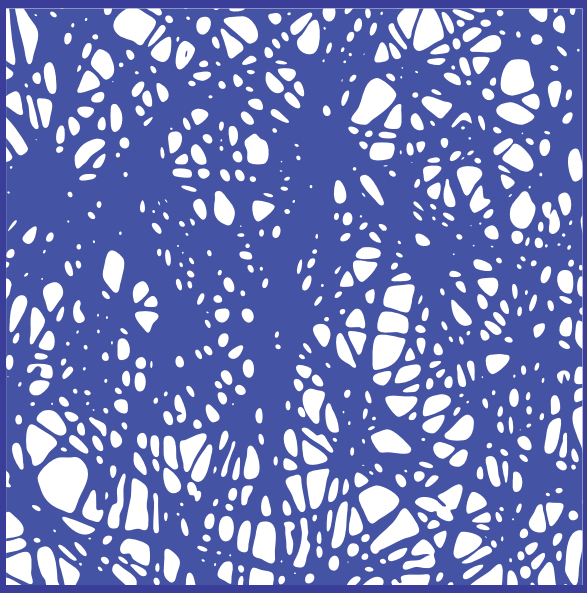
STUDI IN TEMA DI
INTERNET
ECOSYSTEM

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

# 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.