ostacolata, ai nostri fini, dal differente percorso definitorio ed evolutivo che il diritto in esame ha compiuto nei rispettivi ordinamenti, in uno ad opera prevalentemente dei giudici di merito e, nell'altro, attuato dalla legislazione organica e dalla giurisprudenza costituzionale[14].

In entrambi i Paesi, i criteri di bilanciamento in materia di tutela dei dati nel rapporto di lavoro hanno fatto leva sugli indici normativi generali in materia di dati personali – dettati dal "codice" italiano sui dati personali[15] e dalla *Ley Organica* del 1999 (*LOPD*)[16] –, modulandosi in sistema con quelli settoriali della legislazione lavoristica. L'adattamento della legislazione interna al Regolamento presenta tuttavia alcune differenze che si devono alle distinte premesse da cui hanno mosso i legislatori nazionali.

[14] Ciò senza trascurare come in questo caso il "formante" giurisprudenziale, benché produttivo di esiti sostanzialmente omogenei, sia al suo interno differenziato in ragione dello specifico ruolo interpretativo svolto dal giudice costituzionale nei due ordinamenti, in presenza di un'espressa protezione fondamentale della vita privata oppure attraverso l'individuazione di forme di tutela ricavate da altri diritti. In tema v. G. Famiglietti, *Il diritto alla riservatezza o la riservatezza come diritto. Appunti in tema di riservatezza ed* intimidad *sulla scorta della giurisprudenza della Corte costituzionale e del* Tribunal Constitucional, *paper* del *Forum di Quaderni costituzionali*, 2004 (http://www.forumcostituzionale.it/wordpress/wp-content/uploads/pre_2006/212.pdf).

[15] D.lgs. 30 giugno 2003, n. 196.

[16] *Ley Organica* 15/1999, *de 13 de diciembre, de Protección de Datos de Cáracter Personal* (LOPD), su cui v. T.E. Frosini, *La nuova legge spagnola sulla protezione dei dati personali*, in *Il diritto dell'informazione e dell'informatica*, 2000, 769.

Nel caso italiano si è posta, in particolare, la questione del rapporto tra le previsioni del Regolamento e la *lex specialis* rappresentata dallo Statuto dei lavoratori, ritenendosi che le disposizioni statutarie rilevanti (in particolare l'art. 4 in materia di controlli a distanza come novellato nel 2015 dal c.d. *Jobs Act*[17]), già preservate nella loro operatività dal Codice sul trattamento dei dati personali, costituiscano le "norme specifiche vigenti" la cui adozione è abilitata dal Regolamento (in questo caso attenuato nella sua forza *self-executing*[18]); e che sotto il profilo contenutistico esse, stante la loro ampia formulazione e l'adattabilità al contesto moderno, siano congruenti con i principi stabiliti dalla disciplina europea di diretta applicazione.

Inoltre, la novella del Codice del 2003, introdotta nell'anno in corso per adeguare il diritto interno al Regolamento[19], munisce di base giuridica le "regole deontologiche" da adottare in materia di trattamento e tutela dei dati nel rapporto di lavoro (con il nuovo art. 2 *quater* del decreto legislativo di raccordo). Al nucleo normativo con carattere di specialità e di "hard law", rappresentato dalle disposizioni rilevanti dello Statuto dei lavoratori, si affianca dunque l'autoregolamentazione "assistita" o "guidata", qual è quella tipicamente costituita dall'adozione di codici di condotta[20].

[17] Tra i numerosi commenti alla novella del 2015, v. A. Maresca, *Controlli tecnologici e tutele del lavoratore nel nuovo art. 4 dello Statuto dei lavoratori*, in *Riv. it. dir. lav*., 2016, 513; A. Levi (a cura di), *Il nuovo art. 4 sui controlli a distanza. Lo Statuto dei lavoratori dopo il* Jobs Act, Milano, Giuffrè, 2016; P. Tullini (a cura di), *Web e lavoro. Profili evolutivi e di tutela*, Torino, Giappichelli, 2017; R. Del Punta, *La nuova disciplina dei controlli a distanza sul lavoro*, in *Riv. it. dir. lav*., 2016, 77; O. Dessì, *Il controllo a distanza sui lavoratori. Il nuovo art. 4 Stat. lav*., Napoli, E.S.I., 2017.

[18] Una compiuta disamina della disciplina europea in relazione alla sua applicazione al rapporto di lavoro è svolta da A. Maresca-S. Ciucciovino-I. Alvino, *Regolamento UE 2016/679 e rapporto di lavoro*, 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, 311.

[19] D.lgs. 10 agosto 2018, n. 101; v. il commento a "prima lettura" di V. Cuffaro, *Quel che resta di un codice: il D.Lgs. 10 agosto 2018, n. 101 detta le disposizioni di adeguamento del codice della privacy al regolamento sulla protezione dei dati*, in *Corriere giuridico*, n. 10/2018.

[20] Sotto questo aspetto il ricorso alle regole deontologiche pare assumere valenza particolare in virtù del carattere "negoziale" della loro procedura di adozione, che implica il confronto tra i destinatari delle regole e l'autorità di controllo su

La *sedes materiae* della tutela dei dati nel rapporto di lavoro appare dunque ripartita tra fonti diverse: il Regolamento per quanto attiene ai principi generali; il plesso normativo delineatosi tra il Codice dei dati personali, per le parti sopravvissute alle abrogazioni, e il decreto legislativo di raccordo con il Regolamento; le disposizioni rilevanti dello Statuto dei lavoratori, in quanto costitutive della "disciplina specifica" rimessa ai legislatori nazionali; ed infine, la normativa che può formarsi attraverso l'adozione di regole deontologiche, ancor più specifica poiché destinata ad integrare con maggior grado di analiticità il quadro regolatorio del trattamento dei dati nei singoli settori in cui esso è posto in essere.

A fronte di un quadro normativo così frastagliato, una sua sostanziale *reductio ad unum* pare obiettivo perseguibile attraverso l'attività interpretativa della giurisprudenza, aderente all'indirizzo giurisprudenziale fin qui delineato dalla Corte di Strasburgo. Si è appena visto come questa abbia stabilito precisi parametri per l'interpretazione convenzionalmente conforme delle regole applicate in ambito lavoristico. A tali vincoli non sembra intanto potersi sottrarre l'applicazione del nuovo art. 4 Stat. lav., nel senso di rafforzare la preclusione posta (al comma 3) all'utilizzabilità dei dati personali raccolti e trattati per finalità connesse al rapporto di lavoro ma in violazione delle norme generali di protezione[21].

Più articolata è la vicenda legislativa spagnola, giunta di recente ad adeguare compiutamente il diritto interno al Regolamento, auspice un'elaborazione dottrinale che non ha mancato di mettere in risalto le questioni proprie della tutela dei dati personali nel rapporto di lavoro[22].

materie che, nondimeno, hanno rilevanza per le organizzazioni rappresentative delle categorie dei lavoratori interessati: al punto che il loro coinvolgimento potrebbe non limitarsi ad una mera consultazione preliminare, bensì dare luogo a forme sostanzialmente concertative, come tali suscettibili di porsi in collegamento con la contrattazione collettiva che il Regolamento espressamente individua come una delle fonti di specificazione dei propri principi.

[21] Ma in tema v., *amplius*, V, Turco, *I dati personali del lavoratore*, in V. Cuffaro-R. D'Orazio-V. Ricciuto, *I dati personali nel diritto europeo*, *Il regolamento UE 2016/679*, Torino, Giappichelli (in corso di stampa).

[22] Possono qui richiamarsi almeno J.M. Goerlich Peset, *Protección de la privacidad de los trabajadores en el nuevo entorno tecnológico: inquietudes y paradojas*,

Al riguardo può segnalarsi come il progetto spagnolo di *Ley Organica* del 24 novembre 2017 si fosse inizialmente caratterizzato per una particolare opzione di tecnica normativa. Allo scopo di includervi la regolamentazione dei controlli sul lavoratore effettuata mediante strumenti di videosorveglianza, il progetto (a seguito di alcune proposte emendative della disposizione di riferimento[23]) recepiva il disposto della sentenza *Lopez* pronunciata nel 2018 dalla Corte EDU[24], al fine di fissare nel corpo del testo normativo le condizioni di legittimità convenzionale di tali sistemi di controllo. In tale occasione la Corte ha ritenuto non conformi ai canoni di adeguatezza e proporzionalità, e lesivi del diritto alla vita privata, i mezzi adottati dal datore di lavoro al fine – peraltro legittimo – di tutelare i propri interessi e il diritto di proprietà, non avendo egli provveduto ad informare debitamente i propri dipendenti circa la predisposizione di tali strumenti di controllo in determinati ambienti di lavoro.

È qui d'interesse l'argomentazione dei giudici di Strasburgo. In sintesi, essi hanno chiarito che il diritto alla vita privata poggia sulla legittima aspettativa di riservatezza della persona, fondata sulle garanzie e sui diritti riconosciuti dalla legge; e che potendosi applicare ai rapporti di lavoro la disciplina generale sulla protezione dei dati personali (ossia la *LOPD* al tempo vigente), l'interessato è in grado di esercitare in tale contesto il diritto di accesso, informazione, controllo, rettifica e cancellazione dei dati che lo riguardano. Nel vigore di tale disciplina di tutela, e in virtù della sua applicazione universale, il datore di lavoro non poteva dunque esimersi, neanche sospettando gravi irregolarità da parte dei dipendenti, dal dovere di informarli circa all'introduzione di strumenti di videosorveglianza; e si è ritenuto

in *El derecho a la privacidad en un nuevo entorno tecnológico*, Atti della *XX Jornadas de la Asociación de Letrados del Tribunal Constitucional*, Madrid, 2016, 123; J.L. Goñi Sein, *Nuevas tecnologías digitales, poderes empresariales y derechos del los trabajadores: ánalisis desde la perspectiva del Reglamento Europeo de protección de datos de 2016*, in *Revista de Derecho Social*, n. 78/2017, 15.

[23] Trattavasi dell'art. 22 del *Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal*, presentato il 24 novembre 2017.

[24] Corte EDU, *Lopez Ribalda c. Spagna*, 9 gennaio 2018 (ricorso n. 1874/13). Vedine il commento di G. Formici, *Lavoratori e tutela della privacy: l'evoluzione della giurisprudenza della Corte europea dei diritti dell'uomo, tra controllo della corrispondenza elettronica e videosorveglianza*, in *Osservatorio costituzionale*, 1/2018.

perciò superato il diverso orientamento del Tribunale Costituzionale spagnolo che, sulla scorta dei medesimi indici normativi generali, aveva ritenuto sacrificabile il diritto all'intimità e alla vita privata dinanzi all'interesse della parte datoriale quando la relativa limitazione potesse ritenersi adeguata, necessaria e proporzionata.

Nel corso del successivo esame parlamentare il testo della "*nueva LOPD*" ha subito modifiche che hanno comportato una significativa riformulazione (ed una diversa distribuzione) delle disposizioni in materia di privacy del lavoratore (dipendente pubblico o privato). Vale qui la pena esaminarne brevemente il contenuto, poiché intento del legislatore appare quello di inglobarvi i profili maggiormente innovativi che si correlano alla diffusione dei dispositivi digitali (come segnala anche il titolo della legge, che alla "protezione dei dati personali" affianca la "garanzia dei diritti digitali")[25].

In particolare, mentre è riconosciuto il "diritto alla disconnessione" (art. 88 del *proyecto*), la portata del *derecho a la intimidad* è estesa all'uso di dispositivi digitali aziendali nel contesto lavorativo (art. 87), essendo consentito al datore l'accesso ai contenuti derivati da tale utilizzazione al solo fine di verificare l'adempimento della prestazione nonché l'integrità dei dispositivi medesimi. Al datore è fatto obbligo di definire, con la partecipazione delle organizzazioni sindacali, criteri di utilizzazione di tali dispositivi che rispecchino un livello minimo di tutela in conformità ai parametri costituzionali e di legge; e gli è richiesto altresì di stabilire, nel caso sia consentito al lavoratore l'utilizzo anche a fini privati dei dispositivi in questione, di definire i criteri del suo accesso ai relativi contenuti, specificando inoltre quali siano gli usi autorizzati per il dipendente, le garanzie della sua riservatezza e, se del caso, i periodi durante i quali può aver luogo tale uso privato.

La videosorveglianza e le registrazioni sonore negli ambienti di lavoro sono materia dell'art. 89, che individua nella speciale disciplina giuslavoristica (e in quella della funzione pubblica) la base giuri-

[25] *Ley Orgánica de Protección de Datos de Carácter Personal y garantía de los derechos digitales*, 3/2018, del 5 dicembre, in B.O.E., e dicembre 2018. Nelle more dell'iter parlamentare della legge è stato approvato il *Real Decreto Ley* 5/2018, del 27 luglio 2018, che prevede misure urgenti di adeguamento della normativa spagnola al Regolamento europeo.

dica da cui è abilitata la parte datoriale ad esercitare il suo controllo attraverso il trattamento dei dati in tal modo raccolti. L'installazione e l'operatività dei relativi impianti è, in ogni caso, sottoposta alla valutazione della loro effettiva necessità e proporzionalità, ed è preceduta dall'informativa espressa, chiara e concisa dovuta ai lavoratori ed eventualmente anche alle loro rappresentanze.

Il diritto alla riservatezza del lavoratore, infine, è tutelato nel testo normativo con riferimento all'utilizzazione di sistemi di geolocalizzazione (art. 89), sottoposti ad analoghe condizioni quanto alle misure di protezione e agli obblighi informativi che gravano sul datore di lavoro; ed è previsto in chiusura (all'art. 90) che i "diritti digitali" possano costituire materia di contrattazione collettiva, al fine eventuale di prevedere per i lavoratori ulteriori garanzie dei diritti e delle libertà incisi dal trattamento dei loro dati personali.

5. Note conclusive

Da queste sommarie notazioni può trarsi come la materia della tutela dei dati nel rapporto di lavoro si profili, nella sua articolata complessità, come il terreno elettivo della congiunzione, o quanto meno della reciproca implicazione, degli ambiti di tutela tradizionalmente ricondotti alla *data protection* e alla privacy. Esposte schematicamente (e con inevitabile sacrificio della loro dinamicità concettuale e mutevolezza storico-geografica), la prima delle due nozioni, di elaborazione più recente, sorge con l'avvento e la diffusione delle tecnologie informatiche e si collega al controllo riconosciuto all'individuo sui propri dati in virtù del proprio diritto di autodeterminarsi; la seconda, sebbene portatrice anche di un significato generale e assorbente, tramanda l'impronta originaria di *status* negativo e suole riferirsi al potere di escludere intromissioni nella propria sfera privata[26]. La polarità tra le due nozioni è sfumata nelle

[26] S. Rodotà, *Repertorio di fine secolo*, Roma-Bari, Laterza, 1992, 189, segnala la privacy quale concetto mutevole, nella sua accezione funzionale posto in "stretta e costante correlazione" con i «mutamenti determinati dalle tecnologie dell'informazione (ma anche dalle tecnologie della riproduzione, dall'ingegneria genetica)». Con riferimento al situarsi delle nozioni di privacy e di protezione dei dati nel contesto ora caratterizzato dalla vigenza del Regolamento 2016/679, v. altresì

moderne regolamentazioni della circolazione delle informazioni a carattere personale, che assegnano all'individuo il diritto di "inseguire" i propri dati e nel contempo lo muniscono di poteri interruttivi ed inibitori rispetto al loro trattamento.

L'intersecarsi delle tutele non comporta tuttavia che ne sia identico l'oggetto. La Carta dei diritti fondamentali dell'Unione Europea distingue il diritto al rispetto delle vita privata e familiare (art. 7) da quello alla protezione dei dati personali (art. 8) e irradia i suoi effetti attraverso la trama delle fonti che la collega al diritto costituzionale euro-unitario e convenzionale, nonché mediante l'applicazione data dalle Corti alle sue previsioni[27]. Altrettanto risaputo è che il diritto alla vita privata definito dall'art. 8 Cedu è stato recepito dalla Carta dei diritti a motivo dell'applicazione dinamica ed estensiva datane dalla Corte di Strasburgo.

Tra l'una e l'altra area giuridico-semantica – vita privata e protezione dei dati – si annoda dunque una relazione certamente non di mera endiadi, ma di sostanziale complementarità. Ne ha dato prova la Corte di Giustizia nel 2014 con la sua creazione pretoria del "diritto all'oblio"[28], edificato sui fondamenti della tutela dei dati personali e della protezione della vita privata.

Questa funzionalità reciproca tra le rispettive tutele ora si profila fruttuosa nell'ambito particolare del rapporto di lavoro, a fronte della potenzialità applicativa della Cedu al piano dei rapporti tra privati e una volta che l'attuazione degli "obblighi positivi" da parte degli

F. Pizzetti, Privacy *e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, Torino, Giappichelli, 2016, 11.

[27] È appena il caso di rammentare, con massima concisione, che il nuovo art. 6 del Trattato di Lisbona richiama la Carta dell'UE, conferendole lo stesso valore giuridico dei Trattati istitutivi dell'Unione senza ampliare le competenze in questi definite (comma 1) ma investendo alla Corte di giustizia di un ruolo maggiore nella tutela dei diritti fondamentali. Inoltre, le previsioni della Carta, in forza del suo art. 51, impegnano le istituzioni e gli organi dell'UE al loro rispetto nel quadro della propria azione, e gli Stati membri nei limiti nell'attuazione del diritto dell'Unione.

[28] CGUE (Grande Sezione), sentenza del 13 maggio 2014, C131-12, *Google Spain*. Sono tuttavia numerose, com'è noto, le sentenze della Corte il cui dispositivo figura articolato sulla duplice tutela della vita privata e dei dati personali: per una rassegna può consultarsi M. Clément-Fontaine, *L'union du droit à la protection des données à caractère personnel et du droit à la vie privée*, in *Legicom*, 2017, 2, 61.

Stati vi assicuri l'effettiva protezione dei diritti convenzionali. Non a caso, la fecondità rivelata dalla fonte convenzionale ha indotto una parte degli interpreti – criticamente orientata circa le recenti riforme intervenute in ambito lavoristico – a fare affidamento sul più elevato *standard* di tutela che, permeandone il diritto comune, questa sarebbe in grado di garantire rispetto alla disciplina speciale, ora complessivamente caratterizzata, secondo tale opinione, da una recessione delle tutele già apprestate al lavoratore per effetto delle riforme legislative che negli anni recenti hanno interessato il mondo del lavoro[29].

[29] G. Bronzini-S. Giubboni, *op. cit.*, secondo cui «Diritti come quello alla privacy o alla riservatezza, certamente pensati e codificati nella Cedu (e poi anche nella Carta di Nizza) e prevalentemente attinenti al nesso autorità pubblica-libertà individuale [...], estendono così la loro portata civilizzatrice anche nella disciplina del rapporto di lavoro».

Il trattamento dei dati personali dei minori nell'Unione europea: dai codici di condotta al Regolamento 2016/679

Antonina Astone

Sommario: 1. L'art. 8 del Regolamento UE 2016/679 – 2. I rimedi a tutela del minore nel caso di mancato rispetto delle norme sul trattamento dei dati – 3. I nodi controversi: a) l'accertamento dell'effettiva età dei minori; b) La sorte dei dati già conferiti in presenza di un uso non autorizzato e la possibile estensione della disciplina sul *cyberbullismo*

1. L'art. 8 del Regolamento UE 2016/679

È noto che i dati personali sono divenuti, ormai, un "prezzo" necessario "da pagare" per accedere ai servizi della c.d. Società dell'informazione[1], di cui proprio i più giovani sono tra i maggiori fruitori ma, al contempo, le maggiori vittime.

Nonostante a livello internazionale il diritto alla riservatezza e alla protezione dei dati personali sia stato riconosciuto ai minori

[1] Per la definizione di servizio della Società dell'informazione v. art. 1, par. 1, lett. b), Dir. UE 2015/1535, ove si legge che si tratta di «qualsiasi servizio prestato normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi». Sul dato personale, come prezzo di un servizio, v. da ultimo, G. Giannone Codiglione, *I dati personali come corrispettivo della fruizione di un servizio di comunicazione elettronica e la «consumerizzazione» della privacy*, in *Dir. dell'inf. e dell'inf.*, 2017, 2, 418 ss.

dall'art. 16 della Convenzione ONU "sui diritti dell'infanzia e dell'adolescenza"[2], l'accesso ai servizi della Rete e la conseguente immissione dei dati da parte degli stessi, sono stati sguarniti di tutte quelle garanzie a cui sono subordinati gli atti e i contratti che li vedono protagonisti nel mondo reale[3].

Una materia, così delicata, come quella del trattamento dei dati personali dei minori, è stata affidata, in concreto, a codici di autoregolamentazione che, ad esempio, per i principali social network prevedevano un'età minima per accedervi, fissata a 13 anni. Si tratta di un limite di età correlato al fatto che la normativa federale statunitense, cui sono soggetti i c.d. *Over the Top*, il *Children's Online Privacy Protection Act* individua tale soglia d'età.

Nell'Unione europea, invece, in alcuni Stati membri, come l'Italia, non era stata prevista una disciplina specifica in materia, mentre, ad esempio, in Spagna, il Garante aveva fissato a quattordici anni l'età per accedere autonomamente ai social, nel rispetto della normativa nazionale che consentiva, una volta raggiunta tale età, di diffondere online i propri dati personali[4].

[2] Convenzione approvata il 20 novembre 1989, dall'Assemblea generale delle Nazioni Unite. In dottrina, cfr., in generale, M.R. Scotti, *Il diritto del minore alla riservatezza*, Napoli, Esi, 2006; P. Stanzione-G. Sciancalepore, *Minori e diritti fondamentali*, Milano, Giuffrè, 2006.

[3] Nell'ambito dello svolgimento dell'attività giornalistica, la tutela dei minori è regolata dalla c.d. Carta di Treviso, aggiornata dal Consiglio Nazionale dei giornalisti, nel testo pubblicato sulla G.U. il 13 novembre 2006. Nel settore radio televisivo v. *Codice di autoregolamentazione Tv e minori*, recepito dalla *l. 112/2004* e dal *Testo Unico dei servizi di media audiovisivi e radiofonici*, d.lgs 31 luglio 2005, n. 177 che, al cap. II, rubricato *Tutela dei minori nella programmazione audiovisiva*, all'art. 34 ha introdotto un sistema di tutela, per fasce orarie, vietando le trasmissioni che, contengono scene di violenza gratuita, efferata, o pornografiche. L'art. 35 prevede che, ogni anno, sia svolta una relazione sulla tutela dei diritti dei minori, sui provvedimenti adottati e sulle sanzioni erogate. L'Autorità per le Garanzie nelle Comunicazioni ha istituito, nel settembre 2014, l'*Osservatorio delle garanzie per i minori e dei diritti fondamentali della persona su Internet*. Cfr., in generale, *Social media e diritti. Diritto e social media*, G.L. Conti, M. Pietrangelo, F. Romano (a cura di), numero monografico di *Inf.e dir.*,1-2, 2017.

[4] *Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal* su cui, successivamente, è intervenuto il D. r. 1720/2007.

Segnando un'inversione di tendenza, il Regolamento UE 2016/679[5], con riferimento specifico proprio ai servizi della c.d. Società dell'informazione, detta una disciplina destinata al trattamento dei dati di soggetti minori[6], soprattutto al fine di superare, opportunamente, le disomogeneità esistenti fra i vari Stati membri. Ai sensi dell'art. 8, il minore, che ha compiuto i sedici anni, può validamente esprimere il consenso al trattamento dei propri dati; al di sotto di tale soglia il trattamento è illecito se non vi è il consenso da parte del genitore o di chi esercita la responsabilità genitoriale.

Originariamente, la proposta presentata dalla Commissione, che si è occupata della stesura del Regolamento, aveva fissato a 13 anni l'età minima, ma sarebbe stata messa in discussione la scelta dei sedici anni, già effettuata da alcuni ordinamenti dei Paesi membri, come la Germania[7]. Ne è scaturita una soluzione di

[5] Sul GDPR, in generale v. E. Lucchini Guastalla, *Il nuovo regolamento europeo sul trattamento dei dati personali: i principi ispiratori*, in *Contr. e impr*., 2018, 1, 106 ss.; L. Bolognini-E. Pelino-C. Bistolfi, *Il regolamento privacy europeo*, Milano, Giuffrè, 2018; G. Finocchiaro (diretto da), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, Zanichelli, 2017; Id., *Introduzione al regolamento europeo sulla protezione dei dati*, in *Nuove leggi civ. comm*., 2017, 1, 1 ss.; F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla direttiva 95/46 al nuovo Regolamento europeo*, Torino, Giappichelli, 2016; S. Sica-V. D'Antonio-G.M. Riccio (a cura di), *La nuova disciplina europea della privacy*, Padova, Cedam, 2016; M.G. Stanzione, *Il regolamento europeo sulla privacy: origini a ambito di applicazione*, in *Eur. dir. priv.*, 2016, 1249 ss.; F. Piraino, *Il regolamento generale sulla protezione dei dati personali e i diritti dell'interessato*, in *Nuove leggi civ. comm*., 2107, 2, 369 ss.

[6] Nel cons. n. 38 si afferma che proprio i minori meritano una «specifica protezione relativamente ai loro dati personali, in quanto possono essere meno consapevoli dei rischi, delle conseguenze e delle misure di salvaguardia interessate nonché dei loro diritti in relazione al trattamento dei dati personali». In particolare, sull'art. 8 F. Naddeo, *Il consenso al trattamento dei dati personali del minore*, in *Dir. dell'inf. e dell'inf*., 2018, 1, 27 ss.; G. Pedrazzi, *Minori e social media: tutela dei dati personali, autoregolamentazione e privacy*, in *Inf. e dir*., 1-2, 2017, cit., 437 ss; A. Thiene, *Segretezza e riappropriazione di informazioni di carattere personale: riserbo e oblio nel nuovo regolamento europeo*, in *Nuove leggi civ. com*., 2017, 2, 410 ss.; G. Spoto, *Disciplina del consenso e tutela del minore*, in S. Sica-V. D'Antonio-G.M. Riccio (a cura di), *La nuova disciplina europea della privacy*, cit., 111 ss.

[7] L'innalzamento del limite d'età, previsto dall'art. 8 del GDPR, è stato realizzato con un emendamento del 4 dicembre 2015 n.14902/15.

compromesso sì da spingere ad aggiungere, in sede di redazione dell'art. 8, n. 1, par. 2, la possibilità di deroga da parte dei singoli Stati, che possono stabilire un'età diversa non inferiore, comunque, a tredici anni. In tal modo, l'obiettivo dell'armonizzazione della disciplina in materia non appare centrato, sebbene fosse auspicabile, soprattutto in considerazione della circolazione, senza confini spaziali dei dati e tenuto conto del loro trasferimento all'esterno dell'Unione Europea, fattispecie disciplinata nel cap. V, dagli artt. 44 e ss., del Regolamento[8].

Volgendo lo sguardo a quei Paesi, che hanno già adattato la loro legislazione interna alle prescrizioni del Regolamento, emerge, infatti, che la possibilità di deroga ha vanificato quell'esigenza di omogeneità che era alla base della normativa europea. Così, in Germania è stata approvata una disciplina di adeguamento al GDPR, che ha inciso sulla normativa previgente in materia di protezione dei dati personali, il c.d. *Bundesdatenschutzgesetz*, che ha riconfermato la soglia dei sedici anni, mentre in Austria è stato previsto il limite di quattordici anni e in Spagna, la proposta di *ley General de Protección de Datos Personales en Posesión de Sujetos Obligados*, pubblicata il 26 gennaio 2017, ha abbassato ulteriormente la soglia a tredici anni[9].

In Italia, per esprimere il c.d. consenso digitale, l'art. 2-*quinquies*, comma 1, del dlgs 101/2018, recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento 2016/679, stabilisce il limite di quattordici anni, specificando, al comma 2, che il titolare del trattamento deve redigere, con linguaggio particolarmente chiaro e semplice, conciso ed esaustivo, facilmente accessibile e comprensibile dal minore, al fine di rendere significativo il consenso prestato da quest'ultimo, le informazioni e le comunicazioni relative al trattamento che lo riguardi.

[8] V. in generale sul tema G. Resta-V. Zeno-Zencovich, (a cura di), *La protezione transnazionale dei dati personali dai «Safe Harbour Principles» al «Privacy Shield»*, Roma, Roma TrE-press, 2017.

[9] In Germania la legge di adeguamento al GDPR è entrata in vigore il 5 luglio 2017; in Austria il 5 luglio 2017 è stato approvato il *DatenschutzAnpassungsgesetz* 2018; per una comparazione dei dati relativi alla legislazione a protezione dei minori, rispetto all'uso dei social, vigente nei vari Stati della UE v. *www.Betterinternetforkids.eu*

La fissazione della soglia a quattordici anni, certamente condivisibile, è stata piuttosto dibattuta, in quanto la bozza di decreto, che era stata presentata e sottoposta al parere del Garante *privacy*, individuava a sedici anni, l'età per esprimere autonomamente il consenso digitale. L'opzione, in favore della soglia più alta, aveva determinato, a sua volta, una modifica rispetto a quanto contenuto nello schema del decreto legislativo, elaborato da una Commissione di tecnici, istituita presso il Senato[10], che aveva scelto il limite di quattordici anni. Il testo dell'art. 2-*quinquies* della bozza di decreto legislativo, contente il limite più alto, era stato oggetto, tuttavia, di una serie di osservazioni critiche da parte dell'Autorità garante della protezione dei dati personali che, nel parere n. 312, reso il 22 maggio 2018, ha sottolineato come la scelta non appariva coerente con altre disposizioni dell'ordinamento che individuano, invece, a quattordici anni il limite di età consentito per esercitare determinati atti giuridici[11]. Si pensi, fra le tante, alle disposizioni in materia di *cyberbullismo*, di cui alla l. n. 71/ 2017[12], che consentono al minore ultraquattordicenne di esercitare i diritti previsti a propria tutela, *ex* art. 2, comma 1, o al diritto del minore, che ha raggiunto i quattordici anni, di manifestare il proprio consenso all'adozione, ai sensi dell'art. 7, co. 2, l. n. 184/1983. Sottolineava, opportunamente, l'*Authority* che sembrerebbe, pertanto, «incoerente ammettere il quattordicenne a prestare il proprio consenso per essere adottato, ma non per iscriversi a un *social network*».

[10] Lo schema è stato redatto da una Commissione di tecnici, presieduta da G. Finocchiaro; la norma di cui all'art. 2-*quinquies*, come si legge nella relazione alla bozza di decreto, è volta a tutelare il minore in quei contesti virtuali ove risulta maggiormente esposto a causa di una minore consapevolezza dei rischi insiti nella «rete». La disposizione, infatti, rende l'operatore consapevole del fatto che minori possono accedere ai servizi, e quindi richiede di apprestare le relative misure.

[11] Sul tema, in generale, v. A. Falzea, voce *Capacità (Teoria generale)*, VI, in *Enc. dir*., Milano, Giuffrè, 1960; per una disamina di varie ipotesi normative in cui si riconosce al minore la capacità di esprimersi su scelte che riguardano la propria persona v. F. Giardina, *«Morte» della potestà e «capacità» del figlio*, in *Riv. dir. civ*., 6, 2016, 1615 ss.; A. Thiene, *Riservatezza e autodeterminazione del minore nelle scelte esistenziali*, in *Fam. e dir*., 2017, 2, 172 ss. In giurisprudenza Trib. Roma, 23 dicembre 2017 ove si ricorre alla distinzione d'oltralpe tra *petits* e *grands enfants*.

[12] R.M. Colangelo, *La legge sul* cyberbullismo. *Considerazioni informatico-giuridiche e comparatistiche*, in *Inf. e dir*., 2017, 1-2, cit., 397 ss.

Cogliendo tali rilievi, si è proceduto ad abbassare, rispetto a quella minima legale, la soglia a quattordici anni, effettuando così una scelta che, sebbene formalmente meno garantista, appare più aderente alla realtà concreta, in cui le statistiche evidenziano una tendenza ad un uso, sempre più precoce, dei nuovi mezzi di comunicazione e dei relativi servizi.

2. I rimedi a tutela del minore nel caso di mancato rispetto delle norme sul trattamento dei dati

La fissazione di un'età inferiore a quella di sedici anni, per potere esprimere autonomamente il c.d. consenso digitale, oltre che consentire quel raccordo, che appare necessario, con la normativa in materia di *cyberbullismo*[13], sarebbe controbilanciata dal fatto che il Regolamento appresta una serie di rimedi in cui il consenso[14] appare solo uno dei tasselli che compongono il puzzle dal quale si ricava, nella sua globalità, la tutela del titolare dei dati. Con un cambiamento di prospettiva rispetto alla normativa previgente, si prevede l'adozione di «misure tecniche e organizzative adeguate» per garantire il rispetto dei diritti e delle libertà delle persone fisiche, rispetto al trattamento dei dati personali. Si introduce l'obbligo di analisi preventiva dei rischi, in ordine alle operazioni di trattamento il c.d. *Data Protection Impact Assessment*[15]: fondamentale, *ex* art. 25, pertanto, sarà l'approccio di *Privacy* "*by design*" e, quindi,

[13] S. Bolognini, *Il cyberbullismo come volto demoniaco del potere digitale e le (possibili) politiche del diritto antidoto*, Milano, Giuffrè, 2017.

[14] Sul consenso V. Cuffaro, *Il consenso dell'interessato*, in V. Cuffaro-V. Ricciuto (a cura di), *La disciplina del trattamento dei dati personali*, Giappichelli, Torino, 1997, 201 ss.; S. Sica, *Il consenso al trattamento dei dati. Metodi e modelli di qualificazione giuridica*, in *Riv. dir. civ.*, II, 2001, 621 ss.; F. Cardarelli-S. Sica-V. Zeno-Zencovich (a cura di), *Il codice dei dati personali*, Milano, Giuffrè, 2004, 11 ss.; S. Patti, *Commento all'art. 23*, in C.M. Bianca-F.D. Busnelli (a cura di), *La protezione dei dati personali. Commentario al d.lgs. 30 giugno 2003*, n. 196, t. 1., Padova, Cedam, 2007, 553.

[15] M.G. Stanzione, *Genesi ed ambito di applicazione*, in S. Sica-V. D'Antonio-G.M. Riccio (a cura di), *La nuova disciplina europea della privacy*, cit., 21 ss., che sottolinea una possibile estensione dei c.d. principi di prevenzione e precauzione alla protezione dei dati personali.

di progettazione del trattamento dei dati, in modo da proteggerli fin dall'architettura del disegno aziendale e salvaguardarli, altresì, anche nei casi di impostazione predefinita, così come sintetizzato nel cons. n. 78.

Con specifico riferimento ai rimedi accordati in favore dei minori sembrano emergere due diversi piani: il primo è legato al fatto che l'applicazione del Regolamento, lascia impregiudicata la valutazione in ordine alla formazione, validità, ed efficacia dei contratti, alla cui stipula è connesso il trattamento dei dati personali, ai sensi dell'art. 8 n. 3[16]. Ne consegue che, nonostante la conformità dell'acquisizione dei dati alle prescrizioni del Regolamento, i contratti stipulati saranno pur sempre soggetti alla disciplina generale contrattuale ed a quella specifica, a seconda della tipologia[17].

Il secondo è direttamente correlato alla violazione della disciplina regolamentare: in primo luogo dovrà essere valutata la modalità di acquisizione del consenso, che non è più concepito come un adempimento di natura formale e, falsamente garantista, spesso aggirato dagli stessi minori nella Rete. Si richiede, infatti, *ex* art. 7, un consenso da un verso, "inequivocabile", che consenta al titolare di dimostrare che l'interessato ha voluto effettivamente il trattamento dei dati, dall'altro "informato" con il richiamo ad una formula analoga a quella contenuta nell'art. 5 del Codice del consumo[18]. In questo senso, fondamentale è quanto statuito dall'art. 12, n. 1, a proposito di soggetti deboli, come i minori, ove si precisa che l'informazione deve essere resa accessibile, attraverso un linguaggio chiaro e semplice che, come specifica il considerando n. 58, «il minore possa capire facilmente». Ma il consenso, come precedentemente sottolineato, si inserisce in un contesto di previsioni che vanno dal diritto all'accesso ai sensi dell'art. 15 al risarcimento del danno, *ex* art. 82, dalle

[16] F.D. Busnelli, *Capacità e incapacità di agire del minore*, in *Dir. fam. pers*., 1982, 54 ss., ora in *Persona e famiglia*, Pisa, Pacini, 2017, 218ss.

[17] In generale C. Perlingieri, *Profili civilistici dei social networks*, Napoli, Esi, 2014; specificatamente A. Spangaro, *Tutela dei minori e delle fasce deboli*, in G. Finocchiaro-F. Delfini (a cura di), *Diritto dell'informatica*, Torino, Utet, 2014, 219 ss.; E. Andreola, *Gli acquisti* on line *del minore tra invalidità dell'atto e responsabilità dei genitori*, in *Contr. e impr.*, 2018, 2, 953 ss.

[18] S. Sorrentino, *sub art 5*, in V. Cuffaro (a cura di), *Codice del consumo*, con il coordinamento di A. Barba-A. Barenghi-L. Pasquini, Milano, Giuffrè, 2015, 46 ss.

quali emerge quella dimensione superindividuale che la protezione dei dati ha assunto[19].

La legittimazione ad agire spetterà anche all'adolescente che, potendosi iscrivere da solo ai social network, si presume sia dotato anche di quel sufficiente grado di maturazione cognitiva per invocare i rimedi posti a tutela della riservatezza dei suoi dati, con l'esclusione di quelli prettamente giurisdizionali, vista l'incapacità di stare in giudizio dei minori[20]. La rapidità dei tempi impressi per rimediare ad eventuali violazioni, gli elevati importi sanzionatori introdotti dall'art. 83, sembrano dare maggiore spessore a molti di questi strumenti di tutela che, pur previsti dalla disciplina previgente, sono stati di fatto poco attuati[21].

3. I nodi controversi

a) L'accertamento dell'effettiva età dei minori

Il corso intrapreso dal GDPR, diretto ad una maggiore salvaguardia dell'interesse del minore[22], si pone in linea con l'art. 17 della Convenzione ONU che, dopo aver premesso l'importanza esercitata dai mass media, suggerisce agli Stati aderenti «l'elaborazione di principi direttivi appropriati, destinati a proteggere il minore dalle informazioni e dai materiali che possono nuocere al suo benessere».

Tuttavia sembrano sorgere almeno due interrogativi di ordine pratico: il primo riguarda le modalità che dovranno essere seguite

[19] La differenza tra la visione individualistica della riservatezza, che emerge dall'art. 7 e la visione super-individualistica che risulta dall'art. 8 della Carta di Nizza, è tracciata da S. Rodotà, *Il diritto di avere diritti*, Roma-Bari, Laterza, 2012, 397; G. Resta, *Il diritto alla protezione dei dati personali*, in F. Cardarelli-S. Sica-V. Zeno-Zencovich (a cura di), *Il codice dei dati personali*, cit., 26 ss.

[20] A. Thiene, *Riservatezza e autodeterminazione del minore nelle scelte esistenziali*, in *Fam. e dir*., 2017, 174.

[21] È da segnalare che è in corso di elaborazione la proposta di *Regolamento su privacy e comunicazioni elettroniche*, riguardo al trattamento dei dati personali e la tutela della vita privata, nel settore delle comunicazioni elettroniche, destinata ad abrogare la Direttiva 2002/58, c.d. «Direttiva e Privacy» ed apportare modifiche al d.lgs. 259/2003, il c.d. Codice delle comunicazioni elettroniche, al fine di creare un raccordo con il GDPR.

[22] Su cui, da ultimo, per un quadro d'insieme v. V. Scalisi, *Il superiore interesse del minore ovvero il fatto come diritto*, in *Riv. dir civ*., 2018, 2, 405 ss.

per accertare l'età dei minori e il secondo attiene alla sorte dei dati, il cui trattamento non è più autorizzato, e che sono stati già acquisiti.

In relazione al primo profilo, assume un valore fondamentale la responsabilizzazione imposta al titolare del trattamento[23]. Ai sensi dell'art. 8, n. 2, questi si deve adoperare «in considerazione delle tecnologie disponibili» e «in ogni modo ragionevole» per accertarsi se, effettivamente, il consenso sia prestato dal genitore. In questo senso non potrà più essere ritenuto assolto il compito di protezione dei dati personali dei minori, per mezzo dell'invio di una mail alla casella di posta del genitore, il cui indirizzo è, spesso fornito dai minori stessi privi, a loro volta, di un proprio account di posta elettronica, in cui si comunica l'avvenuta iscrizione. Una notifica, *ex post*, con cui si dà atto della creazione di un profilo *social*, senza che sia sorretta da un'adeguata e chiara informazione sull'eventuale modalità di recesso, connotato da procedure, spesso contorte, di *opt-out*, come è accaduto fino all'entrata in vigore del Regolamento, sarà da considerarsi invalida.

Per ovviare all'elusione della normativa da parte dei minori stessi, sarebbe opportuno intervenire, attraverso l'inoltro di una mail diretta ad avvisare il genitore dell'eventuale iscrizione sul social del figlio e del conseguente trattamento dei dati personali. Questo adempimento, che avrebbe la funzione di pubblicità notizia, consentirebbe, a chi esercita la responsabilità genitoriale, di venire a conoscenza dell'utilizzo del social da parte del figlio, soprattutto qualora non ha raggiunto l'età minima richiesta ed ha dichiarato un'età falsa; se, invece, la soglia d'età è effettivamente raggiunta, tale notifica potrebbe consentire al genitore di essere edotto del fatto, e valutare se non vi siano ragioni che possano pregiudicare il superiore interesse del minore, di fronte alle quali può essere espresso un valido diniego. Questo adempimento è importante anche alla luce della responsabilità dei genitori, *ex* art. 2048 c.c., in ordine ai comportamenti connessi alla navigazione sui social [24]. In USA, dal 2015, per

[23] Sul c.d. principio di *accountability* v. A. Mantelero, *Responsabilità e rischio nel Reg. UE 2016/679*, in *Nuove leggi civ. comm.*, 2017, 1, 144 ss.

[24] Il Trib. Sulmona, con una decisione del 10 Aprile 2018, ha condannato al risarcimento dei danni i genitori dei minorenni che avevano diffuso sui social una foto lesiva della riservatezza di una loro coetanea, ritenendoli responsabili per *culpa in vigilando* ed *educando*.

verificare se il consenso sia prestato effettivamente dai genitori, si fa ricorso ad una procedura, che si spera venga estesa globalmente, basata su una comparazione fra una foto personale identificativa, contenuta ad esempio in una *id card*, verificata prima con tecniche di riconoscimento facciale biometrico e un *selfie:* attraverso un processo di validazione, molto rapido, i dati acquisiti vengono, poi, eliminati definitivamente con tecniche di cancellazione sicura[25].

Tutte queste attività dovrebbero, in teoria, scongiurare l'ingresso nei social di minori con un'età inferiore a quella legale ma, nella pratica, debellare l'elusione della normativa si rivela piuttosto complesso.

b) La sorte dei dati già conferiti dai minori, in presenza di un uso non autorizzato, e la possibile estensione della disciplina sul *cyberbullismo*

Un secondo aspetto, non trascurabile, attiene alla sorte dei dati, già immagazzinati, di soggetti minori d'età, che non sono più autorizzati al profilo social. Sulla base dell'art. 17 del GDPR, l'interessato ha diritto di ottenerne, senza ingiustificato ritardo, la cancellazione, da parte del titolare del trattamento, quando ricorrono una serie di condizioni: ad esempio, nell'ipotesi in cui siano stati trattati illecitamente, quindi se i dati si riferiscono ad un minore di età inferiore a quella per esprimere personalmente il consenso, che non sia stato autorizzato dai genitori[26]. In tal caso, dunque, il titolare dovrà procedere alla loro cancellazione e astenersi da ogni successivo trattamento degli stessi, avvalendosi, ai sensi del par. 2 dell'art. 17, della «tecnologia disponibile». Il campo di applicazione del c.d. diritto all'oblio è più esteso di quello di cui all'art. 7, comma 3, lett. b) del Codice Privacy, che prevede già il diritto di chiedere la cancellazione

[25] G.M. Riccio, *Data Protection officer e altre figure*, in S. Sica-V. D'Antonio-G.M. Riccio (a cura di), *La nuova disciplina europea della privacy*, cit., 33 ss.

[26] Sul peso esercitato dal condizionamento tecnologico sulla concreta attuazione dei diritti. v. D. Poletti, *Il c.d. diritto alla disconnessione nel contesto dei «diritti digitali»*, in *Resp. civ. e prev.*, 2017, 1, 8 ss. che sottolinea come tra i nuovi diritti, che la Rete ha fatto emergere, vi è anche quello alla c.d. disconnessione, diritto nato nel contesto lavoristico, inteso come «il diritto alla irreperibilità, a non essere cioè fatto oggetto di richieste e a non doverle soddisfare fuori dell'orario di lavoro o durante le ferie».

dei propri dati, in quanto l'eliminazione, secondo l'art. 17, può essere esercitata anche dopo la revoca del consenso al trattamento. Tale diritto, come è specificato nel cons. 65, è rilevante se l'interessato ha prestato il proprio consenso quando era minore e, quindi, privo di quel livello adeguato di maturazione per comprendere i rischi derivanti dal trattamento, e vuole successivamente eliminarli da Internet[27].

La prospettiva rimediale, prevista dal Regolamento in ordine al c.d. diritto all'oblio, ha una portata generale e può coordinarsi con la disciplina specifica, introdotta con la l. 29 maggio 2017, n. 71: proprio la diffusione dei casi di *cyberbullismo* ha determinato la presa di posizione netta da parte del legislatore europeo, portando ad una definizione del trattamento dei dati personali di soggetti minori. Sulla base dell'art. 2 della l. 71/2017, le vittime di episodi di *cyberbullismo*, se hanno già raggiunto i quattordici anni, o il soggetto esercente la responsabilità, possono adire il titolare del trattamento o il gestore del sito internet o del social media, al fine di ottenere «l'oscuramento, la rimozione o il blocco di qualsiasi altro dato personale del minore, diffuso nella rete internet». In caso di mancata risposta, entro quarantotto ore o, qualora non sia stato possibile identificare il responsabile, l'interessato ha diritto di rivolgersi al Garante per la protezione dei dati personali che, se ne ravvisa i presupposti, provvede al blocco.

I tempi ristretti, finalizzati ad assicurare una tempestiva tutela alla vittima, potrebbero essere estesi anche in tutti i casi in cui si verifichi un trattamento di dati di un soggetto minore, che sia stato

[27] S. Rodotà, *Il diritto di avere diritti*, cit., 406 lo ha definito come «il diritto a liberarsi dell'oppressione dei ricordi, da un passato che continua ad ipotecare pesantemente il presente», in quanto «il passato non può essere trasformato in una condanna che esclude ogni riscatto»; sul bilanciamento tra il diritto di cronaca e il diritto all'oblio Corte eur. giust., V, 28 giugno 2018 *M.L. e W.W.* c. Germania, ric. 60798-65599/10; Cass. civ., sez. I, ord. 20 marzo 2018, n. 6919; Corte eur. giust., Gr. sez., C-131/12, 13 maggio 2014, *Costeja Gonzales* e *Agencia Espanola de proteccion de datos c Google Spain SL* e *Google Inc*., in *Foro it*., 2014, IV, con nota di A. Palmieri-R. Pardolesi, 317ss., in *Giur.it*., 2014, 1323 ss.; C. Bartolini-L. Siry, *The right to be forgotten in the contest of the data subject*, in *Computer Law & Security Review*, 2016, 218 ss.; G. Resta-V. Zeno-Zencovich (a cura di), *Il diritto all'oblio su Internet dopo la sentenza Google Spain*, Roma, Roma-TrEpress, 2015.

revocato o effettuato illecitamente. Ne consegue, come in precedenza sottolineato, che è inevitabile un raccordo tra il decreto legislativo di adeguamento al Regolamento e la normativa in materia di *cyberbullismo*, reso possibile dall'individuazione di un unico limite d'età.

Ma è interessante sottolineare che il contrastato al *cyberbullismo* «in tutte le sue manifestazioni» deve concretizzarsi in «azioni a carattere preventivo», assicurando interventi nell'ambito delle istituzioni scolastiche «nei confronti dei minori coinvolti, sia nella posizione di vittime che in quella di responsabili di illeciti», senza alcuna distinzione d'età. Non si deve trascurare, invero, di considerare come attuare il diritto all'oblio in rete è quasi impossibile, poiché un'immagine, un video, una notizia, possono essere ripresi e diffusi in maniera incontrollabile.

Ne consegue che l'attività di formazione ed educazione, a sostegno di persone deboli, come i minori, non può che giocare un ruolo fondamentale, per fare acquisire loro quella consapevolezza dei rischi connessi al trattamento dei dati e favorirne una gestione consapevole[28].

Ma, come Timothy John Barners Lee ha scritto[29], nel denunziare l'eccessivo potere nelle mani di Google e Facebook, non solo i minori ma soprattutto gli adulti, accettando «termini e condizioni lunghi e confusi», fondamentalmente dimostrano di dare poca importanza a che alcune informazioni vengano raccolte in cambio di servizi gratuiti. «Nei regimi repressivi, è facile vedere il danno che può essere causato: i blogger, gli avversari politici possono essere arrestati, uccisi o monitorati... Ma anche nei paesi democratici il pericolo cui è soggetta la libertà di autodeterminazione è forse più forte, in quanto il suo condizionamento avviene in maniera strisciante». Queste parole suonano come una profezia perché precedono, di pochi giorni, il caso di *Cambridge analytica*[30].

[28] A. Mantelero, *Adolescenti e privacy nella scuola ai tempi di youtube*, in *Nuova giur. civ. comm.*, 2011, 139 ss.

[29] L'analisi di Tim Barners-Lee, il ricercatore inglese che, nel 1991, mise online il primo sito web si può leggere sul sito *www.theguardian.com*, 12 marzo 2018.

[30] Nel marzo 2018, l'Agenzia Cambridge analytica, società inglese di Big Data, secondo un'inchiesta partita dal *New York Times*, si è avvalsa di Facebook per raccogliere i profili di milioni di persone e, sulla base delle loro preferenze e gusti, ha usato questi dati, dapprima per favorire la c.d. Brexit e, poi per sostenere l'elezione di Trump. L'attività è stata basata sugli studi nel campo di D. Stil-

Se l'attività di profilazione, che il Regolamento, non a caso, ha cercato di circoscrivere, attraverso norme dirette a limitare l'incontrollato uso dei dati che è stato fatto, incomincia a rispondere oltre che a logiche di mercato anche a scopi politici, il rischio che si corre è elevatissimo, perché a venire in gioco è la libertà stessa dell'individuo e, quindi, la democraticità di un paese, con effetti che sono ancora più devastanti se si agisce sulla capacità di autodeterminazione dei minori, posti in un'intrinseca condizione psico-fisica di vulnerabilità[31].

lwell e M. Kosinski, sulla c.d. psicometria, scienza che analizza la personalità di qualcuno quantificandola: C. Segalin-F. Celli-L. Polonio-M. Kosinski-D.J. Stillwell-N. Sebe-M. Cristani-B. Lepri, *What your Facebook profile picture reveals about your personality*, *Proceedings of the 2017 ACM on Multimedia Conference*, 2017, 460 ss.

[31] In generale F. Antinucci, *L'algoritmo al potere*, Roma-Bari, Laterza, 2009; S. Rodotà, *Il diritto di avere diritti*, cit., 398.

Il diritto all'oblio dell'articolo 17 Regolamento (UE) 2016/679: una grande novità? Una denominazione opportuna?

Gabriele Rugani

Sommario: 1. L'articolo 17: una grande novità? – 1.1. L'articolo 17 del Regolamento e l'articolo 12 lettera b) della Direttiva – 1.2. L'articolo 17 del Regolamento e la sentenza Google Spain – 2. "Diritto all'oblio": una denominazione opportuna? – 2.1. Le ipotesi in cui l'utilizzo dell'espressione "diritto all'oblio" è giustificato – 2.2. Le ipotesi in cui l'articolo 17 consente la cancellazione – Bibliografia

1. L'articolo 17: una grande novità?

Una delle novità del Regolamento (UE) 2016/679 che ha dato luogo ad un ampio dibattito è il diritto all'oblio, sancito dall'articolo 17. Ricordiamo che, in precedenza, la materia era disciplinata dall'articolo 12 lettera b) della Direttiva 95/46/CE; inoltre, del diritto all'oblio si era occupata anche la sentenza *Google Spain SL*, *Google Inc.* contro *Agencia Española de Protección de Datos (AEPD)*, *Mario Costeja González*, nota più semplicemente come *Google Spain*, pronunciata dalla Corte di giustizia dell'Unione europea nel 2014[1].

La principale questione che si intende affrontare è se l'articolo 17 sia o meno un elemento innovativo rispetto alla disciplina precedente. Detto in altri termini, se esso rappresenti un autentico pro-

[1] Corte giust., sentenza 13 maggio 2014, causa C-131/12.

gresso per il diritto all'oblio. A tal fine occorre dunque raffrontare la disposizione in esame prima con la Direttiva 95/46/CE, poi con la giurisprudenza *Google Spain*.

1.1. L'articolo 17 del Regolamento e l'articolo 12 lettera b) della Direttiva

1.1.1. Le criticità dell'articolo 12 lettera b) della Direttiva

Il primo confronto da attuare è quello tra l'articolo 17 e la soluzione normativa precedente. In base all'articolo 12 lettera b) della Direttiva, gli Stati membri garantiscono a qualsiasi persona interessata il diritto di ottenere la cancellazione «dei dati il cui trattamento non è conforme alle disposizioni della presente direttiva, in particolare a causa del carattere incompleto o inesatto dei dati».

Innanzitutto, occorre evidenziare la scelta terminologica operata dal legislatore europeo: non si parla di "diritto all'oblio", ma solo di "diritto alla cancellazione".

Inoltre, neppure lo stesso diritto alla cancellazione pare avere un ruolo di particolare rilievo: a conferma di ciò, basti pensare che nessuno dei Considerando del preambolo fa riferimento a tale diritto e che lo stesso articolo 12 è rubricato esclusivamente "Diritto di accesso". Nella Direttiva, quindi, il diritto alla cancellazione appare decisamente sottovalutato, ma non dobbiamo certo stupircene. Infatti, nella prima metà degli anni '90, l'uso di Internet è ancora agli albori: non è certo possibile prevedere quale diffusione avranno i dati personali grazie alla rete e dunque quanto sarà importante, e allo stesso tempo difficile, ottenerne la cancellazione.

Nel secondo decennio del XXI secolo la situazione appare però completamente mutata. Come afferma la stessa Commissione europea nella Relazione alla Proposta di Regolamento, in virtù delle tecnologie attuali «la portata della condivisione e della raccolta di dati è aumentata in modo vertiginoso»[2]. Se l'interessato, dopo che i dati in questione sono stati condivisi su scala così ampia, intende chiederne la cancellazione, si pongono due interrogativi: in quali casi possa ottenerla e da parte di chi.

È evidente che una disposizione scarna come l'articolo 12 lettera b) della Direttiva non possa più rispondere a tali esigenze, per due

[2] COM (2012) 11 def.

motivi essenziali. In primo luogo, non definisce in modo sufficientemente chiaro quelli che sono i presupposti per l'esercizio del diritto alla cancellazione. In secondo luogo, prevede esclusivamente la possibilità di rivolgersi al titolare del trattamento e di ottenere la cancellazione da parte di quest'ultimo. Ma, poiché i dati pubblicati in rete sono messi a disposizione di un numero illimitato di ulteriori titolari, ottenere la cancellazione solo da parte del titolare "originario" può giovare ben poco all'interessato.

1.1.2. Le soluzioni dell'articolo 17 del Regolamento.

L'articolo 17 del Regolamento, rubricato "Diritto alla cancellazione ('diritto all'oblio')", cerca di rispondere, rispettivamente coi suoi paragrafi 1 e 2, a tali problematiche.

Il primo paragrafo definisce con grande accuratezza e puntualità i presupposti del diritto. Infatti, in base a tale disposizione, «l'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti [...]», elencati dalla lettera a) alla lettera f). In modo particolare, la lettera a) riguarda il caso in cui i dati personali non siano più necessari per le finalità per cui sono stati raccolti; la lettera b) la revoca del consenso su cui si basa il trattamento; la lettera c) l'esercizio del diritto di opposizione *ex* articolo 21 del Regolamento da parte dell'interessato; la lettera d) il caso in cui i dati siano stati trattati illecitamente; la lettera e) l'adempimento di un obbligo legale previsto dal diritto dell'Unione europea o dal diritto nazionale; la lettera f) il caso in cui i dati personali siano stati raccolti nel contesto dell'offerta diretta di servizi della società dell'informazione ai minori.

Il secondo paragrafo, invece, recita: «Il titolare del trattamento, se ha reso pubblici dati personali ed è obbligato, ai sensi del paragrafo 1, a cancellarli, tenendo conto della tecnologia disponibile e dei costi di attuazione adotta le misure ragionevoli, anche tecniche, per informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali». L'importanza di tale paragrafo è enfatizzata anche da uno dei Considerando del preambolo del Regolamento, il numero 66, che recita: «Per rafforzare il

"diritto all'oblio" nell'ambiente online, è opportuno che il diritto di cancellazione sia esteso in modo tale da obbligare il titolare del trattamento che ha pubblicato dati personali a informare i titolari del trattamento che trattano tali dati personali di cancellare qualsiasi link verso tali dati personali o copia o riproduzione di detti dati personali. Nel fare ciò, è opportuno che il titolare del trattamento adotti misure ragionevoli tenendo conto della tecnologia disponibile e dei mezzi a disposizione del titolare del trattamento, comprese misure tecniche, per informare della richiesta dell'interessato i titolari del trattamento che trattano i dati personali». Dunque, l'articolo 17 paragrafo 2 sancisce l'obbligo in capo al titolare di adottare misure per informare gli altri titolari della richiesta di cancellazione. In questo modo, ancorché rintracciare tutti gli ulteriori titolari sia in alcune circostanze estremamente difficile, la cancellazione avrà una portata indubbiamente più ampia, e maggiori saranno i benefici che l'interessato potrà ottenere.

In conclusione, alla domanda che ci siamo posti, ossia se l'articolo 17 del Regolamento, confrontato con il dato testuale della Direttiva 95/46/CE, risulti davvero essere un elemento innovativo, la risposta ci pare debba essere affermativa. Grazie a quanto disposto dal paragrafo 1, ma ancor di più dal paragrafo 2, la posizione degli interessati risulta essere indubbiamente rafforzata.

1.2. L'articolo 17 del Regolamento e la sentenza Google Spain

1.2.1. L'ampia tutela della sentenza Google Spain

Diversamente, alla luce della sentenza *Google Spain*, alcuni elementi dell'articolo 17 non sembrano avere una portata altrettanto innovativa.

Nella sentenza *Google Spain* il diritto all'oblio riceve, infatti, una tutela amplissima. In primo luogo, tale diritto prevale sul diritto alla libertà di espressione e di informazione: in uno dei suoi passaggi più criticati, la pronuncia della Corte di Lussemburgo afferma che il diritto alla vita privata e il diritto alla protezione dei dati di carattere personale, sanciti rispettivamente dagli articoli 7 e 8 della Carta di Nizza, prevalgono in linea di principio "sull'interesse" del grande pubblico a trovare le informazioni in occasione di una ricerca concernente il nome dell'interessato stesso. Merita di essere evidenziata anche la terminologia utilizzata nella sentenza: i "diritti" degli articoli 7 e 8 della Carta dei diritti fondamentali dell'Unione europea

vengono messi a confronto con un "interesse"; ma in realtà è anch'esso un vero e proprio "diritto", tutelato nella fattispecie dall'articolo 11 della stessa Carta di Nizza. Il diritto alla libertà di espressione e di informazione, dunque, viene declassato anche dal punto di vista terminologico[3] e il timore di molti è che anche le autorità e i giudici nazionali, proprio facendo riferimento alla sentenza *Google Spain*, assegnino a tale diritto un ruolo di secondo piano[4]. Tutto ciò, ovviamente, a vantaggio del diritto all'oblio.

In secondo luogo, il diritto all'oblio può essere fatto valere persino nei confronti del gestore di un motore di ricerca. Secondo la Corte di giustizia, infatti, gli interessati possono rivolgersi direttamente al gestore del motore di ricerca per ottenere la soppressione, dall'elenco dei risultati che si possono ottenere effettuando una ricerca nominativa, dei link verso le pagine web degli archivi pubblicate da terzi e contenenti il loro nome; e ciò anche nel caso in cui i dati in questione non vengano previamente o simultaneamente cancellati dalle pagine web di cui trattasi ed eventualmente anche quando la loro pubblicazione su tali pagine web sia di per sé lecita. Anche tale aspetto presenta notevoli criticità: di fronte ad un numero ingestibile di richieste di deindicizzazione, i motori di ricerca potrebbero dimostrarsi particolarmente propensi ad accoglierle, anche se prive di fondamento, temendo le spese del relativo contenzioso in caso di mancato accoglimento; potrebbero essere così rimossi interi bacini di ricordi e segmenti di passato in maniera pressoché randomica e non derivante da un bilanciamento degli interessi in gioco. A parere di molti, sarebbe stato ben più saggio, da parte del giudice di Lussemburgo, affidare il vaglio delle istanze di deindicizzazione direttamente ai garanti nazionali; o in alternativa, sarebbe stato possibile prevedere l'interpello necessario di questi ultimi da parte dei motori di ricerca: il risultato sarebbe stato quello di evitare *a priori* il rischio di una rimozione indiscriminata dei link verso qualsiasi contenuto oggetto di un'opposizione, garantendo l'obiettività di giudizio e l'ef-

[3] G. Brock, *The right to be forgotten – Privacy and the media in the Digital Age*, London-New York, I.B. Tauris & Co. Ltd, 2016, 43.

[4] S. Kulk-F.Z. Borgesius, *Freedom of Expression and "Right to be Forgotten" Cases in the Netherlands after Google Spain*, in *European Data Protection Law Review*, 2015, 113 ss.

fettivo contemperamento degli interessi in contrapposizione[5]. Ma al di là di queste considerazioni, è certo che quella individuata dalla sentenza *Google Spain* sia una soluzione particolarmente favorevole per l'interessato.

1.2.2. Gli elementi dell'articolo 17 che ne limitano la portata innovativa

Nel Regolamento, invece, la situazione appare completamente diversa.

Innanzitutto, il diritto all'oblio è sottoposto a condizioni; o meglio, l'obbligo del titolare del trattamento, sancito dal paragrafo 2, di adottare le "misure ragionevoli" per informare gli altri titolari della richiesta di cancellazione, è sottoposto alla c.d. condizione "tecnologica" (si deve infatti tenere conto "della tecnologia disponibile") e alla c.d. condizione "finanziaria" (si deve infatti tenere conto dei "costi di attuazione"). Tali condizioni rappresentano strumenti con cui operare in concreto un bilanciamento: ciò significa che potrebbero condurre a legittimare un diniego di tutela da parte del titolare del trattamento, diniego che non dipende assolutamente dalla posizione dell'interessato, ma dal semplice fatto che i costi di attuazione sono eccessivi per quel titolare, o che quel titolare non dispone di una tecnologia adeguata. Inutile dire che, nella sentenza *Google Spain*, il diritto all'oblio non viene presentato come sottoposto a simili condizioni.

Inoltre, il diritto all'oblio è sottoposto anche alle eccezioni del paragrafo 3. In questi casi il bilanciamento non deve essere operato in concreto, caso per caso; al contrario si tratta di un bilanciamento assoluto, definito una volta per tutte: "I paragrafi 1 e 2 non si applicano". Il diritto all'oblio, dunque, soccombe sistematicamente di fronte ad altri valori. E la più significativa tra le eccezioni è senza dubbio quella della lettera a), in base a cui il diritto all'oblio soccombe qualora il trattamento sia necessario "per l'esercizio del diritto alla libertà di espressione e di informazione". La gerarchia stabilita dalla sentenza *Google Spain* e quella sancita dall'articolo

[5] S. Sica-V. D'Antonio, *La procedura di de-indicizzazione*, in G. Resta-V. Zeno-Zencovich (a cura di), *Il diritto all'oblio su Internet dopo la sentenza Google Spain*, Roma, Roma TrE-Press, 2015, 163.

17 del Regolamento 2016/679 sono dunque esattamente agli antipodi l'una rispetto all'altra: nel primo caso prevalgono i diritti alla vita privata e alla protezione dei dati personali; nel secondo prevale il diritto alla libertà di espressione e di informazione. Piuttosto, la soluzione dell'articolo 17 si avvicina a quella della sentenza, della Corte europea dei diritti dell'uomo, *Węgrzynowski* e *Smolczewski* contro Polonia[6]. In tale pronuncia la Corte di Strasburgo, facendo riferimento ai diritti garantiti dalla CEDU all'articolo 8 ("Diritto al rispetto della vita privata e familiare") e all'articolo 10 ("Libertà di espressione"), afferma sì che «as a matter of principle the rights guaranteed by these provisions deserve equal respect», ma fa trapelare un vero e proprio atteggiamento di *favor* nei confronti delle libertà di espressione e di informazione; il loro peso risulta in sostanza prevalente su quello del diritto al rispetto della vita privata e familiare. Ciò si può notare, ad esempio, quando la Corte afferma che «particularly strong reasons must be provided for any measure limiting access to information which the public has the right to receive». Tale atteggiamento riecheggerebbe, a sua volta, una pronuncia della stessa Corte europea dei diritti dell'uomo decisamente più risalente nel tempo: la sentenza *Sunday Times* contro Regno Unito[7], in cui figura in modo esplicito l'affermazione in base alla quale «the Court is faced not with a choice between two conflicting principles but with a principle of freedom of expression that is subject to a number of exceptions which must be narrowly interpreted». Ma ancor di più, una simile impostazione è in linea con le scelte operate negli USA, dove il diritto all'informazione assume, ancor di più a partire dagli anni '70 del secolo scorso, una prevalenza assoluta che deriva dalla *preferred position* accordata al Primo Emendamento. In definitiva, per quanto riguarda il rapporto tra il diritto all'oblio e il diritto alla libertà di espressione e di informazione, l'articolo 17 del Regolamento sembra essere molto vicino alla giurisprudenza della Corte di Strasburgo nonché a quella statunitense, ma molto lontano da quella sancita dalla Corte di Lussemburgo nel caso *Google Spain*.

[6] Corte EDU, sentenza 16 luglio 2013, ric. n. 33846/2007.

[7] Corte EDU, sentenza 26 aprile 1979, ric. n. 6538/1974.

Infine, deve essere sottolineato un ulteriore elemento: l'obbligo dell'articolo 17 paragrafo 2 del Regolamento grava sul titolare che "ha reso pubblici dati personali" e anche il Considerando 66, precedentemente menzionato, fa riferimento al titolare del trattamento "che ha pubblicato dati personali". Il Regolamento lascia così intendere che l'interessato possa rivolgersi direttamente solo al titolare del trattamento che ha pubblicato dati personali, ovvero colui che ha immesso i dati nel web; ad esempio, l'editore della pagina. Su tale soggetto graverebbe, in via esclusiva, l'obbligo di comunicare ai terzi che trattano tali dati della richiesta di cancellazione proveniente dall'interessato. E tra questi terzi figurerebbe anche il gestore del motore di ricerca, che non diventerebbe (almeno *ab origine*) titolare del trattamento e non vedrebbe esercitato direttamente nei suoi confronti il diritto alla cancellazione[8]. Facile intuire che, impedendo all'interessato di rivolgersi fin da subito al gestore del motore di ricerca, il Regolamento anche da questo punto di vista dimostra, rispetto alla sentenza *Google Spain*, un atteggiamento di minor favore nei confronti della persona i cui dati vengono trattati.

Pertanto possiamo concludere che, se è vero che il Regolamento appare sicuramente più attento ad altre esigenze, ad altri valori, ed offre una soluzione decisamente più equilibrata e più apprezzata in dottrina rispetto a quella prospettata nella pronuncia *Google Spain*, per il diritto all'oblio in sé e per sé non solo non è un "passo avanti", ma è un vero e proprio "passo indietro".

Ci si deve quindi chiedere come potrebbe essere risolto l'eventuale contrasto tra la giurisprudenza e il Regolamento: tutto dipenderà, come spesso accade, dalla Corte di giustizia. Solo quando il giudice di Lussemburgo si troverà nuovamente a confrontarsi con il diritto all'oblio, sapremo se la Corte prenderà in considerazione la volontà del legislatore europeo, correggendo o addirittura stravolgendo l'impostazione precedente, oppure se continuerà nel solco tracciato dalla giurisprudenza *Google Spain*, trovando comunque gli appigli normativi giusti per confermarla.

[8] E. Stradella, *Cancellazione e oblio: come la rimozione del passato, in bilico tra tutela dell'identità personale e protezione dei dati, si impone anche nella rete, quali anticorpi si possono sviluppare, e, infine, cui prodest?*, in *Rivista AIC*, 4/2016, 5.

2. "Diritto all'oblio": una denominazione opportuna?

2.1. Le ipotesi in cui l'utilizzo dell'espressione "diritto all'oblio" è giustificato

Vi è infine un'altra questione che merita una breve riflessione, ovvero l'opportunità della denominazione "diritto all'oblio" nel contesto del Regolamento. L'utilizzo dell'espressione "diritto all'oblio", infatti, può avere una sua ragion d'essere solo quando la pubblicazione originaria della notizia è lecita e l'interesse sociale alla diffusione dell'informazione è sempre presente, pur essendo trascorso del tempo, ma nonostante ciò l'interessato può comunque ottenere la rimozione dell'informazione. In tal caso, infatti, l'interesse al permanere in vita dell'informazione a suo tempo diffusa, ovvero l'interesse ad un nuovo, o continuativo, trattamento dei dati personali, soccomberebbe di fronte al puro e semplice interesse alla rimozione della memoria della persona, che magari vuole semplicemente salvaguardare la propria "nuova vita", le proprie condizioni attuali ormai diverse da quelle passate[9].

2.2. Le ipotesi in cui l'articolo 17 consente la cancellazione

Ma l'articolo 17 del Regolamento consente la cancellazione dei dati solo in due gruppi di ipotesi. In base al primo, la cancellazione è consentita quando il trattamento è illecito *ab origine*, come nei casi delle lettere d) ed e). È palese che in tali situazioni non si possa parlare di "diritto all'oblio": siamo infatti di fronte ad un mero strumento per rimediare ad un errore del titolare che, fin dall'inizio, ha pubblicato i dati illecitamente.

In base al secondo gruppo di ipotesi, invece, la cancellazione è consentita quando il trattamento è originariamente lecito, ma in un secondo momento viene a mancare l'interesse sociale alla diffusione dell'informazione, come nei casi delle altre lettere: emblematici sono i casi della lettera a), ovvero dati non più necessari per le finalità per cui sono stati raccolti, e della lettera b), ovvero revoca

[9] E. Stradella, *Cancellazione e oblio: come la rimozione del passato, in bilico tra tutela dell'identità personale e protezione dei dati, si impone anche nella rete, quali anticorpi si possono sviluppare, e, infine, cui prodest?*, cit., 16.

del consenso su cui si basa il trattamento. Ma, quando manca completamente l'interesse sociale, non vi è motivo di chiamare in causa il diritto all'oblio: siamo semplicemente di fronte a un limite alla libertà di espressione e d'informazione, riconosciuto come tale da numerose corti, tra cui la Corte europea dei diritti dell'uomo e anche la stessa Corte di Cassazione italiana nella celeberrima giurisprudenza risalente al 1984[10], in cui elabora i tre parametri della "veridicità" dei fatti, della "continenza" con cui la notizia è espressa e, appunto, dell'interesse pubblico alla conoscenza della notizia ("pertinenza"). Di conseguenza, se manca l'interesse alla diffusione di un'informazione, la sua legittimità può essere messa in discussione, e quindi l'informazione stessa potrebbe essere cancellata, anche senza far riferimento ad uno specifico "diritto all'oblio".

L'espressione "diritto all'oblio" viene quindi utilizzata nel Regolamento senza che ve ne sia una reale necessità e in modo forse un po' demagogico[11]. In verità siamo di fronte ad un semplice diritto alla "cancellazione", meglio disciplinato e dalla portata più ampia rispetto al passato, ma pur sempre un semplice diritto alla "cancellazione".

In ragione di quanto esposto possiamo dunque concludere che, sia i toni entusiastici della Commissione nel presentare il nuovissimo diritto all'oblio dell'articolo 17, sia i toni apocalittici di chi descrive tale disposizione come un fattore di contrasto insanabile tra Europa e Stati Uniti per quanto concerne il rapporto tra libertà di espressione e diritto alla "privacy"[12], appaiono eccessivi e forse dovrebbero essere ridimensionati.

Bibliografia

G. Brock, *The right to be forgotten – Privacy and the media in the Digital Age*, London-New York, I. B. Tauris & Co. Ltd, 2016.

[10] Cass., sez. I civ., 18 ottobre 1984, n. 5259.

[11] E. Stradella, *Cancellazione e oblio: come la rimozione del passato, in bilico tra tutela dell'identità personale e protezione dei dati, si impone anche nella rete, quali anticorpi si possono sviluppare, e, infine, cui prodest?*, cit., 4.

[12] J. Rosen, *The Right to be Forgotten*, in *Stanford Law Review*, 2012. https://www.stanfordlawreview.org/online/privacy-paradox-the-right-to-be-forgotten/

M. Fumagalli Meraviglia, *Le nuove normative europee sulla protezione dei dati personali*, in *Diritto comunitario e degli scambi internazionali*, 2016.

G. González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Dordrecht, Springer, 2014.

M.L. Jones, *Ctrl+Z: The Right to be Forgotten*, New York, New York University Press, 2016.

M. Krzysztofek, *Post-Reform Personal Data Protection in the European Union: General Data Protection Regulation (EU) 2016/679*, Alphen aan den Rijn, Kluwer Law International, 2017.

S. Kulk-F.Z. Borgesius, *Freedom of Expression and "Right to be Forgotten" Cases in the Netherlands after Google Spain*, in *European Data Protection Law Review*, 2015.

R. Pardolesi, *"Gooooglelaw". Del ricorso alla disciplina antitrust per colpire il tiranno benevolente*, in *Foro italiano*, 2013.

J. Rosen, *The Right to be Forgotten*, in *Stanford Law Review*, 2012. https://www.stanfordlawreview.org/online/privacy-paradox-the-right-to-be-forgotten/

S. Sica-V. D'Antonio, *La procedura di de-indicizzazione*, in G. Resta-V. Zeno-Zencovich (a cura di), *Il diritto all'oblio su Internet dopo la sentenza Google Spain*, Roma, Roma TrE-Press, 2015.

E. Stradella, *Cancellazione e oblio: come la rimozione del passato, in bilico tra tutela dell'identità personale e protezione dei dati, si impone anche nella rete, quali anticorpi si possono sviluppare, e, infine, cui prodest?*, in *Rivista AIC*, 4/2016.

Langdell, Pound e il risarcimento del danno non patrimoniale da illecito trattamento dei dati personali. La prassi italiana anche alla luce dell'entrata in vigore del Regolamento (UE) 2016/679

Giulio Ramaccioni

Sommario: 1. Una questione di metodo: Langdell v. Pound – 2. Il principio generale nella materia del risarcimento del danno non patrimoniale da illecito trattamento dei dati personali – 3. L'approccio realista alla materia fondato sullo studio del *legal process* – 4. Quale funzione del danno non patrimoniale, anche in considerazione delle disposizioni del Regolamento (UE) 2016/679? – 5. Conclusioni

«Ma in realtà, niente noi conosciamo
per averlo visto; perché la verità è
nascosta nel profondo»
Democrito

1. Una questione di metodo: Langdell v. Pound

Fra i diversi cambiamenti apportati da Christopher Columbus Langdell, sul finire dell'Ottocento, come Preside della Harvard Law School, vi era quello relativo allo studio del diritto: occorreva concentrarsi sulla individuazione dei principi di diritto i quali emergono dai materiali giuridici, che devono essere identificati con le decisioni dei giudici e non con la legislazione. Per Langdell però, ai fini di uno studio

scientifico del diritto, che era il metodo da lui propugnato, la maggior parte delle decisioni giurisprudenziali erano inutili, in quanto solo da pochissimi casi era possibile trarre qualche insegnamento perché da essi emergeva un principio ispiratore – che era compito del giurista individuare e verbalizzare – capace di governare un ambito assai vasto di problemi. È questa quella che viene definita *legal doctrine*, che diventa così stabilmente uno dei formanti del sistema e il caposaldo dell'intera costruzione metodologica langdelliana.

Come è noto questo approccio al diritto venne fortemente criticato, più tardi, dal realismo giuridico, su cui grande influenza ebbero gli scritti di Roscoe Pound[1] (Preside della Harvard Law School nel 1916 e fra i più autorevoli giuristi accademici americani). I realisti proposero un cambiamento radicale del paradigma scientifico: il giurista divenne colui che studia il *legal process* ovvero le situazioni fattuali ed i meccanismi sociali che portano ad una certa decisione, cercando di vedere le regole effettivamente applicate dalla giurisprudenza ed i percorsi, a volte nascosti, dalla stessa seguiti; l'obiettivo era di andare al di là dei principi declamati dalle sentenze, che spesso celano, invece, un quadro complesso, non univoco, soggetto a torsioni e legato a diverse matrici culturali.

2. Il principio generale nella materia del risarcimento del danno non patrimoniale da illecito trattamento dei dati personali

A questo punto ci si potrebbe legittimamente chiedere il perché di questa premessa riguardante l'esperienza americana tra il finire del XIX secolo e la prima metà del XX secolo. Il motivo è presto detto: mi sembra che la controversia tra i formalisti langdelliani ed i realisti possa essere utilizzata per analizzare, in modo esplicativo, il discorso che intendo sviluppare sul tema della funzione svolta dal

[1] Pound è il fondatore della *sociological jurisprudence* e non può essere considerato un realista in senso stretto (il realismo americano in senso stretto si colloca, infatti, intorno al 1930), ma possiamo farlo rientrare in quella forma di realismo allargato che coincide con la critica al formalismo giuridico, in cui grande rilievo ebbe anche Oliver Wendell Holmes (giudice della Corte Suprema dal 1902 al 1932).

risarcimento del danno non patrimoniale da illecito trattamento dei dati personali, già regolato dall'art. 15 del d.lgs. 196/2003 [recentemente abrogato dall'art. 27, comma 1, lett. a), n. 2), del d.lgs. 101/2018[2]] e che ha trovato attualmente una precisa disciplina in ambito europeo con l'entrata in vigore del Regolamento (UE) 2016/679, il cui art. 82 prevede espressamente la risarcibilità del danno immateriale in caso di violazione delle norme regolamentari da parte del titolare o del responsabile del trattamento[3].

Lasciando da parte l'analisi del formante legislativo (anch'esso di grande utilità per trattare in modo avveduto i temi che si stanno esaminando, ma che ci porterebbe ad una analisi troppo ampia per poter essere affrontata in questa sede)[4], concentriamo la nostra attenzione sulle decisioni delle corti.

[2] Questo recente intervento legislativo – il cui titolo è "Disposizioni per l'adeguamento della normativa 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 (regolamento generale sulla protezione dei dati)" – ha profondamento modificato l'impianto normativo di cui al d.lgs. 196/2003.

[3] L'art. 82 viene puntualmente richiamato dall'art. 152, comma 1, del d.lgs. 196/2003, come riformulato dall'art. 13, comma 1, lett. h), del d.lgs. 101/2018.

[4] Si riportano, per completezza di indagine, alcuni di questi interventi legislativi da cui può rilevarsi una curvatura in senso sanzionatorio e deterrente dello strumento risarcitorio: *a)* l'art. 2 della l. 8 febbraio 2006, n. 54, che ha introdotto l'art. 709-*ter* c.p.c. In particolare, il 2° comma, nn. 2 e 3, in cui si prevede, per il caso di gravi inadempienze o di atti che comunque arrechino pregiudizio al minore od ostacolino il corretto svolgimento delle modalità dell'affidamento, che il giudice possa sia disporre il risarcimento dei danni a carico di uno dei genitori, nei confronti del minore, sia il risarcimento dei danni a carico di uno dei genitori, nei confronti dell'altro. Non sembra, dunque, estranea al tessuto normativo una finalità sanzionatoria e preventiva delle misure risarcitorie adottate, peraltro confermata, al punto n. 4 dello stesso comma, dal potere del giudice di condannare il genitore inadempiente al pagamento di una sanzione amministrativa pecuniaria; *b)* l'art. 5 del d.lgs. 16 marzo 2006, n. 140, che ha sostituito l'art. 158 della l. 22 aprile 1941, n. 633, in cui si prevede, al comma 3, a tutela del diritto d'autore, anche la risarcibilità del danno non patrimoniale; mentre, il comma 2 dello stesso articolo conferisce al giudice il potere di attribuire un risarcimento, riferito al lucro cessante, parametrato agli utili realizzati dal trasgressore in violazione dei diritto: cercando così di realizzare obiettivi di tutela in senso

Nella materia del danno non patrimoniale da illecito trattamento dei dati personali la declamazione ufficiale, dichiarata a mò di principio generale in grado di governare tutte le problematiche ad essa attinenti, è fondata sui seguenti assiomi[5], idonei a rendere palesi tutte le valenze precettive del principio stesso:

a) la lesione non patrimoniale non può essere considerata *in re ipsa*, e cioè, in altre parole, il solo fatto che vi sia stato un trattamento illecito di dati non determina, di per sé stesso, l'affiorare di un danno di natura appunto non patrimoniale;
b) si tratta, dunque, di un danno conseguenza che deve essere provato secondo le consuete regole;
c) è da escludere, in questo ambito, una funzione sanzionatoria dello strumento risarcitorio.

deterrente e dissuasivo; *c)* il d.lgs. 11 aprile 2006, n. 198 ("Codice delle pari opportunità tra uomo e donna"), che all'art. 38, prevede la possibilità di richiedere, in caso di discriminazione, anche il risarcimento del danno non patrimoniale, che assume in questo contesto una specifica funzione sanzionatoria e dissuasiva; *d)* il d.lgs. 6 novembre 2007, n. 196, in tema di parità di trattamento di uomini e donne, il cui art. 55-*quinquies*, comma 7, riconosce la possibilità del risarcimento del danno non patrimoniale, che deve essere liquidato dal giudice anche in considerazione dei comportamenti di cui all'art. 55-*ter*, comma 7, posti eventualmente in essere dal convenuto; *e)* il d.lgs. 1° settembre 2011, n. 150, art. 28, che, in tema di controversie in materia di discriminazione, prevede espressamente la possibilità di ottenere il ristoro della lesione non patrimoniale subita. Stabilendo, inoltre, che, ai fini della liquidazione del danno, il giudice deve tener conto «del fatto che l'atto o il comportamento discriminatorio costituiscono ritorsione ad una precedente azione giudiziale ovvero ingiusta reazione ad una precedente attività del soggetto leso volta ad ottenere il rispetto del principio della parità di trattamento».

[5] La verbalizzazione compiuta del principio la si trova riportata in un'ampia gamma di pronunce della Cassazione: si può fare riferimento, in questa sede, alle note sentenze delle Sezioni unite (denominate di "San Martino"), nn. 26972-26975, dell'11.11.2008, in *Resp. civ. prev.*, 2009, 1, 38, che si concentrano sulla categoria generale del danno non patrimoniale. Per quanto riguarda il tema specifico del danno non patrimoniale da illecito trattamento dei dati personali, il principio è enunciato, *ex multis*, da Cass., 15.7.2014, n. 16133, in *Foro it.*, 2015, 1, I, 120; Cass., 20.5.2016, n. 10510, in *Diritto & Giustizia*, 2016, 23 maggio; Cass., 25.1.2017, n. 1931, in *Resp. civ. prev.*, 2017, 3, 837.

3. L'approccio realista alla materia fondato sullo studio del *legal process*

In questo lavoro intendo approfondire l'esame di tale principio e se esso è davvero in grado di sistemare in maniera concettualmente coerente – anche sotto un profilo delle funzioni svolte – la tematica del danno non patrimoniale da illecito trattamento dei dati personali. Per affrontare questa analisi mi soffermerò, con attitudine realista, sullo studio di alcuni casi giurisprudenziali[6] e sulle situazioni fattuali che li caratterizzano.

Questa impostazione ci consentirà di verificare come quella "verità" giuridica – che abbiamo già sottolineato nel paragrafo precedente essere stata enunciata dalla giurisprudenza in modo apparentemente chiaro e coerente – non si presenta poi come tale o, comunque, non riesce a imporsi sulla vitalità del diritto giurisprudenziale, che risulta essere molto più complesso e composito di quanto il *mainstream* sembra affermare.

Lo studio del *legal process*, ovvero dell'insieme dei meccanismi sociali che portano ad una data decisione, ci permette di delineare un quadro in cui è difficile individuare un percorso evolutivo coerente; al contrario, è come se ci trovassimo all'interno di un edificio spesso costellato da corridoi nascosti, che di volta in volta emergono come fiumi carsici, rappresentandoci tutta la loro forma disordinata e complessa. Un quadro, dunque, molto più frastagliato rispetto alle declamazioni ufficiali sopra analizzate, che appaiono sempre più come confortanti luoghi in cui potersi rifugiare, piuttosto che affidabili criteri conoscitivi della mutevole realtà.

Questo contesto, alquanto multiforme e magmatico, si presenta, inoltre, in particolare nella materia del danno non patrimoniale, sottoposto a diverse torsioni, come diverse sono le matrici culturali e le ideologie che lo hanno nel tempo ispirato. Proviamo a indicarne almeno alcune:

[6] Il carattere del presente lavoro non consente di poter affrontare l'analisi di una gamma più ampia di casi giurisprudenziali. In ogni caso, nelle pagine che seguono saranno evidenziati (cfr., *infra*, in nota 12) gli estremi delle decisioni che sembrano confermare l'impostazione seguita con la ricerca che si sta conducendo.

a) Innanzitutto le funzioni sanzionatoria e deterrente sono sempre state presenti all'interno dello strumento risarcitorio previsto dall'illecito aquiliano, come è stato da poco, *ex professo*, ulteriormente evidenziato dalle Sezioni unite della Cassazione con la decisione n. 16601/2017[7], in cui tra l'altro si afferma che queste funzioni hanno assunto un rilievo, sia a livello legislativo che giurisprudenziale, sempre più crescente negli ultimi anni: «In sintesi estrema può dirsi che accanto alla preponderante e primaria funzione compensativo riparatoria dell'istituto (che immancabilmente lambisce la deterrenza) è emersa una natura polifunzionale (un autore ha contato più di una decina di funzioni), che si proietta verso più aree, tra cui sicuramente principali sono quella preventiva (o deterrente o dissuasiva) e quella sanzionatorio-punitiva», sottolineando, infine, come «nella stessa giurisprudenza costituzionale si trovano agganci meritevoli di considerazione» (si fa riferimento a Corte Cost. n. 303/2011; Corte Cost. n. 152/2016; Corte Cost. n. 238/2014)[8].

Le due funzioni sanzionatoria e deterrente, come è noto, sono diverse: quando si parla di carattere sanzionatorio viene presa in esame la condotta antigiuridica del danneggiante e la sua gravità, mentre quando si parla di deterrenza si allude al complesso di effetti generati sul piano della prevenzione del rischio; e proprio in questo senso deve essere letto il Regolamento (UE) 2016/679, fortemente caratterizzato da un approccio basato sul rischio e su misure di *accountability* dei titolari e dei responsabili del trattamento.

b) Si pensi, inoltre, al danno morale ed alla sua nota interpretazione originaria, chiaramente fondata su una lettura dell'art. 2059 c.c. in senso sanzionatorio, in quanto il risarcimento – previsto esclusivamente nei casi determinati dalla legge – veniva legato soltanto ai danni derivanti da reato. La prima stagione del danno non patrimoniale era, appunto, connotata dalla predominanza della teoria punitiva, la quale individuava lo scopo del risarcimento del danno morale nella punizione dell'autore dell'illecito, attesa la particolare gravità e riprovevolezza del suo comportamento, così da pro-

[7] Cass., sez. un., 5.7.2017, n. 16601, in *Foro it.*, 2017, 9, I, 2613.

[8] Tutte le sentenze richiamate sono leggibili nel sito internet della Consulta *https://www.cortecostituzionale.it*

porre la previsione normativa come una sorta di pena privata, con scopo chiaramente sanzionatorio[9].

c) Allo stesso modo non dobbiamo dimenticare la lezione di Pietro Trimarchi che ci ha più volte ricordato – spostando l'attenzione sulla dimensione collettiva del danno – che il risarcimento elimina il danno dal punto di vista (soggettivo) della vittima; ma non lo elimina dal punto di vista (oggettivo) della società nel suo insieme, che continua a soffrire per la risorsa distrutta[10].

d) Infine, uno sguardo realista al *case law* CEDU consente di cogliere al fondo dell'operato della Corte più un uso strumentale del (risarcimento del) danno non patrimoniale che non la preservazione di una sua qualche intangibile essenza. In ambito europeo, infatti, come dimostra, ad esempio, la decisione emessa nel caso *Rotaru c. Romania*[11], in tema di rispetto della vita privata ai sensi dell'art. 8 della Convenzione, il danno morale viene risarcito per il solo fatto del comportamento gravemente antigiuridico posto in essere dal Governo rumeno attraverso i propri servizi segreti. Ci trovia-

[9] Ben nota è la tradizionale lettura del danno non patrimoniale, inteso quale ingiusto perturbamento dello stato d'animo del danneggiato a seguito dell'offesa ricevuta, che attribuisce al relativo risarcimento il significato di *pretium doloris* per le sofferenze morali derivanti da fatti dannosi particolarmente offensivi. In questa ottica si giustifica la limitazione di risarcibilità di tali danni al settore dei fatti illeciti costituenti reato (art. 185 c.p.) e agli altri casi previsti dalla legge, poiché in tali ipotesi – come esplicitamente avverte la Relazione al Re – «è più intensa l'offesa al bene giuridico e maggiormente sentito il bisogno di una più energica repressione con carattere anche preventivo» (R. Scognamiglio, voce *Illecito (diritto vigente*), in *Noviss. Dig. it.*, vol. VII, Torino, 1962, 146). In buona sostanza, quantomeno nel primo periodo della vigenza del codice del 1942, il danno morale sembrava poggiare sul carattere personale della responsabilità per colpa e pareva ispirarsi ad un'esigenza di collegamento tra la valutazione del pregiudizio subito dal danneggiato e la valutazione della gravità della condotta del danneggiante, di modo che la finalità preminente del risarcimento di questa specie di pregiudizi, poteva consistere nell'ulteriore sanzione e prevenzione contro gli illeciti.

[10] Si veda, da ultimo, P. Trimarchi, *La responsabilità civile: atti illeciti, rischio, danno*, Milano, Giuffrè, 2017. Molto utile per comprendere l'impostazione complessiva seguita da Trimarchi è il recente lavoro di V. Roppo, *Pensieri sparsi sulla responsabilità civile (in margine al libro di Pietro Trimarchi)*, in *Questione Giustizia*, 2018, 1, 108.

[11] Corte EDU, Grande Camera, 4.5.2000, n. 28341/95, *Rotaru c. Romania*, leggibile nel sito internet della Corte *http://www.echr.coe.int/*

mo, dunque, davanti a un apprezzamento di fatto dei giudici di Strasburgo (che si concentrano sul comportamento tenuto dall'autorità pubblica), nel quale non entrano valutazioni circa la qualificazione dell'interesse leso, così come non hanno rilevanza alcuna tutte le discussioni nostrane circa la duplicazione tra danno patrimoniale e non patrimoniale.

4. Quale funzione del danno non patrimoniale, anche in considerazione delle disposizioni del Regolamento (UE) 2016/679?

Nel caleidoscopio riflesso dalla giurisprudenza italiana si possono individuare tutte le tracce delle torsioni di cui sopra si parlava.
I giudici nazionali spesso adottano un'ampia nozione di danno non patrimoniale, ricorrendo ad una sorta di astrazione delle lesioni effettivamente determinate alla sfera immateriale della persona, e cioè affermando un concetto di danno molto vago e in grado di prestarsi al raggiungimento di finalità anche sanzionatorie e deterrenti piuttosto che compensative.

Il repertorio della giurisprudenza sul tema è assai ampio e in questa sede non può che offrirsene una breve sintesi organizzata intorno al tema del risarcimento del danno non patrimoniale da illecito trattamento dei dati personali.

Davvero paradigmatico del percorso interpretativo fin qui delineato è il noto caso *Vieri c. Inter - Telecom*[12] deciso dal Tribunale di Milano, in cui la lesione non patrimoniale della privacy del calciatore Vieri – che, peraltro, non aveva specificamente richiesto tale posta di danno ai sensi dell'art. 15 del d.lgs. 196/2003 – viene non solo ritenuta

[12] Trib. Milano, 3.9.2012, n. 9749, in *Danno e resp.*, 2013, 1, 51. Altri casi molto interessanti ai fini della impostazione esegetica che si ritiene preferibile in *subiecta materia*, ma che non possono essere analizzati in questa sede, sono: Trib. Milano, 13.4.2000, in *Foro it.*, 2000, I, 3004; Trib. Milano, 8.8.2003, in *Danno e resp.*, 2004, 303; Trib. Milano, 27.6.2007, in *Guida al dir.*, 2007, 41, 56; Trib. Brescia, 4.3.2013, leggibile nel sito internet *http://www.lawyersonweb.it/*, ultima consultazione del 19.6.2018; Cass., 22.1.2015, n. 1126, in *Responsabilità civ. prev.*, 2015, 3, 827; Cass., 21.6.2018, n. 16311, leggibile nel sito internet della Corte di Cassazione *http://www.cortedicassazione.it*

esistente in riferimento all'*an*, ma liquidata, in riferimento al *quantum*[13], con la cospicua somma di un milione di euro.

Al riguardo, il nodo centrale della sentenza è quello relativo alla esistenza del danno ed alla sua prova. Il Tribunale milanese ha osservato che «l'indebita intromissione nella propria sfera privata da parte di soggetti estranei, tanto più quando viene effettuata in modo subdolo e con modalità illecite, ingenera nella vittima uno stato di sofferenza», con ciò concentrando l'attenzione più sul comportamento antigiuridico posto in essere dal danneggiante che sulla lesione non patrimoniale subita dal danneggiato (che è rimasta sostanzialmente non provata e, in ogni caso, tale da apparire *ictu oculi* del tutto priva di collegamento con l'importo effettivamente liquidato).

Interessante è, inoltre, rilevare come la statuizione suddetta è stata confermata dalla Corte di Appello di Milano[14], in riferimento all'accertamento dei presupposti della responsabilità, dell'esistenza del danno e della sua risarcibilità. È pur vero che il risarcimento è stato drasticamente ridotto in euro 70.000,00, ma la Corte si è soffermata a ribadire «che senza dubbio le condotte di cui le società per tutto quanto innanzi illustrato sono responsabili, appaiono particolarmente riprovevoli per il loro carattere subdolo e sleale e in considerazione dell'utilizzo di strumenti di cui il gestore telefonico, in posizione di particolare favore, poteva disporre in funzione dell'espletamento di un servizio pubblico e che venivano invece in maniera distorta piegati a tutt'altre finalità». In questa prospettiva – dove sembra trasparire una curvatura del rimedio risarcitorio in senso sanzionatorio e deterrente – viene, inoltre, evidenziato come nella liquidazione del danno da violazione della privacy si debba tener conto di alcuni elementi, che possono essere così sintetizzati:

i) la gravità oggettiva delle condotte poste in essere e le modalità operative attraverso cui si sono svolte;
ii) gli ambiti di vita esplorati;

[13] Evidenziano la centralità del *quantum* risarcitorio – troppo spesso confinato in un'area di marginalità dalle analisi della dottrina – nel quadro complessivo del rimedio previsto dagli artt. 2043 e ss. c.c., V. Roppo, cit., 112 e G. Ponzanelli, *La nuova frontiera della responsabilità civile: la quantificazione del danno patrimoniale*, in *Questione Giustizia*, 2018, 1, 114.

[14] App. Milano, 22.7.15, in *Foro it.*, 2015, 10, I, 3312.

iii) la durata dell'intrusione;
iv) il numero delle persone coinvolte nelle indagini e loro capacità e risorse professionali;
v) le modalità di trattamento dei dati e, quindi, la maggiore o minore diffusione delle notizie riservate apprese.

Pertanto, anche laddove si voglia valutare la vicenda complessiva e le soluzioni individuate dai giudici in modo formalistico, nel senso di una adesione alla declamazione ufficiale sopra vista e cioè che, nel caso di specie, siamo comunque davanti ad un risarcimento ancora contraddistinto da una *ratio* compensativa e concesso in via equitativa, non si può non vedere che l'obiettivo appunto compensativo è perseguito in modo ondivago e del tutto disancorato dalla lesione subita dal danneggiato.

La questione può, dunque, essere sinteticamente esposta nel modo seguente: anche a voler ammettere una legittima adesione formale da parte della giurisprudenza al *mainstream* in materia, questa si presenta formulata in modo acritico e non riesce a far velo al tenore sostanziale della sentenza, che sembra andare in una direzione del tutto diversa.

Rappresenta un esempio emblematico di tale ragionamento aporetico il caso recentemente deciso dal Tribunale di Catania[15], caratterizzato da una lite tra vicini proprietari di due villette a schiera confinanti; una con un cane maleducato e dotata di videocamere di sorveglianza e l'altra abitata da persone accusate di maltrattamenti nei confronti del suddetto animale e addirittura di aver tentato di ucciderlo.

Lasciando da parte tutte le articolate questioni giuridiche (anche di natura penale) che hanno caratterizzato la vicenda, appuntiamo la nostra attenzione sulla questione relativa alla lesione della privacy determinata dall'impianto di videosorveglianza, il cui angolo di visuale si estendeva sulla proprietà altrui (ricomprendendo le finestre e l'ingresso della abitazione confinante). Il Tribunale – verificata l'esistenza di una violazione della disciplina di cui al d.lgs. 196/2003 – è poi costretto a ricorrere ai principi formali che governano la materia e cioè: *i)* la lesione non patrimoniale non può essere considerata *in re ipsa*; *ii)* si tratta, dunque, di un danno conseguenza che deve

[15] Trib. Catania, 31.1.2018, n. 466, leggibile nel sito internet *http://www.quotidianogiuridico.it/*, ultima consultazione 29.6.2018.

essere allegato e provato; *iii)* è da escludere in questo ambito una funzione sanzionatoria dello strumento risarcitorio.

Applicando questi canoni al caso di specie, il giudice si rende conto di due cose. La prima è che non risulta provato alcun danno di carattere non patrimoniale da parte del proprietario dell'abitazione su cui era illecitamente rivolto l'occhio delle telecamere: di conseguenza non potrebbe disporre alcuna condanna di tipo risarcitorio. La seconda è che tale soluzione sarebbe inappagante visto il comportamento gravemente antigiuridico posto in essere dal proprietario dell'impianto di videosorveglianza: per questo ricorre alla categoria dei danni puntivi (con il richiamo a Cass., sez. un., 16601/2017), ricordando, inoltre, – in contraddizione con la propria preliminare affermazione di pieno rispetto dei criteri esegetici forniti dalla declamazione ufficiale sopra analizzata – la funzione sanzionatoria e deterrente della responsabilità civile; onde per cui il danno non patrimoniale viene accertato in euro 2.000,00.

Al di là della correttezza o meno della conclusione a cui è pervenuto il Tribunale di Catania, il dato da sottolineare è come si percepisca chiaramente il disagio del giudice nell'applicare il principio generale che dovrebbe governare la materia del risarcimento del danno non patrimoniale da illecito trattamento dei dati personali, che è ritenuto del tutto inappagante a risolvere la fattispecie e lo obbliga a torsioni lessicali e giuridiche evidenti pur di poter affermare il diritto al risarcimento del danno.

Un'ultima pronuncia della Cassazione, la n. 14242 del 4.6.2018[16], ci evidenzia ancora meglio le torsioni a cui l'adesione in modo soltanto formale al principio crea.

Un agente di Dogana, a seguito di un'indagine nei propri confronti, nel corso della quale era stato sottoposto a perquisizione personale, domiciliare e locale, viene trasferito. Il provvedimento di tale trasferimento, in cui si citava la vicenda giudiziaria, viene però comunicato utilizzando il protocollo ordinario aperto a tutti e non il protocollo riservato, come dovuto trattandosi di dati giudiziari. L'interessato fa ricorso al Garante per la protezione dei dati personali per illecito trattamento, ma ottiene, da parte dell'Autorità adita, un rigetto (in quanto

[16] Cass., 4.6.2018, n. 14242, leggibile nel sito internet della Corte di Cassazione *http://www.cortedicassazione.it*

non si è rinvenuta alcuna violazione della normativa in materia) e così si rivolge al Tribunale di Roma che, invece, gli dà ragione e gli riconosce il danno non patrimoniale nella misura di euro 10.000,00.

L'Agenzia delle Dogane e dei Monopoli ricorre in Cassazione sostenendo che nella sentenza impugnata non si accerta, in realtà, alcun danno non patrimoniale e che, in ogni caso, tale pregiudizio non è stato provato.

La Suprema corte, nell'esaminare la fattispecie, si trova di fronte ad un danno effettivamente non accertato secondo i *principia* sopra elencati e non provato in nessuno dei suoi aspetti: circostanza che avrebbe dovuto portare – ripetiamo: sulla scorta dei criteri ermeneutici formalmente adottati dalla giurisprudenza – ad una pronuncia in cui si indicava l'erroneità dell'operato del Tribunale di Roma in punto di riconoscimento del danno non patrimoniale. Ma i Giudici di legittimità – ritenendo che il comportamento antigiuridico posto in essere dalla Agenzia delle Dogane non possa non avere conseguenze di tipo risarcitorio – sottopongono i suddetti principi generali ad una fortissima torsione per arrivare ad affermare che l'esistenza del danno non patrimoniale nelle violazioni della normativa di cui al d.lgs. 196/2003 è da presumersi *in re ipsa (sarebbe, quindi, determinato dallo stesso comportamento antigiuridico posto in essere, in una sorta di riproposizione del concetto di danno-evento)*, salvo che il danneggiante non dia prova contraria: «la fattispecie delineata dai due commi dell'art. 15 del d.lgs. 196/03 pone quindi due presunzioni: [...] e quella secondo la quale le conseguenze non patrimoniali di tale danno [...] sono da considerare *in re ipsa* a meno che il danneggiante non dimostri che esse non vi sono state [...]. Ed infatti il danno maggiormente connaturato all'illecito trattamento è proprio quello non patrimoniale sicché il non avere adottato le misure idonee ad evitarlo si rivela in sostanza, come una violazione delle regole di correttezza e di liceità le quali sono finalizzate a bilanciare la libertà di chi tratta i dati con la preservazione della sfera del danneggiato».

5. Conclusioni

Occorre allora notare come la giurisprudenza esaminata sancisca, di fatto, un principio di diritto diverso e più ampio di quello che si vuole evidenziare come l'unico che governa la materia: il risarcimento del

danno non patrimoniale da illecito trattamento dei dati personali non può fondarsi sull'assunto che debba svolgere la sola funzione della *restitutio in integrum* della vittima. Questo approdo potrà essere variamente considerato e anche avversato con argomenti idonei, ma per il momento rappresenta lo stato delle cose. Uno stato in cui emerge in controluce il riconoscimento della funzione sanzionatoria e deterrente dello strumento risarcitorio di cui all'art. 15 del d.lgs. 196/2003. Ciò comporta «che il risarcimento del danno non deve solo tenere conto della gravità della condotta del convenuto, ma anche coprire un'altra quota, quella che serve a deterrere per il futuro eventuali altri agenti dal commettere le stesse incurie del convenuto»[17].

Questa lettura non subisce alcun mutamento in seguito alla già ricordata abrogazione dell'art. 15 da parte dell'art. 27, comma 1, lett. a), n. 2), del recente d.lgs. 101/2018; anzi, come visto sopra al paragrafo 1 (nota 1), trova una ulteriore conferma nell'art. 82 del Regolamento (UE) 679/2016 [espressamente richiamato dall'art. 152, comma 1, del d.lgs. 196/2003, come riformulato ad opera dell'art. 13, comma 1, lett. h), del d.lgs. 101/2018], in cui viene stabilito il diritto di ottenere il risarcimento del danno materiale e immateriale da chiunque subito a causa della violazione del regolamento. Inoltre, il Regolamento, in una prospettiva di prevenzione e di deterrenza, propone, al considerando (148), la necessità di individuare, nella disciplina, profili sanzionatori, arrivando anche a fissare alcuni criteri relativi alla quantificazione degli stessi: «Per rafforzare il rispetto delle norme del presente regolamento, dovrebbero essere imposte sanzioni [...] per violazione del regolamento [...]. Si dovrebbe prestare tuttavia debita attenzione alla natura, alla gravità e alla durata della violazione, al carattere doloso della violazione e alle misure adottate per attenuare il danno subito, al grado di responsabilità o eventuali precedenti violazioni pertinenti [...] all'adesione a un codice di condotta e eventuali altri fattori aggravanti o attenuanti».

[17] A. Gambaro, *Le funzioni della responsabilità civile tra diritto giurisprudenziale e dialoghi trasnazionali*, in *NGCC*, 2017, 10, 1405. Lungo questa prospettiva, v. anche P.G. Monateri, *Le sezioni unite e le molteplici funzioni della responsabilità civile*, in *NGCC*, 2017, 10, 1410.

Il Regolamento (UE) 2016/679 alla prova dei flussi migratori diretti verso l'Europa mediterranea. La tutela dei dati personali di rifugiati e migranti

Mirko Forti

Sommario: 1. Introduzione – 2. L'evoluzione del diritto alla privacy e il suo riconoscimento internazionale – 3. La tutela dell'identità personale dei migranti all'epoca del GDPR – 4. La tutela dei dati personali e la lotta al traffico illegale di esseri umani – 5. Conclusioni

1. Introduzione

Da diversi anni flussi migratori sempre crescenti, provenienti principalmente dall'Africa e dal Medio Oriente, si stanno dirigendo verso il continente europeo. Nel solo 2018 ben 17.258 persone, di cui 14.769 via mare, sono entrate nei confini dell'Unione europea. Nel 2017[1] furono invece in 186.768 ad arrivare nel territorio europeo, ma 3.116 perirono durante il pericoloso viaggio intrapreso dai loro Stati di origine, alla ricerca di una vita migliore. Le cause di un simile fenomeno migratorio sono molteplici; limitandosi a un breve accenno introduttivo e non esaustivo, possono essere menzionati elementi quali l'intensa crescita demografica e l'aumentata urbanizzazione avvenuta nelle regioni di provenienza, nonché l'instabilità politica ed economica di dette zone[2].

[1] Dati aggiornati al 1 aprile 2018, fonte *http://migration.iom.int/europe/* (consultato il 3 aprile 2018).

[2] M. Stoicovici, *Who are the migrants of today*, in *International Journal of Juridical Science*, 2010.

Un simile afflusso di persone pone numerose sfide che l'Unione europea non può esimersi dall'affrontare, e tra queste non deve essere trascurata la salvaguardia della privacy dei migranti. La raccolta e il trattamento dei dati personali di questi ultimi sono passi necessari per un controllo efficace dei movimenti migratori, per una loro facilitazione e per comprendere appieno le ragioni che hanno spinto così tante persone a intraprendere simili viaggi, nonché per rispettare la loro dignità umana. Le autorità nazionali e le agenzie europee, così come le Organizzazioni internazionali coinvolte nell'accoglienza dei migranti arrivati nel territorio europeo, devono infatti raccogliere dati sensibili di diversa natura: ad esempio, informazioni biografiche come il nome e la data di nascita, dati genetici e biometrici come le impronte digitali e campioni di DNA, documenti personali come la storia clinica[3].

La recente approvazione del Regolamento (UE) 2016/679[4] (di seguito, anche, il "Regolamento GDPR" o il "Regolamento") apre una nuova fase della normativa dell'Unione in materia di protezione dei dati personali, con importanti conseguenze anche nella gestione dei dati sensibili relativi ai migranti.

Il presente articolo si propone perciò di analizzare i profili di novità introdotti dal Regolamento, al fine di valutare la sua possibile incidenza sulla gestione della crisi migratoria. Dopo una breve introduzione sull'evoluzione del diritto alla privacy alla luce del costante progresso tecnologico, saranno infatti esaminati alcuni aspetti particolarmente rilevanti del GDPR nell'ambito della tutela dell'identità personale dei migranti. Il diritto alla riservatezza viene inoltre in rilievo nella lotta all'immigrazione illegale; sarà quindi valutato come l'utilizzo, a questo fine, di strumenti quali i droni o la geo-localizzazione possano porre a rischio la privacy dei soggetti coinvolti.

[3] R. Martens, *IOM data protection manual*, Ginevra, 2010, 14 e ss.

[4] 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 (regolamento generale sulla protezione dei dati), in GUUE n.119 del 4 maggio 2016, 1-88.

2. L'evoluzione del diritto alla privacy e il suo riconoscimento internazionale

Il continuo sviluppo delle nuove tecnologie di comunicazione ha fatto sì che ogni individuo sia costantemente connesso alla rete internet, condividendo le informazioni che lo riguardano con i restanti membri della comunità sociale. Il progresso tecnologico si è rivelato essere, come prevedibile, assai più rapido e incisivo della consapevolezza sociale e giuridica che avrebbe dovuto accompagnarlo di pari passo; le soluzioni normative previste per singoli casi specifici si stanno dimostrando inadeguate a rappresentare il continuo mutamento della società attuale, rendendo quindi necessaria l'individuazione di principi e valori riferibili al lungo periodo[5], che possono rimanere validi a prescindere dall'avanzamento delle nuove tecnologie. Questa continua connessione dei singoli a internet comporta la riduzione dei rispettivi spazi privati, provocando la moltiplicazione degli appelli alla privacy e la consapevolezza della necessaria evoluzione di questo concetto, al fine di adattarlo alle nuove e mutate esigenze della società attuale[6]. La privacy non è infatti più intesa solamente come *ius excludendi alios*, ossia come diritto individuale di escludere qualsiasi ingerenza esterna dalla propria sfera privata[7], ma anche come possibilità di ciascuno di controllare l'uso e la disponibilità dei propri dati personali[8]. Al centro della nuova concezione di privacy viene quindi posto l'individuo e il suo diritto ad avere l'ultima parola sulla raccolta e sul trattamento delle informazioni che lo riguardano, alla luce di una più ampia nozione di "protezione dei dati personali" che va a sostituire e integrare la sola tutela della riservatezza individuale, delineandosi inoltre come criterio di legalità dell'azione pubblica.

Si afferma perciò una sorta di diritto all'autodeterminazione informativa di ogni singolo individuo, da inserire in un più ampio

[5] S. Rodotà, *Tecnologie e diritti*, Bologna, Il Mulino, 1995, 19 e ss.

[6] S. Rodotà, cit.

[7] S.D. Warren-L.D. Brandeis, *The right to privacy*, in *Harvard Law Review*, 1890, 4, 193.

[8] A.F. Westin, *Privacy and freedom*, New York, Atheneum, 1970; A.R. Miller, *The assault on privacy*, University of Michigan Press, Ann Arbor, 1971; L. Lusky, *Invasion of privacy: a clarification of concepts*, in *Columbia Law Review*, 1972, 72, 693-710.

novero di prerogative che contribuiscono a salvaguardarne il diritto alla personalità[9], quali il diritto di «cercare, ricevere e diffondere informazioni e idee»[10] e il principio della riservatezza informatica. Il valore della privacy non viene più collegato al diritto di proprietà[11], bensì alla tutela della propria identità personale: controllare la, e influire sulla, circolazione delle proprie informazioni contribuisce a definire il ruolo dell'individuo nella società[12].

La disciplina giuridica attuale in materia di trattamento dei dati personali trova una sua prima espressione in due atti internazionali quali la Convenzione 108 del Consiglio d'Europa[13] e la Raccomandazione 131 dell'OCSE[14]; dall'analisi di questi documenti è possibile enucleare una serie di principi che caratterizzano ancora oggi la normativa attualmente in vigore. Alla stregua di tali principi, la raccolta dei dati personali deve essere condotta all'insegna della correttezza e dell'esattezza delle informazioni collezionate, a cui è collegato l'obbligo del loro aggiornamento periodico. Il soggetto interessato dal trattamento dei dati ha il diritto di essere informato sulle finalità alla base del suddetto trattamento prima che questo abbia luogo. Viene riconosciuto anche il principio della pubblicità delle banche dati che trattano informazioni personali, di cui deve esistere un registro accessibile[15], nonché il principio dell'accesso individuale che rende possibile a chiunque conoscere quali e quanti dati sul proprio conto sono stati raccolti. Ai fini della presente analisi, risulta particolarmente significativa proprio la Convenzione 108, il cui scopo principale è, ai sensi dell'articolo 1, garantire a ogni persona, indipendentemente da elementi quali la cit-

[9] D. Messinetti, voce *Personalità (diritti della)*, in *Enciclopedia del diritto*, vol. XXXIII, 355 e ss.

[10] Art. 19 della Dichiarazione Universale dei Diritti dell'Uomo, 1948.

[11] Y. Poullet, *Le fondement de la protection des donnés nominatives:"propriétes ou libertés"*, in *Nouvelles technologies et propriété*, LITEC, Montréal, 1991, 175; J. Rubenfeld, *The right of privacy*, in *Harvard Law review*, 1988-89, 102, 737

[12] S. Rodotà, cit.

[13] Convenzione del Consiglio di Europa del 28 gennaio 1981 sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale.

[14] Raccomandazione del Consiglio OCSE relativa alle linee-guida per la sicurezza dei sistemi informativi e delle reti: verso una cultura della sicurezza, adottata dal Consiglio nel corso della sua 1037ma riunione, il 25 luglio 2002, C (2002)131/FINAL.

[15] S. Rodotà, cit.

tadinanza, sul territorio di ciascun Paese contraente, il rispetto della propria vita privata in relazione all'elaborazione automatica dei dati personali che la riguardano. Appare evidente, dal tenore di tale articolo, che l'attenzione degli Stati contraenti viene posta principalmente sulla protezione dei dati personali, come corollario e logica evoluzione del diritto alla privacy precedentemente inteso solo come diritto alla riservatezza. Ratificando la Convenzione 108, la stessa Unione europea ha mostrato di condividerne i valori, che informano quindi la produzione normativa UE in tale ambito.

Il diritto al rispetto della vita privata è inoltre riconosciuto dall'art. 8 della Convenzione europea sui diritti dell'uomo, che inoltre vieta interferenze in tale ambito da parte dei pubblici poteri, ad eccezione di quelle previste dalla legge e per salvaguardare l'ordine pubblico. L'art. 7 della Carta dei diritti fondamentali dell'Unione europea, come noto dotata del medesimo valore giuridico dei Trattati istitutivi in virtù dell'art. 6 TUE, garantisce a ogni individuo il valore irrinunciabile del rispetto della vita privata. L'art. 8 della Carta compie un passo ulteriore, garantendo il diritto alla protezione dei dati personali e stabilendo che il loro trattamento deve avvenire secondo il principio di lealtà e per finalità prestabilite dalla legge. I valori appena ricordati sono alla base del sopra citato Regolamento di recente approvazione e devono guidare l'azione dell'Unione europea anche nella gestione della crisi migratoria.

3. La tutela dell'identità personale dei migranti all'epoca del GDPR

3.1. Dalla Direttiva 95/46 al Regolamento (UE) 2016/679

Il valore della privacy e il diritto alla riservatezza sono ormai da tempo parte fondamentale dell'*acquis communautaire*; già nel 1995, infatti, l'Unione europea aveva adottato una direttiva in materia di protezione dei dati personali[16] per far sì che i vari Paesi membri aggiornassero la propria legislazione in tale ambito.

[16] Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, in GUUE n.281 del 23 novembre 1995, 31-50.

La direttiva 95/46 rappresentava il testo di riferimento, a livello europeo, in materia di tutela della privacy e della riservatezza. Si riconosceva inoltre il valore della vita privata, sulla scia di quanto proclamato da atti internazionali quali la Convenzione 108: l'art. 1 della direttiva impegnava infatti gli Stati membri a riconoscere tale principio, con particolare attenzione alla tutela dei dati personali. Venivano fissati confini definiti alla raccolta di suddette informazioni, fissando inoltre per i Paesi membri l'obbligo di creare un'Autorità indipendente e garante della correttezza di tale raccolta. L'art. 29 della suddetta direttiva stabiliva la formazione di un gruppo di esperti a livello europeo, il cosiddetto art. 29 *Working Party*, formato da un rappresentante per Stato membro delle varie Autorità garanti e da un membro della Commissione, con un ruolo consultivo nei confronti delle istituzioni europee nella formulazione di proposte legislative in materia di trattamento dei dati personali.

Il continuo progresso tecnologico ha tuttavia messo a dura prova la menzionata direttiva in quanto l'esigenza di protezione non è rimasta costante nel corso degli anni e il livello di tutela accordato dalla normativa comunitaria si è rivelato inidoneo a salvaguardare le informazioni sensibili dai rischi posti dai nuovi mezzi di comunicazione[17]. Un ulteriore problema era costituito dalla diversità delle legislazioni nazionali in materia, considerato che una direttiva si limita a fissare un obbiettivo comune, lasciando ai vari Stati membri l'implementazione delle varie misure atte a raggiungerlo; alla luce di ciò, si comprende la decisione dell'Unione europea di emanare un regolamento, dato che – come noto – tale atto è obbligatorio nella sua interezza e immediatamente applicabile[18]. L'attuazione del regolamento non richiede quindi, in linea di principio, alcuna azione da parte dei vari Paesi UE.

Una simile caratteristica può rivelarsi assai utile nel trattamento dei dati personali dei migranti arrivati in territorio europeo, garan-

[17] B.A. Safari, *Intangible privacy rights: how Europe's GDPR will set a new global standard for personal data protection*, in *Seton Hall Law Review*, 2017, 47, 809-848.

[18] J.Wagner-A. Benecke, *National legislation within the framework of GDPR. Limits and opportunities of member State data protection law*, in *European data protection Law Review*, n.3/2016, 353-361.

tendo un'uniformità di applicazione che non subisce difformità secondo il Paese di sbarco.

3.2. Il criterio di applicazione territoriale del nuovo Regolamento

La sopra citata direttiva 95/46 stabilisce, all'art. 4 comma 1, il proprio campo di applicazione; rientrano in tale ambito le attività di trattamento dati svolte/espletate all'interno del territorio di uno Stato membro dell'Unione europea, o dello Spazio Economico Europeo (SEE). Tale previsione ha però limitato fortemente la tutela fornita dalla normativa europea rivelatasi, come detto, inadeguata a rispondere alle nuove esigenze di una connessione informatica globale. Le attività di aziende informatiche con sede negli Stati Uniti, si pensi a Google o Facebook a mero titolo di esempio, avrebbero potuto quindi evitare l'applicazione della normativa in questione. L'unico criterio determinante, secondo quanto previsto dal summenzionato art.4, è infatti il luogo fisico in cui vengono trattati i dati, non rilevando in alcun modo parametri alternativi quali la cittadinanza del soggetto interessato dal trattamento o la sua residenza abituale. Risulta evidente che una simile disposizione può condurre a una mancata tutela uniforme dei dati dei cittadini, europei e non, e che può essere facilmente aggirata. La direttiva non trovava inoltre applicazione relativamente alla cooperazione in materia penale e al trattamento di dati effettuato per finalità esclusivamente personale tra privati, come previsto dall'art. 3 punto 2.

La Commissione, attraverso una Comunicazione[19] del novembre 2010, evidenziava queste criticità, riconoscendo la necessità di una revisione normativa volta a determinare con certezza le competenze dei vari Paesi membri nell'ambito della protezione dei dati personali. Il nuovo Regolamento, prendendo spunto da quanto affermato nella recente giurisprudenza della Corte di giustizia[20], vuole invece tutelare

[19] Comunicazione, *Un approccio globale alla protezione dei dati personali nell'Unione europea*, COM (2010) 609, 4 novembre 2010.

[20] Una su tutte, Corte di giustizia, sentenza del 13 maggio 2014, *Google Spain Sl*, causa C-131/12, ECLI:EU:C:2014:317. Nella suddetta sentenza la Corte ha specificato la nozione di "stabilimento" presente nella direttiva 95/46, chiarendo che, qualora i dati personali vengano trattati da una succursale o agenzia situata all'interno del territorio europeo, tale trattamento sarà sottoposto alla direttiva. La pronuncia in questione ha quindi spinto a una riforma della normativa, facendo sì che non venga applicata in base al luogo di trattazione dei dati personali, ma secondo

qualsiasi soggetto, indipendentemente dalla sua cittadinanza o residenza abituale, anche qualora la gestione delle informazioni venga portata avanti fuori dal territorio europeo. L'art. 3 del GDPR stabilisce l'applicabilità del nuovo Regolamento indipendentemente dal fatto che il trattamento dei dati personali sia condotto all'interno dell'Unione europea. Il trattamento di suddetti dati sarà soggetto alle disposizioni del GDPR qualora abbia ad oggetto l'offerta di beni o servizi a soggetti che si trovano nell'Unione, o il monitoraggio del loro comportamento se questo si esplica nei confini europei. Il considerando 22 del Regolamento spiega che qualsiasi trattamento effettuato da una succursale o filiale stabilita nel territorio UE, anche se la gestione delle informazioni viene poi concretamente effettuata al di fuori dei confini europei, deve essere sottoposto alle disposizioni del GDPR; è qui evidente l'influenza della pronuncia *Google Spain*.

Alla luce di quanto detto, si comprende che il Regolamento trova applicazione anche nei confronti dei migranti arrivati in territorio europeo, che potranno quindi godere delle tutele previste dal GDPR indipendentemente dalla loro nazione di provenienza e dal luogo del trattamento dei loro dati.

3.3. Il principio della portabilità dei dati nel nuovo GDPR. Riflessi applicativi nella gestione della crisi migratoria

Il nuovo Regolamento prevede, all'art.20, il cd. diritto alla portabilità dei dati, che consente al soggetto interessato di richiedere le proprie informazioni personali fornite al responsabile del trattamento dati in un formato strutturato, di uso comune e leggibile attraverso mezzi automatici, senza che il predetto responsabile possa ostacolare o rifiutarsi di soddisfare tale richiesta. L'articolo in questione riconosce la possibilità di valutare quali sono le informazioni condivise e di riappropriarsene. Una simile facoltà dovrebbe permettere una più agevole circolazione dei dati personali, a favore dei consumatori che potranno rientrare in possesso delle informazioni cedute a un gestore di servizi per l'ottenimento di una prestazione al fine di rivolgersi a un altro operatore del settore[21].

la posizione dei soggetti titolari delle informazioni gestite, ossia se si trovano all'interno dei confini europei.

[21] L. Valle-L. Greco, *Transnazionalità del trattamento dei dati personali e tutela degli interessati, tra strumenti di diritto internazionale privato e la prospettiva di*

Il Regolamento sembra prevedere una sorta di "interoperabilità"[22] della lettura di tali dati da parte di qualsiasi gestore di servizi e porre dei requisiti minimi a cui i gestori del trattamento delle informazioni devono adeguarsi al fine di raggiungere l'obbiettivo della portabilità dei dati[23]. Lo stesso regolamento, tuttavia, al considerando 68 dispone altresì – apparentemente contraddicendosi – che il diritto del soggetto a trasmettere e ricevere i propri dati personali *non* crea un'obbligazione per il responsabile del trattamento ad adottare specifici sistemi tecnici e informatici.

L'applicazione di quanto previsto dall'art. 20 del Regolamento è soggetta inoltre a determinati requisiti legali, poiché può essere richiesta esclusivamente per i dati personali per cui il soggetto ha acconsentito al trattamento. Il diritto alla portabilità non viene esteso ai dati che il gestore del trattamento ha collezionato da altre fonti e che non provengono quindi dal diretto interessato. Si potrebbe perciò riscontrare una qualche contraddittorietà rispetto a quanto affermato dall'art. 15 (3) dello stesso Regolamento, che prevede il diritto per il soggetto interessato di richiedere una copia delle proprie informazioni trattate, senza però poterne domandare anche la portabilità. Al fine di ovviare a questa possibile discrasia, è stata proposta un'interpretazione del dettato normativo più ampia ed estensiva, includendo quindi anche dati generati da un fornitore di servizi attraverso processi quali l'utilizzo di algoritmi[24]. Un'ulteriore eccezione all'applicazione del diritto alla portabilità si ha quando il trattamento dei dati personali è necessario al perseguimento di finalità di pubblico interesse o quando è portato avanti da un'autorità pubblica nell'esercizio delle sue funzioni.

Quest'ultima previsione potrebbe rivestire una notevole importanza nella gestione delle informazioni sensibili dei migranti, specialmente se l'accoglienza di tali persone venisse qualificata, come

principi di diritto privato di formazione internazionale, in *Diritto dell'Informazione e dell'Informatica*, fasc. 2, 1 aprile 2017, 168 e ss.

[22] L. Scudiero, *Bringing your data everywhere: a legal reading of the right to portability*, in *European data protection Law Review*, 1/2017, 119-127.

[23] Article 29 Data Protection Working Party (A29 WP), *Guidelines on the right to data portability* (13 dicembre 2016) 16/EN WP 242, 4 http://ec.europa.eu/newsroom/article29/item-detail.efm?id=611233

[24] Article 29 Data Protection Working Party (A29 WP), cit.

prevedibile, attività di pubblico interesse o esercizio di pubbliche funzioni. Una simile determinazione farebbe sì che il diritto alla portabilità dei dati non debba essere applicato alle informazioni raccolte durante l'accoglienza dei migranti, causando però un possibile detrimento al diritto all'identità personale dei migranti stessi, che vedrebbero la loro facoltà di conoscere i propri dati raccolti limitata a quanto previsto dall'art. 15 (3) del Regolamento, che garantisce il diritto a richiedere una copia di dette informazioni, escludendone però la portabilità.

L'interoperabilità dei sistemi di collezione dei dati personali potrebbe però essere utile per uniformare le procedure di accoglienza tra i vari Paesi dell'Unione, permettendo inoltre una veloce circolazione di tali dati all'interno del territorio europeo, seguendo i movimenti dei migranti tra i vari Paesi.

3.4. Il trasferimento dei dati all'estero sotto la normativa del GDPR

La diffusione globale della rete internet ha reso ormai possibile il trasferimento di dati e informazioni tra i vari Paesi, senza che confini territoriali e diverse disposizioni normative nazionali possano essere di ostacolo. La diffusione e la commercializzazione di dati sono ormai elementi fondamentali dell'economia odierna.

Secondo la disciplina prevista dall'art. 25 della direttiva 95/46, trasferimenti transfrontalieri di informazioni sensibili possono essere autorizzati solo verso Paesi terzi che, su giudizio della Commissione europea, presentano un livello di tutela della riservatezza adeguato rispetto agli standard europei. La normativa prevede delle deroghe, elencate tassativamente, al giudizio preventivo della Commissione, che può essere ovviato qualora il trasferimento dei dati è necessario per finalità quali la chiusura di un contratto, la salvaguardia di un interesse pubblico o di un interesse fondamentale della persona.

Il nuovo GDPR dedica diversi articoli, dal 44 al 50, alla regolazione dei trasferimenti dei dati personali oltre i confini nazionali; il testo del regolamento riconosce il diritto all'identità personale e alla salvaguardia della riservatezza delle informazioni sensibili trattate oltre frontiera, riprendendo e specificando inoltre, all'art. 45, il concetto di "adeguatezza" che caratterizzava il giudizio della Commissione ai sensi della previgente disciplina. Lo standard di protezione richiesto al Paese terzo non deve essere identico a quello previsto dalla normativa europea, ma deve essere a questo equivalente, ap-

plicandolo inoltre alla luce di quanto previsto dalla Carta dei diritti fondamentali dell'Unione europea[25]. Il Regolamento specifica che la Commissione, nel suo giudizio di adeguatezza, è tenuta a verificare ulteriori criteri politici e sociali che dovrebbero evidenziare l'attenzione del Paese terzo alla corretta tutela dell'identità personale dei soggetti coinvolti, oltre quelli prettamente tecnico-giuridici. Il GDPR prevede inoltre un riesame su base quadriennale delle conclusioni formulate dalla Commissione nel suo giudizio, al fine di valutare eventuali evoluzioni da parte del Paese esaminato. L'art.49 elenca le deroghe, riprese perlopiù dalla previgente direttiva, che permettono il trasferimento transfrontaliero dei dati anche in mancanza dei requisiti summenzionati; un'importante aggiunta che viene fatta è relativa al perseguimento dell'interesse del titolare del trattamento, qualora questo abbia valutato tutte le circostanze del caso e abbia fornito adeguate garanzie di tutela dell'identità personale del soggetto interessato.

Simili trasferimenti di dati tra diversi Stati sono altrettanto importanti per la corretta gestione dei flussi migratori; le varie autorità nazionali hanno difatti la necessità di sapere le caratteristiche di detti flussi, considerando che spesso i migranti non si stabiliscono nel primo Paese di sbarco. Una condivisione di tali informazioni si rivela fondamentale anche per combattere fenomeni illegali come il traffico di esseri umani. L'art. 44 del GDPR permette il trasferimento dati anche con Organizzazioni internazionali, alcune delle quali impegnate nella gestione della crisi migratoria, creando quindi la possibilità di una collaborazione con gli Stati di origine dei migranti.

4. La tutela dei dati personali e la lotta al traffico illegale di esseri umani

Il tema della salvaguardia dell'identità personale è di primaria importanza nell'ambito della lotta al traffico illegale di esseri umani, con particolare attenzione a quanto concerne le informazioni sensibili delle vittime di tali odiosi traffici, come prescritto anche

[25] C. Kuner, *Reality and illusion in EU data transfer Regulation post Schrems*, in *German Law Journal*, 2017, 18, 881-914.

dall'art. 6 del "Palermo Protocol"[26].

La direttiva 2011/36[27] non prevede alcuna disposizione specifica in materia di tutela dei dati personali, limitandosi a segnalare che la normativa rispetta quanto previsto dalla Carta dei diritti fondamentali dell'UE e che le vittime hanno specifici diritti nei procedimenti penali riguardanti i traffici di cui sono stati oggetto. La legislazione attuale pone infatti l'attenzione principalmente sul rapporto tra rispetto dell'identità personale e lotta all'immigrazione illegale limitatamente al profilo processual-penalistico, ossia agli interessi delle vittime all'interno del processo[28]. Un'analisi delle conseguenze che strumenti di sorveglianza e prevenzione dei suddetti traffici possono avere sulla privacy dei soggetti coinvolti deve però prendere in considerazione non solo la fase processuale, ma anche la fase di raccolta e catalogazione dei dati personali che avviene durante le operazioni di sorveglianza, cercando di trovare un equilibrio tra il rispetto della riservatezza delle vittime e la lotta al traffico di esseri umani.

La geo-localizzazione può essere uno degli strumenti sopra menzionati; il tracciamento della posizione attraverso strumenti elettronici è ormai una realtà diffusa, e viene utilizzato anche per rilevare la posizione dei sospetti trafficanti nell'ambito delle indagini penali. Gli stessi trafficanti possono però utilizzare pratiche di sorveglianza simili, con lo scopo di controllare le proprie vittime e far sì che non riescano a sfuggire dalla propria rete di abusi. Nonostante i rischi che la geo-localizzazione può arrecare alla privacy delle persone coinvolte, essa può costituire un ottimo aiuto alla lotta contro i trafficanti. Al fine di ridurre i predetti rischi, possono essere previsti degli accorgimenti come una limitazione dell'utilizzo degli strumenti di tracciamento della posizione solo a casi eccezionali, di fronte al concreto

[26] Protocollo per la prevenzione, soppressione e repressione del traffico di persone, adottato dall'Assemblea Generale dell'ONU con la Risoluzione 55/25 del 15 novembre 2000.

[27] Direttiva 2011/36/UE del Parlamento europeo e del Consiglio, del 5 aprile 2011, concernente la prevenzione e la repressione della tratta di esseri umani e la protezione delle vittime, e che sostituisce la decisione quadro del Consiglio 2002/629/GAI, in GUUE, n.101, 15 aprile 2011, 180-190.

[28] F. Gerry-J. Muraszkiewicz-N. Vavoula, *The role of technology against human trafficking: reflections on privacy and data protection concerns*, in *Computer law e security review*, 2016, 32, 205-217.

sospetto di attività illegale. Il soggetto coinvolto può inoltre ritirare il proprio consenso alla condivisione dei dati relativi alla propria posizione in qualsiasi momento, anche durante il corso di un'indagine.

Le autorità nazionali utilizzano anche droni, ossia veicoli guidati a distanza che non necessitano di un pilota a bordo, nelle attività di pattugliamento dei confini e di prevenzione delle attività illegali come il traffico di esseri umani e l'immigrazione illegale. Lo spiegamento di droni da parte dei Paesi europei è ancora limitato[29], seppur si segnala il loro utilizzo da parte dell'Italia nell'ambito dell'operazione "Mare Nostrum"[30].

L'utilizzo di simili apparecchiature comporta però rilevanti rischi per l'integrità dell'identità personale, considerando che i droni sono spesso attrezzati con una telecamera per le riprese, che consente di raccogliere immagini idonee a identificare una persona. Alla luce di ciò, le azioni che vedono coinvolti tali strumenti devono essere compiute nel rispetto della normativa sulla privacy, ossia il GDPR per il territorio europeo. La sorveglianza operata dai droni si caratterizza per l'alta pervasività; possono essere infatti riprese immagini anche di soggetti non inclusi tra gli obbiettivi di dette operazioni. Deve inoltre esserci chiarezza nelle modalità di utilizzo di tali immagini, affinché non vi siano rischi di violazioni immotivate della privacy dei soggetti coinvolti.

5. Conclusioni

Il continuo progresso tecnologico ha portato a una costante evoluzione del diritto alla privacy, considerato ora come un diritto all'autodeterminazione informativa del singolo soggetto, che può quindi decidere quali dati personali rendere accessibili e secondo quali modalità. Questa evoluzione ha certamente influenzato anche

[29] L. Marin-K. Krajcíková, *Deploying drones in policing European borders: constraints and challenges for data protection and human rights*, in A. Završnik (a cura di), *Drones and Unmanned Aerial Systems: Legal and Social Implications for Security and Surveillance*, Londra, Springer, 2016.

[30] Amnesty International, *LivesAdrift: Refugees and Migrants in Peril in the Central Mediterranean* https://www.amnesty.org/en/documents/EUR05/006/2014/en/ accessed 15 October 2015 (consultato il 15 maggio 2018).

la normativa più recente in materia di privacy, ossia il più volte citato Regolamento (UE) 2016/679, che pone infatti al centro del trattamento dati proprio il soggetto interessato, il quale ha l'ultima parola sulla condivisione delle proprie informazioni sensibili.

Il nuovo Regolamento andrà ad incidere anche sulle pratiche di tutela dell'identità personale dei migranti e rifugiati che arrivano sul territorio europeo, in particolar modo attraverso alcune sue previsioni. Il principio della portabilità dei dati, pur formalmente non applicabile alle attività di gestione della crisi migratoria, potrebbe infatti, considerata la loro finalità di interesse pubblico, spingere le varie autorità nazionali a modificare i propri sistemi informatici all'insegna dell'interoperabilità, velocizzando la condivisione delle informazioni relative ai migranti che si spostano da un Paese all'altro dell'Unione europea. Il Regolamento disciplina inoltre il trasferimento transfrontaliero di suddette informazioni, permettendo quindi una maggiore collaborazione tra gli Stati di origine dei migranti e quelli di destinazione, al fine di garantire un'accoglienza più efficace, nonché di valutare le cause primarie di tali flussi migratori. Una simile condivisione di informazioni è possibile anche con le Organizzazioni internazionali attive in tale ambito. La tutela dell'identità personale è un tema che viene in rilievo anche nella lotta al traffico illegale di esseri umani, dato che strumenti di sorveglianza quali i droni o la geo-localizzazione potrebbero collezionare e catalogare dati personali di soggetti non direttamente coinvolti in tali traffici, nonché delle vittime stesse. Pur a fronte della necessità di continuare ad utilizzare tali strumenti, indubbiamente efficaci e proficui nel prevenire e sopprimere tali odiosi traffici, non possono trascurarsi i profili di rischio per la riservatezza delle persone coinvolte, di cui la legislazione deve quindi tenere conto.

Il trattamento di dati personali a fini di prevenzione, di indagine, di accertamento e di perseguimento di reati o di esecuzione di sanzioni penali: quali passi avanti alla luce dei recenti sviluppi?

Gianluca Borgia

Sommario: 1. Introduzione – 2. I punti critici della previgente disciplina eurounitaria – 3. La Direttiva 2016/680/UE tra problemi risolti e questioni aperte – 4. Prime considerazioni su alcuni aspetti del d.lgs. n. 51 del 2018 – 5. Note di chiusura

1. Introduzione

Il rapporto di complementarietà tra il Regolamento 2016/679/UE e la Direttiva 2016/680/UE[1] emerge chiaramente dal *considerando* n. 11 del primo fra i provvedimenti richiamati: se il trattamento dei dati

[1] Si tratta, rispettivamente, del Regolamento 2016/679/UE 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* e della Direttiva 2016/680/UE 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 2005/977/GAI del Consiglio.

personali risponde ad esigenze di carattere preventivo, processuale o sanzionatorio, la base normativa è rappresentata dalla Direttiva; se le finalità sono diverse ovvero se le autorità «proced[o]no ad un loro ulteriore trattamento per adempiere ad un obbligo legale cui sono soggett[e]», si applica il Regolamento[2]. Di qui, l'opportunità di soffermarsi – anche in un contesto come questo, per l'appunto dedicato all'entrata in vigore dell'atto regolamentare – su alcune importanti novità introdotte dalla richiamata Direttiva e dalla relativa disciplina di attuazione.

La riflessione non può che prendere le mosse dall'analisi delle questioni problematiche emerse già all'indomani dell'approvazione, sotto il previgente quadro istituzionale caratterizzato dalla struttura a "pilastri", della Decisione Quadro 2008/977/GAI dedicata alla protezione dei dati personali nell'ambito della cooperazione giudiziaria e di polizia in materia penale la quale, oltre a rappresentare l'antesignana della Direttiva, costituisce il primo atto dell'Unione diretto ad approntare un sistema di tutela uniforme dei dati trattati per finalità preventive e repressive nello spazio giudiziario europeo. Un'esigenza, quest'ultima, riconducibile all'esclusione dallo spettro applicativo della Direttiva 95/46/CE[3] (oggi integralmente sostituita, come noto, dal Regolamento 2016/679/UE) dei trattamenti effettuati per l'esercizio delle attività di cui ai titoli V e VI del Trattato sull'Unione europea[4] (i quali, nella versione "pre-Lisbona", si riferivano, rispettivamente, alla politica estera e di sicurezza comune e, appunto, alla cooperazione giudiziaria e di polizia in materia penale) cosicché, da

[2] F. Falato, *L'uso (preventivo e repressivo) di dati personali come compressione di un diritto inviolabile*, in *Giust. pen.*, 2016, f. 10, pt. 3, 568-569.

[3] Direttiva 95/46/CE del parlamento europeo e del Consiglio del 24 ottobre 1995 *relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*.

[4] L'art. 3 § 2 della Direttiva 95/46/CE stabiliva, infatti, che «Le disposizioni della presente direttiva non si applicano ai trattamenti di dati personali [...] effettuati per l'esercizio di attività che non rientrano nel campo di applicazione del diritto comunitario, come quelle previste dai titoli V e VI del trattato sull'Unione europea e comunque ai trattamenti aventi come oggetto la pubblica sicurezza, la difesa, la sicurezza dello Stato (compreso il benessere economico dello Stato, laddove tali trattamenti siano connessi a questioni di sicurezza dello Stato) e le attività dello Stato in materia di diritto penale».

un lato, tutto il settore *de quo* restava privo di quell'articolata tutela che, come opportunamente sottolineato, poteva essere considerata «quale *standard* mondiale della protezione dei dati personali»[5]; dall'altro, la salvaguardia del diritto all'autodeterminazione informativa non trovava una disciplina omogenea, ma veniva affidata, sul fronte comunitario, alle regole di volta in volta dettate in relazione ai singoli meccanismi di collaborazione interstatuale[6] e, sul fronte nazionale, alle varie normative interne.

Inoltre, a partire dal Programma dell'Aia del 4 novembre 2004, la protezione dei dati personali diventa una priorità per il settore della cooperazione giudiziaria e di polizia[7], e questo – è opportuno precisarlo – non solo e non tanto perché la realizzazione di un autentico spazio di libertà, sicurezza e giustizia, necessitava anche del rafforzamento della tutela dei diritti garantiti dalla CEDU e dalla Carta di Nizza, primi fra tutti quelli al rispetto della vita privata e alla protezione di dati personali[8]; ma anche e soprattutto in ragione della vieppiù crescente consapevolezza che l'esistenza di differenti livelli di protezione dei dati avrebbe potuto essere di intralcio a quella particolare forma di cooperazione rappresentata dallo scambio di informazioni che, proprio in quegli anni, iniziava a dare i suoi frutti[9].

[5] S. Allegrezza, *Giustizia penale e diritto all'autodeterminazione dei dati*, in D. Negri (a cura di), *Protezione dei dati personali e accertamento penale. Verso la creazione di un nuovo diritto fondamentale?*, Roma, Aracne, 2007, 80.

[6] Quali, ad esempio, quelle relative al funzionamento di *Eurojust* ed *Europol*, nonché quelle che riguardano il Sistema informativo di Schengen (SIS) e il Sistema informativo doganale (SID).

[7] Al punto n. 7 del Programma si afferma che «Lo scambio di informazioni fra autorità di contrasto è essenziale per combattere il terrorismo e per poter svolgere indagini relative alla criminalità transfrontaliera efficacemente. L'Unione deve favorire un dialogo costruttivo fra tutte le parti interessate per trovare soluzioni equilibrate fra la disponibilità delle informazioni e il rispetto di diritti fondamentali quali la tutela della privacy e la protezione dei dati personali. L'Ufficio europeo di polizia (Europol) ha un ruolo centrale in tale contesto».

[8] G. Di Paolo, *La circolazione dei dati personali nello spazio giudiziario europeo dopo Prüm*, in *Cass. Pen.*, 2010, 1978.

[9] Questa preoccupazione emerge in modo chiaro dalla lettura della Relazione alla *Proposta di decisione quadro del Consiglio sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale* COM (2005) 475 def.

2. I punti critici della previgente disciplina eurounitaria

Se questo è il terreno sul quale era stato edificato l'articolato della Decisione Quadro, è evidente come con l'approvazione di tale atto il legislatore europeo intendesse colmare un vuoto ormai non più sostenibile; secondo quanto stabilito dall'art. 1 § 1 l'ambito operativo dello strumento coincideva, infatti, con il settore della cooperazione giudiziaria e di polizia in materia penale.

Ma proprio dalla disposizione in parola emergeva anche un primo profilo problematico: la circostanza per cui la Decisione Quadro non si applicava ai trattamenti effettuati a livello domestico, ma riguardava soltanto quelli aventi ad oggetto lo scambio transnazionale di informazioni, denunciava l'urgenza di addivenire ad una tutela uniforme del diritto all'autodeterminazione informativa a cui si è fatto riferimento in precedenza[10].

Un ulteriore elemento di criticità si ravvisava, poi, nell'assenza di qualsiasi distinzione fra i dati personali in relazione allo *status* dei soggetti coinvolti dal momento che l'art. 2 – rubricato «Definizioni» – si limitava a delineare la nozione di "persona interessata" coincidente con quella di «persona fisica identificata o identificabile» (lett. a)[11]. Da ciò derivava un duplice ordine di conseguenze: in primo luogo, la mancanza di uno *standard* più elevato di garanzie per il trattamento dei dati relativi a persone – quali ad esempio i testimoni o le persone offese – che prendono sì parte al procedimento penale, ma non in ragione di un addebito a loro carico; in secondo luogo, l'impossibilità per le autorità riceventi di utilizzare immediatamente i dati, i quali necessitavano di una preliminare operazione volta a stabilirne la natura. Orbene, rispetto al primo ri-

[10] Come sottolinea B. Piattoli, *Sistema di protezione dei dati personali nel terzo pilastro: esigenze di tutela e di rafforzamento delle indagini*, in *Dir. pen. proc.*, 2007, 1688, è stato questo l'aspetto più controverso nel corso dei lavori preparatori.

[11] Nella medesima lettera si specifica, poi, che «si considera identificabile la persona che può essere identificata, direttamente o indirettamente, in particolare mediante riferimento a un numero di identificazione o a uno o più elementi caratteristici della sua identità fisica, fisiologica, psichica, economica, culturale o sociale».

lievo è appena il caso di sottolineare come la distinzione in diverse categorie di "interessati" rappresentasse un presupposto per il pieno rispetto del principio di proporzionalità che la stessa Decisione Quadro declinava all'art. 3[12]: la valutazione in ordine alla necessarietà e adeguatezza della compressione del diritto all'autodeterminazione informativa non poteva e non può, infatti, prescindere dal grado di coinvolgimento del soggetto interessato nella vicenda che legittima la raccolta dei dati[13].

Per ciò che concerne i cc.dd. "dati sensibili" (*id est* «dati personali relativi alla salute e alla vita sessuale o che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale»), la Decisione Quadro ne ammetteva il trattamento solo in casi "eccezionali", secondo una clausola che risultava tutt'altro che determinata. Invero, tali dati potevano essere impiegati laddove ciò fosse "strettamente necessario" e la legislazione nazionale avesse previsto "adeguate garanzie". Non stupisce, allora, che durante l'*iter* di approvazione, il Parlamento europeo avesse proposto l'introduzione di un corredo di guarentigie più ampio, tra cui quella della previa autorizzazione da parte dell'autorità giudiziaria[14].

Rispetto al diritto di accesso della persona interessata dal trattamento, appariva difficilmente qualificabile come tale il diritto, previsto dall'art. 17, di ottenere «"almeno" conferma» del fatto che i dati che la riguardano fossero stati trasmessi o resi disponibili (lett. a) e che fossero state effettuate tutte le verifiche necessarie (lett. b)[15].

[12] Art. 3 («Principi di legalità, proporzionalità e finalità») § 1: «I dati personali possono essere raccolti dalle autorità competenti soltanto per finalità specifiche, esplicite e legittime nell'ambito dei loro compiti e possono essere trattati solo per la finalità per la quale sono stati raccolti. Il trattamento dei dati deve essere legale e adeguato, pertinente e non eccessivo rispetto alle finalità per le quali sono stati raccolti».

[13] Cfr. F. Morelli, *Data Protection Issues in Transnational Financial-Economic Investigations*, in A. Bernanrdi-D. Negri (a cura di), *Investigating European Fraud in the EU Member States*, Oxford, Bloomsbury, 2017, 147.

[14] Ancora G. Di Paolo, *La circolazione dei dati*, cit., 1984.

[15] Cfr. M. Fumagalli Meraviglia, *Le nuove normative europee sulla protezione dei dati personali*, in *Diritto comunitario e degli scambi internazionali*, 2016, 9.

Anche il regime dettato per lo scambio con Paesi non facenti parte dell'Unione europea destava non poche perplessità. Presupposto necessario affinché il trasferimento potesse aver luogo era che lo Stato ricevente assicurasse un adeguato livello di protezione; una garanzia, quest'ultima, che veniva richiesta, però, solo nel caso in cui i dati fossero già stati oggetto di un preventivo scambio fra Stati membri[16]. In altri termini, i dati personali originati nel territorio dell'UE e trasmessi a Paesi terzi erano passibili di livelli di protezione diversi a seconda che la trasmissione dovesse essere effettuata direttamente dallo Stato membro che li aveva raccolti oppure attraverso la mediazione di un altro Paese dell'Unione[17].

Da ultimo, è opportuno osservare come la Decisione Quadro lasciasse impregiudicati gli altri atti eurounitari adottati in precedenza per i quali fosse stata dettata una disciplina specifica, indipendentemente dal livello di tutela del diritto di autodeterminazione informativa (art. 28)[18]. Tale opzione, che finiva per attribuire alla Decisione Quadro una mera funzione sussidiaria, era da imputarsi alle raccomandazioni espresse dal Garante europeo della protezione dei dati, il quale, però, aveva affermato che il provvedimento normativo in esame non avrebbe dovuto trovare applicazione «qualora un altro strumento giuridico specifico adottato in virtù del titolo VI del trattato UE [prevedesse] condizioni o restrizioni "più" precise per il trattamento dei dati o per l'accesso ai dati»[19]; e questo, evidentemente, sulla base di un giudizio comparativo che non era dato riscontrare nel testo della Decisione Quadro.

[16] Prevede infatti l'art. 13 che il trasferimento può avvenire solo se «il paese terzo o l'organismo internazionale interessati assicurano un adeguato livello di protezione» (lett. d); una tutela che, però, è riconosciuta, a mente del comma 1, ai soli «dati personali trasmessi o resi disponibili dall'autorità competente di un altro Stato membro».

[17] In questi termini, G. Di Paolo, *La circolazione dei dati*, cit., 1985.

[18] Oltre agli strumenti richiamati nel precedente paragrafo (v. *supra* § 1, 1) viene in considerazione, ad esempio, la Decisione 2008/815/GAI *sul potenziamento della cooperazione transfrontaliera, soprattutto nella lotta al terrorismo e alla criminalità transfrontaliera* che, nel recepire nel quadro giuridico dell'Unione la sostanza delle disposizioni del Trattato di Prüm, disciplina il trasferimento automatizzato tra Stati membri di profili DNA, dati dattiloscopici e dati nazionali di immatricolazione dei veicoli.

[19] Garante europeo della protezione dei dati 2006/C 47/12.

3. La Direttiva 2016/680/UE tra problemi risolti e questioni aperte

Venendo ai contenuti della Direttiva – la quale, a seguito del Trattato di Lisbona, trova la propria base giuridica nell'art. 16 TFUE[20] – e ponendo mente, anzitutto, al profilo concernente lo spettro applicativo, si ha subito la sensazione di un cambio di passo: l'art. 1, infatti, non ne circoscrive la portata al solo settore della cooperazione, ma si riferisce, più in generale, al trattamento effettuato «a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia e la prevenzione di minacce alla sicurezza pubblica».

Sennonché, il successivo art. 2 § 3 stabilisce che la Direttiva non copre i trattamenti «effettuati per attività che non rientrano nell'ambito di applicazione del diritto dell'Unione» (e quelli «posti in essere da istituzioni, organi o organismi dell'Unione»). Si potrebbe quindi pensare che, nonostante la lettera del primo fra gli articoli richiamati, il perimetro della Direttiva coincida, di fatto, con quello della Decisione Quadro[21]. In realtà, come emerge dal *considerando* n. 14, ai fini della Direttiva, il riferimento al diritto eurounitario vale soltanto ad escludere dallo spettro di quest'ultima «le attività concernenti la sicurezza nazionale» e quelle che attengono alla politica estera e di sicurezza comune[22].

[20] Tale articolo dispone, infatti, al § 1, che «Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano» e, al § 2, che «Il Parlamento europeo e il Consiglio, deliberando secondo la procedura legislativa ordinaria, stabiliscono le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale da parte delle istituzioni, degli organi e degli organismi dell'Unione, nonché da parte degli Stati membri nell'esercizio di attività che rientrano nel campo di applicazione del diritto dell'Unione, e le norme relative alla libera circolazione di tali dati. Il rispetto di tali norme è soggetto al controllo di autorità indipendenti».

[21] Questa la tesi di F. Sorrentino, *Il controllo del garante per la protezione dei dati personali e l'autorità giudiziaria secondo le più recenti norme eurounitarie*, in *Questione giustizia*, 15 febbraio 2018, § c).

[22] In questo senso deve leggersi il riferimento, contenuto nel *considerando* n. 14, al «Titolo V, capo 2, del Trattato sull'Unione europea».

Chiarito tale equivoco, sembrerebbe comunque porsi un problema di coordinamento tra la formula "sicurezza nazionale" utilizzata dal suddetto *considerando* e l'ultimo inciso dell'art. 1 che richiama l'apparentemente simile "sicurezza pubblica"[23]. Nondimeno, anche questo specifico profilo può essere risolto e, segnatamente, facendo leva sui lavori preparatori. Invero, il riferimento alla "sicurezza pubblica" non figurava nella versione originaria dell'art. 1, ma è frutto di una successiva modifica dovuta all'esigenza, particolarmente sentita dalle delegazioni di alcuni Paesi membri, di far rientrare nel perimetro della Direttiva anche quelle attività di polizia che, secondo il loro diritto interno, non possono considerarsi poste in essere a fini di prevenzione, indagine, accertamento e perseguimento di reati. Tuttavia, non essendo possibile rinvenire, in ambito europeo, una definizione univoca di "sicurezza pubblica" in grado di scongiurare la violazione dell'art. 4 § 2 TUE che, come noto, affida in via esclusiva agli Stati membri la competenza in tema di "sicurezza nazionale", per fugare ogni dubbio si è proceduto a chiarire i contenuti della nozione di "sicurezza pubblica" tanto in negativo, quanto in positivo. Così, dal *considerando* n. 14 emerge che il concetto di "sicurezza nazionale", in quanto escluso dal perimetro della Direttiva, non rientra in quello di "sicurezza pubblica", mentre dal *considerando* n. 12 si ricava che quest'ultimo coincide con le attività condotte dalla polizia «senza previa conoscenza della rilevanza penale di un fatto» e che tali attività «possono comprendere anche l'esercizio di poteri mediante l'adozione di misure coercitive quali le attività di polizia in occasione di manifestazioni, grandi eventi sportivi e sommosse»[24].

Con riguardo, poi, alla necessità di operare una differenziazione "soggettiva" dei dati, si assiste alla previsione di quattro categorie di interessati: a) «persone per le quali vi sono fondati motivi di ritenere che abbiano commesso o stiano per commettere un reato»; b) «persone condannate per un reato»; c) «vittime di reato o [...]

[23] V. C. Di Francesco Maesa, *Balance between Security and Fundamental Rights Protection: An Analysis of the Directive 216/651 on the use of passenger name record (PNR)*, in *Eurojus*, 24 maggio 2016, § 3.

[24] V., in particolare, il Documento del Consiglio dell'Unione europea del 25 novembre 2014 reperibile all'indirizzo *http://data.consilium.europa.eu/doc/document/ST-15730-2014-INIT/it/pdf*

persone che alcuni fatti autorizzano a considerare potenziali vittime di reato»; d) «altre parti rispetto a un reato, quali le persone che potrebbero essere chiamate a testimoniare nel corso di indagini su reati o di procedimenti penali conseguenti, le persone che possono fornire informazioni su reati o le persone in contatto o collegate alle persone di cui alle lettere a) e b)» (art. 6). In questo senso, il fatto che non sia stato accolto il suggerimento del Parlamento europeo di introdurre una disposizione che regolasse anche le conseguenze di una tale distinzione in categorie[25], disvela come alla base della novità vi sia l'esigenza di rendere più efficace lo scambio informativo tra autorità, ma non quella di calibrare il livello di protezione dei dati a seconda del coinvolgimento del soggetto nel procedimento così da assicurare, *ex ante* e sulla base di parametri prestabiliti, il rispetto del principio di proporzionalità che pure la Direttiva sancisce all'art. 4 § 1 lett. c.

In relazione ai dati sensibili, oltre alla ricomprensione in tale classe dei dati genetici, biometrici e relativi all'orientamento sessuale, merita di essere segnalata l'introduzione di due ulteriori requisiti che contribuiscono a rafforzare il carattere di eccezionalità del trattamento in questione. Essi si sostanziano nella necessità che il trattamento sia, anzitutto, autorizzato dal diritto dell'Unione o da quello nazionale e, inoltre, finalizzato alla salvaguardia di un interesse vitale dell'interessato o di un altro soggetto (art. 10 lett. a e b). Ciò detto, permane anche per questa categoria di dati la logica per cui l'intervento del giudice può aver luogo solo dopo che la violazione si è verificata, non essendo l'autorità procedente tenuta a richiedere l'autorizzazione a un organo giurisdizionale.

Circa i diritti dei soggetti interessati, è degna di apprezzamento la nuova configurazione del diritto di accesso. Eliminato l'avverbio "almeno", l'interessato, ricevuta conferma del fatto che è in corso un trattamento di dati che lo riguarda, ha infatti non solo il diritto di accedere ai propri dati, ma anche quello di conoscere la finalità e la base giuridica del trattamento, le categorie di dati personali trattati, i destinatari a cui i dati in questione sono stati trasmessi, il periodo di conservazione, nonché le facoltà che gli spettano (art. 14).

[25] M. Fumagalli Meraviglia, *Le nuove normative europee sulla protezione dei dati personali*, cit., 37.

In secondo luogo, a chiusura del capo III dedicato, appunto, ai diritti dell'interessato, si introduce una disposizione *ad hoc* per l'ipotesi in cui i dati figurino in una decisione giudiziaria, in un casellario o in un fascicolo giudiziario oggetto di trattamento nel corso di un'indagine o di un procedimento penale. In particolare, al ricorrere di tali evenienze, gli Stati membri possano continuare ad applicare la disciplina interna in tema di esercizio dei diritti dell'interessato (art. 18). Come è stato sottolineato, una simile previsione è in grado di dimidiare l'efficacia della Direttiva[26], rimettendo di fatto alla sensibilità dei singoli legislatori nazionali il raggiungimento di quel livello uniforme di salvaguardia del diritto all'autodeterminazione informativa della cui importanza si è già detto. Se questo è vero, è altresì evidente che la Direttiva non lascia completamente liberi gli Stati membri e non è dunque priva, almeno in potenza, di qualsiasi effetto armonizzante: essa, infatti, nel circoscrivere la possibilità in parola alle sole modalità di "esercizio" dei diritti, stabilisce una obbligazione di risultato per gli Stati membri, i quali potranno sì mantenere in vigore le disposizioni previste dall'ordinamento interno ma, laddove ciò non bastasse ad assicurare i diritti riconosciuti dal testo eurounitario, dovrebbero comunque integrarle o prevederne di nuove.

Completamente risolta può dirsi, poi, la problematica che riguardava la trasmissione dei dati a Paesi terzi. La regola generale è, infatti, quella per cui, indipendentemente dal luogo in cui essi sono stati raccolti, spetta alla Commissione, sulla base di criteri specificamente individuati dalla stessa Direttiva, stabilire preventivamente se il Paese di destinazione assicuri un adeguato livello di protezione e se sia, quindi, possibile procedere al trasferimento (artt. 35 ss.).

Quanto al rapporto con gli strumenti preesistenti, stando al disposto dell'art. 60, la situazione sembrerebbe sostanzialmente invariata, sebbene dal testo del successivo art. 62 § 4 sia dato comprendere come la scelta di non intaccare gli atti adottati nel settore della cooperazione giudiziaria in materia penale e di polizia sia, in realtà, solo momentanea; entro un anno dalla scadenza del termine di trasposizione la Commissione dovrà, infatti, riesaminare tali atti per

[26] Cfr. C. Di Francesco Maesa, *Balance between Security and Fundamental Rights Protection*, cit., § 3.

formulare le opportune proposte di modifica al fine di allinearli ai contenuti della Direttiva e garantire, così, un approccio coerente alla protezione dei dati personali.

4. Prime considerazioni su alcuni aspetti del d.lgs. n. 51 del 2018

Spostando l'attenzione sul piano interno, lo scorso 18 maggio è stato approvato il d.lgs. n. 51 di attuazione della Direttiva che, peraltro, è entrato in vigore proprio nel primo dei due giorni durante i quali si è svolto questo Convegno.

Non essendo possibile in questa sede passare in rassegna ogni singola disposizione dell'articolato[27], merita appuntare l'attenzione su quei profili che investono le questioni trattate nei paragrafi precedenti al fine di verificare se, ed in che modo, le problematiche che ancora residuano sul piano eurounitario, siano state affrontate a livello nazionale.

È evidente, anzitutto, che per il legislatore delegato la Direttiva si applica anche al trattamento *purely domestic*: come si evince dalla Relazione illustrativa, infatti, nel recepire la normativa sovranazionale si è inteso, prima di tutto, predisporre una regolamentazione organica del trattamento dei dati personali delle persone fisiche per fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, superando in gran parte quella contemplata nei titoli I e II della parte II seconda del Codice della privacy[28] che fino ad ora aveva rappresentato la disciplina di riferimento per i trattamenti effettuati a livello nazionale. Il decreto legislativo interviene, così, ad integrare le disposizioni di cui agli artt. da 46 a 52 Co-

[27] Per un primo esame dei contenuti del decreto legislativo v. A. Scarcella, *Trattamento dati personali in* ámbito *penale: in G.U. il D.Lgs. che attua la direttiva 2016/680/UE*, in *il Quotidiano Giuridico*, 25 maggio 2018, 11-13; S. Carrer, Privacy *e diritto penale: approvato in via definitiva il d.lgs. 51/2018 che attua la direttiva europea sulla tutela dei dati personali a fini di pubblica sicurezza e penali*, in *Giurisprudenza Penale* (web), 30 maggio 2018, 1-2.

[28] Relazione illustrativa, trasmessa alla Presidenza del Senato il 21 febbraio 2018, è reperibile all'indirizzo *http://www.senato.it/service/PDF/PDFServer/BGT/1066660.pdf*

dice della privacy che riguardano il settore giudiziario[29] e ad assorbire quelle previste dagli artt. da 53 a 57 del medesimo codice concernenti i trattamenti effettuati da parte delle forze di polizia (art. 49).

In tema, poi, di dati sensibili, il decreto legislativo non aggiunge nulla rispetto al contenuto della previsione sovranazionale, di cui riproduce sostanzialmente il testo (art. 7).

Viene rimessa pressoché nella sua interezza alla successiva approvazione di un D.P.R. adottato ai sensi dell'art. 17 co. 1 della legge 23 agosto 1988, n. 400 la disciplina dell'esercizio dei diritti relativi a dati trattati per finalità diverse da quelle riconducibili al processo penale[30]. Sul punto si osserva che è la stessa Direttiva a precisare, al *considerando* n. 33, che quando la norma eurounitaria fa riferimento al «diritto dello Stato» non è richiesta «necessariamente l'adozione di un atto legislativo», ben essendo possibile il ricorso ad una fonte secondaria.

Quando invece il trattamento riguardi dati personali contenuti in una decisione giudiziaria, in atti o documenti oggetto di trattamento nel corso di accertamenti o indagini, nel casellario giudiziale o in un fascicolo oggetto di trattamento nel corso di un procedimento penale o in fase di esecuzione penale troveranno applicazione le disposizioni del codice di procedura penale e quelle relative al Testo unico sul casellario giudiziale[31]. Con l'art. 14 comma 1 è stata, infatti, esercitata la facoltà di rimettere alla normativa interna la disciplina dell'esercizio dei diritti di informazione, di accesso, di rettifica o cancellazione, nonché di limitazione del trattamento risultando così avvalorate le preoccupazioni legate al profilo dell'uniformità della tutela in ambito eurounitario.

Ponendo mente alla seconda parte della disposizione ora richiamata, si potrebbe però pensare – riprendendo quanto già evidenziato nel paragrafo precedente – che un qualche effetto positi-

[29] Sul punto è opportuno evidenziare che gli artt. da 46 a 49 sono stati abrogati dal d.lgs. 10 agosto 2018, n. 101 recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento 2016/679/UE.

[30] Dispone, infatti, l'art. 5 co. 2 che con il D.P.R. sono individuate anche «le modalità e le condizioni» per l'esercizio dei diritti di cui agli artt. 9 («Comunicazioni e modalità per l'esercizio dei diritti dell'interessato»), 10 («Informazioni da rendere disponibili e fornire all'interessato»), 11 («Diritto di accesso dell'interessato») e 13 («Esercizio dei diritti dell'interessato e verifica da parte del Garante»).

[31] D.P.R. 14 novembre 2002, n. 313.

vo la Direttiva l'abbia pur sortito. La previsione introduce, infatti, quella che lo stesso legislatore definisce una "norma di chiusura" volta a evitare che diritti riconosciuti dalla Direttiva restino sguarniti di tutela in quanto non contemplati dalle disposizioni processuali che, come detto, continuano, immutate, a regolare il diritto all'autodeterminazione informativa in questo specifico ambito. In particolare, chiunque vi abbia interesse può, durante o dopo il procedimento penale, chiedere la «rettifica, la cancellazione o limitazione» dei dati che lo riguardano, secondo un meccanismo che rinvia, quanto alle modalità, all'art. 116 c.p.p. in tema di accesso agli atti, quanto alla procedura, all'art. 130 c.p.p. relativo alla correzione di errori materiali. Sennonché, la circostanza per cui non è stato richiamato il diritto di accesso o, quantomeno, quello di avere conoscenza del fatto che sia in corso o sia stato effettuato un trattamento, fa venir meno il presupposto stesso per esercitare tutti gli altri diritti di modo che la norma non pare in grado di fornire un reale apporto.

Si consideri la questione che investe la disciplina delle intercettazioni e, segnatamente, il diritto di ottenere la distruzione delle registrazioni non acquisite, di cui all'art. 269 c.p.p. così come recentemente novellato[32]. Secondo quanto previsto dal comma 2 di tale articolo, il diritto *de quo* viene riconosciuto a tutti gli interessati. Nondimeno, occorre osservare che perché gli interessati possano chiedere la distruzione dei dati intercettati è necessario che siano al corrente della loro stessa esistenza. In questo senso, non si comprende come un soggetto terzo estraneo ai fatti oggetto di accertamento potrebbe esercitare un siffatto diritto posto che, in quanto terzo, non viene informato dell'avvenuta captazione ed è escluso dalle dinamiche acquisitive; e posto altresì che il comma 1 del suddetto articolo riconosce il diritto di accedere all'archivio in cui sono contenute le conversazioni intercettate esclusivamente (al p.m., al gip e) ai difensori dell'imputato. Verrebbe da dire che

[32] Sul rapporto fra diritto all'autodeterminazione informativa e intercettazioni v., fra i molti, A. Camon, *Il diritto della* privacy *di fronte alle intercettazioni: le circolari delle procure ispirano la riforma Orlando*, in *Arch. pen.*, 2017, f. 2, 639 ss.; G. Giostra, *Intercettazioni fra indagini e* privacy. *Primo, evitare soluzioni improvvisate*, in *D&G*, 31/2006, 99 s.

l'unica situazione in cui il terzo è messo in condizione di esercitare il diritto alla distruzione è proprio quella che la disposizione in esame dovrebbe evitare, ovvero quella della c.d. "fuga di notizie". Ecco che, muovendo dai rilievi di chi si è occupato di questo aspetto prima ancora che la Direttiva trovasse attuazione, l'inclusione nell'art. 14 comma 1 seconda parte anche del diritto di ottenere informazioni sull'esistenza del trattamento avrebbe consentito al terzo di avvalersi della facoltà di cui si discute[33].

Infine, in relazione alla suddivisione degli interessati in diverse classi, si è in presenza di una mera traduzione della previsione eurounitaria nelle categorie interne del diritto processuale penale, senza però tenere in considerazione le divergenze che possono sussistere a livello definitorio tra l'ordinamento dell'Unione e quello italiano. È quello che accade, in particolare, con l'espressione contenuta nella lett. a dell'art. 6 della Direttiva «persone per le quali vi sono fondati motivi di ritenere che abbiano commesso o stiano per commettere un reato» implementata dall'art. 4 comma 1, attraverso il ricorso alle nozioni di "persone sottoposte a indagini" e "imputati"[34]. Da qui, l'impossibilità di rinvenire una collocazione per i dati trattati per finalità che rientrano nello spettro della Direttiva, ma relativi a interessati che non assumono la qualità di indagato, come accade nel caso dei dati concernenti gli "indiziati" di alcuni particolari reati che, in quanto tali, possono essere destinatari di una c.d. "misura di prevenzione".

[33] Cfr. S. Renzetti, *Una riforma (radicale?) per tornare allo spirito originario della legge: la nuova disciplina acquisitiva delle intercettazioni tra legalità, diritto vivente e* soft law, in *Legisl. pen.* (web), 4 aprile 2018, 66-71, la quale, durante l'*iter* di approvazione del d.lgs. 51/2018, auspicava, sulla base dell'art. 11 della Direttiva («Diritto di accesso dell'interessato»), il riconoscimento del diritto del terzo di richiedere ed ottenere informazioni sull'esistenza di «intercettazioni che lo coinvolgono e, in caso di risposta affermativa, di ottenere la possibilità di ascolto delle registrazioni, al fine ultimo di attivare la procedura di distruzione di cui all'art. 269 Cpp» comma 3; 71.

[34] Per un'efficace disamina delle differenze che sussistono fra il termine "sospettato" a cui la formulazione dell'art. 6 lett. a rinvia e quello di "indagato", v. B. Galgani, *Report on Italy*, in *Committee on Civil Liberties, Justice and Home Affairs, EU and Member States' policies and laws on persons suspected of terrorism-related crimes*, Bruxelles, European Union, 2017, 103-107.

5. Note di chiusura

Seppur focalizzata sulle problematiche emerse a seguito dell'adozione della Decisione Quadro, la disamina fin qui condotta mette in evidenza come gli sforzi normativi profusi si siano essenzialmente incentrati sull'esigenza di promuovere la collaborazione interstatuale piuttosto che su quella di salvaguardare più efficacemente il diritto all'autodeterminazione informativa. Di ciò non c'è da stupirsi in quanto, differentemente da quello che si potrebbe pensare, la logica sottesa ai recenti mutamenti non differisce di molto da quella che circa dieci anni fa aveva ispirato l'emanazione della Decisione Quadro. Come si legge, infatti, nel *considerando* n. 7 della Direttiva, l'uniformazione e l'innalzamento del livello di protezione dei dati personali si rendono necessari perché «essenzial[i] al fine di garantire un'efficace cooperazione giudiziaria in materia penale e di polizia».

Senza disconoscere i progressi che innegabilmente hanno caratterizzato i trattamenti che rientrano nel dominio della Direttiva anche sotto l'aspetto della salvaguardia dei diritti degli interessati, in definitiva si ha la sensazione che le questioni che residuano non potranno trovare soluzione se non attraverso un ripensamento del rapporto tra diritto all'autodeterminazione informativa ed esigenze di prevenzione, di indagine, di accertamento e di perseguimento di reati o di esecuzione di sanzioni penali. In altre parole, occorre affrancarsi dall'idea che la protezione dei dati personali debba essere valorizzata solo ed in quanto strumentale a soddisfare le necessità appena menzionate, delle quali dovrebbe, viceversa, rappresentare il presupposto legittimante.

Indice degli Autori

- **Antonina Astone**, ricercatrice di Diritto privato, Università degli Studi di Messina.
- **Gianluca Borgia**, dottorando di ricerca in diritto dell'Unione europea e ordinamenti nazionali, Università degli Studi di Ferrara.
- **Federica Casarosa**, research fellow EUI.
- **Maria Concetta Causarano**, dottoranda di ricerca in Diritto privato, Università di Pisa.
- **Aurora Cavo**, avvocato del Foro di Lucca.
- **Enrico Cottu**, dottore di ricerca in Diritto e Politiche UE, Università degli Studi di Ferrara.
- **Vicenzo Cuffaro**, ordinario di Diritto privato, Università degli Studi Roma Tre.
- **Alberto De Franceschi**, associato di Diritto privato, Università degli Studi di Ferrara.
- **Roberto D'Orazio**, funzionario parlamentare presso la Camera dei Deputati.
- **Maria Samantha Esposito**, dottoressa di ricerca in Diritto civile, assegnista Politecnico di Torino.
- **Fernanda Faini**, dottoressa di ricerca Università di Bologna, Responsabile Assistenza giur. amministrazione digitale Regione Toscana.
- **Fiore Fontanarosa**, ricercatore di Diritto privato comparato, Università degli Studi del Molise.
- **Mirko Forti**, dottorando di ricerca in Diritto dell'Unione europea, Università degli Studi di Genova.
- **Augusta Iannini**, vice presidente Autorità Garante per la Protezione dei Dati Personali.
- **Emma A. Imparato**, associato di Diritto pubblico, Università degli Studi di Napoli L'Orientale.

- **Gianclaudio Malgieri**, avvocato, dottorando di ricerca Vrije Universiteit, Brussel.
- **Alessandro Mantelero**, associato di Diritto privato, Politecnico di Torino.
- **Joana Marí**, responsable de evaluación y estudios tecnológicos, Autoritat Catalana de Protecció de Dades.
- **Edoardo Mazzanti**, dottore di ricerca in Diritto penale, Scuola Superiore Sant'Anna, Pisa.
- **Cristina Pauner Chulvi**, profesora titular de Derecho Constitucional, Universitat Jaume Castellón I.
- **José Luis Piñar Mañas**, catedrático de Derecho Administrativo, Università CEU Sau Pablo-Madrid, Presidente de la Sección de Derecho Público de la Comisión General de Codificación, ex Director de la Agencia Española de Protección de Datos.
- **Franco Pizzetti**, docente di Diritto costituzionale, Università di Torino e LUISS, già Presidente Autorità Garante per la Protezione dei Dati Personali.
- **Dianora Poletti**, ordinario di Diritto privato e di Diritto dell'informatica, Università di Pisa.
- **Giulio Ramaccioni**, ricercatore in Diritto civile, Università degli Studi di Perugia.
- **Giorgio Resta**, ordinario di Diritto privato comparato, Università degli Studi Roma Tre.
- **Gabriele Rugani**, dottorando di ricerca in Scienze giuridiche, Università di Pisa.
- **Salvatore Sica**, ordinario di Istituzioni di Diritto Privato, Università degli Studi di Salerno.
- **Guido Scorza**, avvocato, team Trasformazione Digitale della Presidenza del Consiglio dei Ministri.
- **Matteo Trapani**, assegnista di ricerca in Diritto costituzionale, Università di Pisa.
- **Mònica Vilasau Solana**, profesora de Derecho Civil, Universitat Oberta de Catalunya.

Finito di stampare nel mese di dicembre 2018
da Tipografia Impressum srl - Carrara (MS)
per conto di Pisa University Press

L'entrata in vigore del Reg. UE 2016/679 in materia di protezione dei dati personali (GDPR) e l'inizio di operatività dello stesso hanno rappresentato un punto di arrivo di un lungo processo di riforma, ma hanno altresì costituito il momento di inizio di una, non meno complessa, fase di applicazione. Fase che già suscita diversi interrogativi e richiede una riflessione giuridica che guardi oltre i confini nazionali e si dimostri attenta alle concrete applicazioni della società digitale ed alle nuove sfide che il rapido evolvere del progresso tecnologico pone.

Questo volume, che raccoglie i contributi di studiosi e regolatori, con uno sguardo su due ordinamenti, rappresenta un tentativo concreto di aprire il dibattito sul tema. Mostra inoltre la volontà dell'accademia di dar vita ad una consapevole e dialogante riflessione sull'integrazione fra diritto e tecnologia, condotta con piena contezza delle istanze della società e dell'esigenza di fornire a queste risposta.

Alessandro Mantelero Professore associato di Diritto Privato presso il Politecnico di Torino, è rapporteur su *Artificial Intelligence* e dati personali per il Consiglio d'Europa. Partecipa al dibattito ed alla ricerca internazionale in materia di *data protection* ed ha ricoperto il ruolo di esperto per l'UN-ILO, l'EU Agency for Fundamental Rights, l'UN-OHCHR, la Commissione europea, il Ministero della giustizia e l'AGCOM.

Dianora Poletti Professore ordinario di Diritto Privato presso l'Università di Pisa, è docente di Diritto dell'Informatica e direttrice del Master in Internet Ecosystem: Governance e diritti, attivo nello stesso ateneo. È autrice di pubblicazioni e ha organizzato numerosi seminari e convegni aventi ad oggetto le tematiche del diritto dell'*internet* e delle nuove tecnologie. Ha curato la pubblicazione del primo volume della presente collana.