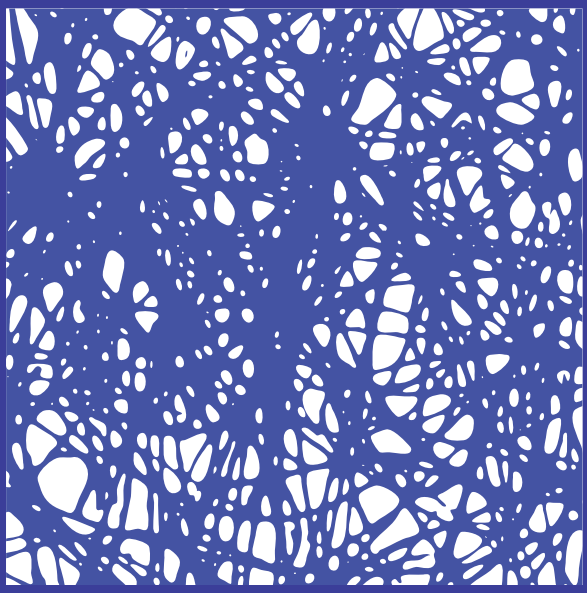
STUDI IN TEMA DI
INTERNET
ECOSYSTEM

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 978-88-3339-167-0

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.

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.

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.

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.