Introduzione

di *Franco Pizzetti*

Questo volume si compone di tre Parti.

La Parte Prima è dedicata a una analisi molto ampia del Codice italiano novellato e dei suoi rapporti col GDPR.

Essa ha lo scopo di collocare nel modo più chiaro possibile il d.lgs. n. 196/2003 come modificato dal d.lgs. n. 101/2018 nel quadro della regolazione della tutela dei trattamenti dei dati personali e della libera circolazione dei dati nel territorio italiano ed europeo. Un quadro che deve essere concepito necessariamente come un sistema regolatorio multilivello che muove dall'art. 8 della Carta dei diritti fondamentali dell'Unione Europea e dall'art. 16 del Trattato sul funzionamento dell'Unione; passa attraverso il Regolamento europeo (UE) 2016/679 e la Direttiva (UE) 2016/680; giunge infine alla normativa nazionale di adeguamento al GDPR (il Codice italiano novellato), da un lato e alla normativa nazionale che completa la armonizzazione dell'ordinamento italiano con la nuova normativa UE (il d.lgs. n. 51/2018), dall'altro.

A questa complessa tematica, che costituisce l'ordito sul quale si basano quasi tutti i saggi di questo volume, è dedicato, in particolare, il Capitolo I della Prima Parte.

I Capitoli II, III, e IV sono invece incentrati specificamente sul Codice italiano novellato.

Il Capitolo II ricostruisce in modo sintetico, ma non superficiale, il processo di elaborazione, esame e attuazione del d.lgs. n. 101/2018 e i suoi rapporti col Codice previgente, basato invece sul d.lgs. n. 196/2003.

Lo scopo è quello di aiutare il lettore a comprendere meglio le ragioni delle molte complessità, anche testuali, del Codice novellato e delle non poche aporie che esso contiene, nonché il motivo delle diverse tecniche di elaborazione e di "scrittura" delle norme che caratterizzano le diverse parti del nuovo Codice. La ragione di fondo che ha spinto all'elaborazione di questo Capitolo è la convinzione che sia sempre opportuno conoscere il processo di formazione di una normativa, soprattutto quando essa è così complessa e "stretta" tra l'obbligo di "adeguamento al GDPR" e il "peso" dell'eredità del Codice previgente. Le norme non nascono mai dal "nulla". Esse sono sempre condizionate dall'esperienza (e dal fardello) del passato, dalle contingenze del momento in cui sono

elaborate e dall'obiettivo di regolare e di "progettare" il futuro. Nel caso del Codice novellato tutti e tre questi elementi sono stati particolarmente importanti. Per questo si ritiene utile che resti memoria del rilievo che essi hanno avuto rispetto al contenuto attuale del Codice.

Il Capitolo III analizza la Parte I del Codice novellato, che contiene i principi e le disposizioni generali. Essa è la sola delle tre Parti che compongono il Codice attualmente vigente che è stata interamente riformulata, secondo una tecnica legislativa unitaria e coerente. La scelta di commentare in modo analitico le norme in essa contenute è dovuta però soprattutto al rilievo che esse hanno nel sistema nazionale di adeguamento al GDPR.

Il Capitolo IV è dedicato essenzialmente all'analisi delle norme della Parte III del Codice novellato che riguardano composizione, ruolo, poteri e compiti del Garante. La scelta di dedicare un Capitolo specifico a queste disposizioni è dovuta al nuovo, strategico, ruolo che il Garante, come le altre Autorità di controllo, assume nel nuovo quadro normativo sia in virtù del GDPR che degli ulteriori, molto ampi, poteri che il Codice, avvalendosi in particolare di quanto previsto dall'art. 58, paragrafo 6 del GDPR, assegna alla Autorità nazionale italiana di controllo, cioè al Garante della protezione dei dati personali.

Il Capitolo V costituisce, infine, non solo la parte conclusiva della Prima Parte del volume ma anche la ragione di fondo dei quattro Capitoli precedenti. Esso è dedicato a confrontare le numerose difficoltà riscontrate nel raccordare il contenuto normativo del GDPR e del Codice novellato con l'evoluzione delle nuove tecnologie e della sempre più tumultuosa esplosione di quelle fondate sui Big Data e sulla Intelligenza Artificiale. Il filo rosso di tutto il Capitolo, che costituisce però lo scopo vero (e quindi anche la giustificazione) dell'analisi minuziosa svolta nei Capitoli precedenti, è dimostrare che è stato necessario un grande sforzo di adeguamento della regolazione multilivello UE in materia di tutela dei dati personali e della loro libera circolazione, per adattare questa normativa, che costituisce il più solido baluardo regolatorio a tutela dei diritti fondamentali e delle libertà delle persone, a quella che la Presidente della Commissione europea von der Leyen definisce la *Digital Age*, e cioè la nuova epoca in cui sono ormai entrati sia la UE che l'umanità intera. Una esigenza fondamentale, soprattutto dopo la pandemia Covid-19, anche per consentire alla UE di competere alla pari con USA e Cina nella corsa all'Intelligenza Artificiale, senza però rinunciare a salvaguardare i propri valori fondamentali.

In questo quadro il Capitolo V ha anche lo scopo di sottolineare la sfida che il programma della nuova Presidente von der Leyen e, soprattutto, le indicazioni contenute nella Mission Letter con la quale ella definisce i compiti della Vicepresidente-esecutiva Margrethe Vestager nell'ambito del programma "*A Europe fit for Digitale Age*", pongono a tutte le Autorità di controllo competenti a vario titolo in materia di trattamenti di dati, anche non personali. Una sfida che vede in prima fila, oltre alle Autorità Antitrust e Garanti delle comunicazioni, anche, e soprattutto, le Autorità indipendenti di controllo a tutela dei trattamenti dei dati personali.

Il Capitolo V si conclude con un invito al nuovo Garante italiano che gestirà la Autorità dal 2020 al 2027, a svolgere una significativa attività proattiva sia nell'applicazione delle norme del GDPR e del Codice sia, soprattutto, nel quadro dei rapporti con le Autorità nazionali di controllo degli altri Paesi UE, interessate all'uso e alla circolazione dei dati, sia, e soprattutto, con le altre Autorità europee di protezione dei dati personali. Il nuovo Garante, sulla scia dei Garanti che lo hanno preceduto, può e deve fare un lavoro lungimirante e prezioso tanto nel quadro dei meccanismi di coerenza e di collaborazione previsti dal GDPR quanto nell'ambito dell'attività del Comitato europeo di protezione dati (EDPB).

Il Capitolo, infine, si chiude con l'auspicio che le Autorità di controllo a tutela dei dati personali, anche tenendo conto delle posizioni assunte dalle altre Autorità competenti in materia di trattamento dati e di vigilanza sullo stato di sviluppo dell'economia e della ricerca nella società della *Digital Age*, concorrano periodicamente a aggiornare e rendere pubblica una "*European Periodic Overview on personal data*". Lo scopo comune, infatti, deve essere quello di promuovere una riflessione costantemente aggiornata sulla regolazione in materia di trattamenti dei dati, finalizzata anche a una condivisa e pubblica evoluzione dei criteri guida, di carattere anche etico, da seguire di fronte allo sviluppo delle tecnologie digitali. Un contributo importante che si chiede alle Autorità di controllo per orientare in modo condiviso l'evoluzione delle applicazioni proattive delle norme in vigore, lasciando ai futuri legislatori europei e nazionali il compito di adottare, quando i tempi saranno maturi, le modifiche normative che, a quadro stabilizzato, potranno essere necessarie.

La Parte Seconda di questo volume, riguarda gli aspetti più innovativi della materia rispetto ad alcuni dei contenuti più nuovi del GDPR e del Codice novellato. Essa comprende tre saggi.

La prima riflessione, di Giuseppe D'Acquisto, è specificamente dedicata alla "agenda digitale" e al suo rapporto con la protezione dei dati personali ed è per questo che essa è collocata all'inizio di questa Parte.

Il saggio si concentra sul tema della "fiducia" quale tassello fondamentale per una libera circolazione dei dati che sia anche capace di generare sviluppo economico.

La parte più interessante, e più nuova, di questa riflessione è che D'Acquisto considera come elemento essenziale per la valorizzazione economica dei dati anche la fiducia nei rapporti tra Stati e nelle relazioni tra regolatori e mercati. Ovviamente il contenuto del saggio guarda essenzialmente agli aspetti tecnologici ma le conclusioni alle quali perviene sono assolutamente in linea con i ragionamenti giuridici svolti in altri contributi pubblicati in questo volume.

La creazione di fiducia nelle tecnologie non è una esigenza nuova. La novità di oggi è, però, che le tecnologie riguardano direttamente le persone e le loro relazioni. Per questo esse, mentre promettono grandi benefici per le vite e la salute delle persone richiedono, anche la piena fiducia nell'uso he esse fanno dei loro dati. Per questo le tutele relative ai trattamenti dei dati personali

sono non solo dovute ma devono essere connaturate allo sviluppo stesso delle nuove tecnologie.

In questo contesto, le questioni di fondo che il saggio affronta sono:

– la neutralità dei tanti mediatori con cui le persone si relazionano e si relazioneranno sempre di più, compresi gli operatori relativi all'uso delle Intelligenze Artificiali, che devono garantire sempre anche che la quantità dei dati raccolti e il loro dettaglio non vada a scapito della qualità degli stessi;

– la trasparenza sulle finalità e le modalità dei trattamenti necessaria per consentire alle persone di fare scelte libere e rispondenti alle loro reali necessità;

– una profilazione non orientata solo al profitto ma capace di aiutare le persone a individuare i servizi digitali ad esse utili e a sollevarle dalle nuove "fatiche digitali" della ricerca, del confronto e della complessità di conoscenza dei servizi offerti dalle nuove tecnologie;

– il rafforzamento della *privacy by design* come "paradigma di progetto" della tecnologia;

– una concezione della sicurezza non come strumento "difensivo" ma come "valore funzionale", da introdurre nelle modalità di fornitura dei beni e servizi, per rassicurare le persone sul corretto funzionamento delle tecnologie utilizzate.

Si tratta di un saggio estremamente stimolante e assai utile per capire le nuove dimensioni della tutela dei dati personali, anche in raccordo col Capitolo V della Parte Prima.

Il secondo saggio di questa Parte, scritto da Raffaele Bifulco, è dedicato ai Codici di condotta e alle Regole deontologiche. Due strumenti, il primo di regolazione europea (art. 40 del GDPR) e il secondo di regolazione nazionale (art. 2-*quater* del Codice novellato), che hanno in comune l'obiettivo di affidare alle Autorità di controllo, da un lato, alle Associazioni di categoria degli operatori, dall'altro, la possibilità di flessibilizzare la normativa generale per adeguarla, nei limiti consentiti dalla normativa europea e nazionale, alle esigenze e specificità dei diversi settori di attività degli operatori.

L'importanza di questo saggio è proprio quella di sottolineare, da un lato, gli elementi di flessibilità contenuti nel GDPR e rafforzati dal Codice novellato e, dall'altro, di indicare i limiti, anche costituzionali, di tale flessibilità.

I Codici di condotta, del resto, sono un fenomeno giuridico in forte espansione non solo nel campo della tutela dei dati personali. Basti pensare che da strumenti di autoregolazione dell'attività di soggetti privati, essi sono diventati strumenti di regolazione anche dei rapporti tra privati e istituzioni pubbliche: proprio questo, del resto, è il caso dei Codici di condotta nel settore della tutela della protezione dei dati. Già presenti nella disciplina comunitaria contenuta nella Direttiva 95/46/CE, essi ricevono ora una rinnovata regolazione da parte del GDPR, che ne fa addirittura uno strumento per dimostrare la conformità dell'attività svolta dal titolare/responsabile del trattamento al nuovo parametro regolamentare.

Questo vale anche per le regole di condotta. Infatti, l'art. 2-*quater*, comma 4,

del Codice definisce il loro rispetto come condizione di liceità e correttezza.

Di qui l'importanza del saggio di Bifulco e degli approfondimenti, anche di carattere sistematico, che contiene.

Il terzo saggio, di Rocco Panetta, affronta il tema dei flussi relativi ai trattamenti transfrontalieri di dati personali.

Contrariamente a quanto auspicato dal legislatore europeo, l'obiettivo di unificazione legislativa a cui tende il GDPR è ostacolato da diversi fattori, tra i quali la permanenza di aree riservate alle legislazioni nazionali e, ovviamente, anche le possibili diverse interpretazioni giurisprudenziali negli Stati membri. Inoltre nel GDPR non vi è chiarezza circa i possibili conflitti per i casi in cui i trattamenti transfrontalieri possano riguardare aree di competenza dei legislatori nazionali. A questi temi il saggio di Panetta dedica ampia attenzione, richiamando anche i problemi relativi a una non chiara definizione del concetto di stabilimento.

Il cuore del saggio riguarda però il tema della competenza transfrontaliera delle Autorità di controllo, con riguardo all'istituto dello *one-stop-shop*, ovvero dello "sportello unico".

In questo quadro Panetta sottolinea che all'aumento della complessità delle relazioni inter-istituzionali si associa un quadro normativo sostanzialmente immutato che richiederà molto impegno da parte delle Autorità coinvolte, siano esse capofila o Autorità interessate, nonché dello EDPB nell'ambito del meccanismo di coerenza.

Infine, aspetto questo di particolare importanza, si affronta la questione della competenza giurisdizionale delle corti nazionali, anche ponendo a confronto il GDPR col Regolamento Bruxelles I-*bis* rispetto al luogo in cui l'attore può instaurare la controversia.

Importante l'invito che Panetta fa, alla fine del suo saggio, a farsi guidare sempre dal ragionamento giuridico e non dalle diverse, e frequentemente contrapposte, visioni ideologiche che in materia spesso si contendono il campo.

La Parte Terza del volume raccoglie tre saggi relativi ad aspetti specifici, ma molto importanti, della normativa contenuta nel Codice e nelle leggi nazionali di adeguamento e armonizzazione.

Il primo saggio, di Francesco Modafferi, analizza il regime particolare dei trattamenti dei dati personali necessari per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri.

Partendo dalla constatazione che il Regolamento non fornisce alcuna specifica definizione di interesse pubblico, il saggio affronta il tema della base giuridica dei trattamenti effettuati "in ambito pubblico" mettendo in evidenza che, stante la mobilità del confine tra enti pubblici e privati e in piena armonia con gli sviluppi della legislazione europea, le disposizioni del Regolamento guardano più alla natura dell'interesse perseguito col trattamento che alla qualificazione giuridica del soggetto che lo effettua. In questo quadro Modafferi affronta poi le scelte effettuate dal legislatore delegato in ordine ai presupposti per il trattamento dei dati in ambito pubblico e il peculiare ruolo affidato al-

l'Autorità. Il saggio sviluppa inoltre una penetrante riflessione sul principio di accountability nel trattamento dei dati nell'ambito pubblico, approfondendo il tema di quali possano essere gli strumenti a disposizione del titolare per dimostrare di essere in regola con la protezione dati, in particolare con riguardo alla figura del DPO.

Tra le parti più stimolanti di questo saggio va segnalato l'esame di quello che l'autore definisce lo "statuto speciale dei diritti degli interessati rispetto ai trattamenti dei loro dati effettuati nell'ambito pubblico" e alle implicazioni connesse al loro effettivo utilizzo, anche avendo a mente i trattamenti automatizzati di dati, il ruolo degli algoritmi e le tecniche di profilazione.

Nella parte finale si affronta anche il tema degli "usi ulteriori" dei dati personali e, in questo contesto, Modafferi riflette sull'individuazione di un "modello sostenibile" di trattamento dei dati personali nell'ambito pubblico, capace di coniugare efficienza e economicità dei trattamenti con il rispetto dei diritti degli interessati.

Segue il saggio di Laura Ferola dedicato alla "misure di garanzia", con particolare riguardo ai dati biometrici, genetici e sulla salute.

La riflessione dell'Autrice muove dall'analisi di un istituto introdotto dal d.lgs. n. 101/2018 che, sia per la sua particolare natura di provvedimento cogente, sia per i tipi di informazioni e di trattamenti che intende disciplinare, assume un ruolo centrale nel nuovo contesto italiano. Il legislatore nazionale, infatti, sfruttando gli spazi di flessibilità del GDPR, ha voluto, da un lato, assicurare con questo strumento un elevato livello di tutela dei dati genetici, biometrici e relativi alla salute e, dall'altro, richiamare il Garante a esercitare un ruolo proattivo, segnando la strada che i titolari e i responsabili del trattamento sono tenuti a percorrere per tutelare adeguatamente tali tipologie di dati in una realtà che deve confrontarsi con una continua evoluzione della tecnologia.

La peculiarità del nuovo istituto ha richiesto, in ragione della sua complessa strutturazione, una analisi specifica, che però presenta numerosi addentellati con altre norme del Codice. Ne consegue che il saggio di Laura Ferola offre una panoramica completa sulla disciplina riguardante il trattamento dei dati in questione.

L'ultimo saggio, quello di Federica Resta, analizza il sistema sanzionatorio penale introdotto dal d.lgs. n. 101/2018, nonché le principali fattispecie di reato previste del d.lgs. n. 51/2018, evidenziando sia gli elementi di continuità che quelli di discontinuità rispetto alla disciplina previgente.

In generale entrambi i sistemi sanzionatori previsti dai due decreti recepiscono la dicotomia – propria del d.lgs. n. 196 "originario" – tra i delitti lesivi del diritto individuale alla protezione dei dati qualificati e i reati d'inosservanza, idonei dunque a pregiudicare il bene giuridico intermedio (strumentale al primo) rappresentato dall'efficiente esercizio dei poteri del Garante.

Ciascuna delle due discipline presenta caratteristiche sue proprie, che sottendono scelte di politica criminale diverse. Così, se le fattispecie di reato previste dal d.lgs. n. 51/2018 si allineano maggiormente, nel complesso, alla siste-

matica propria del d.lgs. n. 196/2003, le norme incriminatrici introdotte dal d.lgs. n. 101/2018 se ne discostano in taluni aspetti, nel segno di una più marcata selettività e residualità dell'intervento penale rispetto a quello sanzionatorio amministrativo. Ciò deriva anche dalle scelte compiute, nell'ambito dei due decreti, dal legislatore nazionale in ordine alla disciplina degli illeciti amministrativi e alla conseguente esigenza di evitare possibili violazioni del principio del *ne bis in idem* considerato alla luce della lettura fornita dalle Corti di Strasburgo e Lussemburgo, oltre che, recentemente, dalla nostra Corte costituzionale.

In sostanza questo volume, grazie alla sua articolazione in tre Parti distinte e ai temi affrontati nei contributi pubblicati, ha l'ambizione di fornire al lettore e all'operatore uno strumento utile sia a comprendere meglio i nessi di raccordo tra GDPR e Codice novellato, sia ad affrontare con una visuale ampia i problemi posti dalle disposizioni più innovative e importanti del Codice italiano vigente.

Infine, tanto nel Capitolo V della Parte Prima quanto nel saggio di D'Acquisto, questo volume cerca anche di mettere a disposizione del Garante, e in particolare dei Collegi che gestiranno l'Autorità negli anni futuri, alcune prospettive, anche operative, nella speranza che esse possano risultare utili per il lavoro estremamente importante e impegnativo che attende i futuri Garanti nei prossimi anni. Anni che saranno cruciali per trovare il giusto equilibrio tra la tutela dei diritti e delle libertà delle persone e lo sviluppo delle tecnologie digitali, in un quadro che vede l'UE determinata ma anche obbligata a operare con sempre maggiore decisione e impegno per il completamento del Digital Single Market nel quadro di una competizione globale, ormai già chiaramente in atto, con USA e Cina.

2. Nelle more della stampa di questo volume il mondo è stato travolto dalla pandemia e da tutti i mutamenti che essa ha apportato nelle abitudini e nelle relazioni tra le persone, invitate o costrette a forme di distanziamento sociale che hanno incentivato sempre di più all'uso delle tecnologie digitali in ogni settore della vita economica e sociale.

Il ritardo tra la fine della messa a punto dei diversi contributi qui raccolti e la stampa del volume, dovuto essenzialmente a problemi, ora del tutto superati, di chi scrive questa Introduzione, è del resto, almeno per i lettori più esperti, facilmente "leggibile" nei contributi di molti di Autori. Quasi tutti, infatti anticipano, con notevole preveggenza, fenomeni e problemi che nel corso del 2020, di fronte a una emergenza non prevista, si sono puntualmente manifestati. A questo va aggiunto l'effetto che la decisione della Corte di Giustizia dell'Unione europea del 16 luglio 2020, nota come la "sentenza Schrems II", ha determinato rispetto alla non applicabilità del Privacy Shield al trasferimento di dati all'estero (meglio negli USA) quando esso si basi solo sull'adesione del soggetto ricevente ai vincoli e limiti posti appunto dal Privacy Shield. Di questa decisione ovviamente non tiene conto il saggio di Panetta e questo

non può sfuggire certo al lettore più attento anche se il saggio qui pubblicato contiene considerazioni valide e illuminanti che, muovendo dalla decisione della Corte di Giustizia nota come decisione Schrems I del 6 ottobre 2015, aiutano a capire meglio anche la situazione determinatasi in seguito al nuovo intervento della Corte di Giustizia del 16 luglio 2020.

Per non prolungare ancora la pubblicazione di questi scritti, la cui validità è stata confermata dall'evoluzione dei fenomeni citati, si è deciso di procedere comunque alla pubblicazione del volume lasciando ai lettori di leggere queste pagine anche alla luce di quanto accaduto dopo la loro stesura, generalmente avvenuta tra la fine del 2019 e l'inizio del 2020.

3. In questi mesi comunque i fatti più rilevanti relativi all'Unione Europea hanno riguardato molto più l'avvio della nuova Commissione von der Leyen che non le conseguenze della pandemia, fermo restando che proprio il manifestarsi della pandemia e il connesso accelerato passaggio alla *Digital Age* sono certamente l'aspetto fondamentale che ha consentito lo sviluppo così rapido dell'indirizzo politico già delineato dalla allora candidata alla Presidenza della Commissione Ursula von der Leyen nel documento che accompagnò l'ufficializzazione della sua candidatura "*A Unione strives for more. My agenda of Europe 2019-2024*".

In realtà, infatti, nel presentare il suo programma per l'Europa Ursula von der Leyen ha delineato con grande chiarezza una linea politica che, confermando quella seguita dalla Commissione Junker, ha indicato nello sviluppo dell'economica digitale e, soprattutto, nel rafforzamento del quadro regolatorio
Europeo finalizzato all'istituzione del *Single European Marcket*, il programma politico della UE alle soglie della *Digital Age.*
Del resto anche in molti saggi qui raccolti si sottolinea con forza che lo steso GDPR è stato visto all'inizio, e con grande chiarezza, come il primo e fondamentale pilastro di una nuova Unione Europea, capace di rinnovare le ragioni fondative del Mercato Unico e della stessa Unione anche nella nuova, imminente epoca digitale.

Proprio per questo, del resto, è così importante continuare a seguire con la massima attenzione lo sviluppo dell'attuazione del GDPR: il che spiega anche le motivazioni di fondo di questo volume.

Va sempre ricordato inoltre che nel progetto politico della von der Leyen non meno importante è anche la rapida approvazione di un nuovo e più ambizioso apparato regolatorio capace di dare sostanza e forma al *Digital Single Market* nonché a implementare e stimolare il *Data sharing* nel quadro di una ben organizzata e disciplinata regolazione della messa in comune tra tutti gli europei dei dati prodotti e trattati dalle amministrazioni pubbliche e dagli operatori privati all'interno dell'Unione al fine di rafforzare la capacità della UE e della sua economia di competere nella gara globale al domino economico nell'epoca digitale e a un ben strutturato sistema di interoperabilità delle

reti di trasmissione dei dati e delle comunicazioni elettroniche nell'ambito dell'Unione.

4. Questo programma, basato tutto sulla logica che presiede al GDPR e cioè sulla necessità di offrire ai cittadini europei un quadro regolatorio che ne rafforzi la fiducia nella società digitale e nei trattamenti dei loro dati, è l'asse portante del progetto politico della nuova Commissione von der Leyen, come risulta con chiarezza nella lettera di Missione indirizzata il 10 settembre 2019 dalla Presidente von der Leyen alla vicepresidente Margrethe Vesteger, commissaria incaricata di lavorare per una *Europe fit for the Digital Age*.

In quella lettera, la von der Leyen indica con chiarezza che la Vesteger deve lavorare, insieme a lei e a tutta la Commissione, per una "*new longterm strategy for Europe's industrial future*" e per una "*new SME strategy*". A tal fine, la von der Layen chiede alla Vestager di lavorare affinché fin dai primi 100 giorni del suo mandato, la nuova Commissione possa indicare "*a new approach on artificial intelligence, including its human and ethical implications*". Inoltre, sempre nella citata Lettera di Missione, la Presidente von der Layen chiede alla Commissaria Vestager di presentare una proposta per rafforzare "*our liability and safety rules for digital platforms services and products of a new Digital Services Act*". Infine, alla Vestager è chiesto anche di lavorare per presentare, per la fine del 2020, la proposta di una *digital taxation* che possa incontrare il consenso di tutti gli Stati membri.

Tutto questo, però, va chiaramente inserito in una specifica strategia: quella di rafforzare la spinta alla *competition*, anche rivedendo le regole che disciplinano la competizione e la stessa concorrenza all'interno dell'Unione.

Contemporaneamente, l'appello della Presidente von der Leyen alla Commissaria Vestager è quello di ridefinire le regole sulla concorrenza anche allo scopo di "*develop tools and policies to better tackle the distorsive effects of foreign state ownership and subsides in the internal market*",

Tralasciando le ulteriori, ma importanti, indicazioni contenute nella Lettera di Missione, bastano i punti richiamati a spiegare l'importanza che i temi trattati nel Volume, e soprattutto nella Prima Parte e nel saggio di D'Acquisto, hanno per capire non solo il contenuto del GDPR ma anche le proposte presentate alla Commissione nei primissimi mesi del 2020.

Per comprendere appieno quanto sta succedendo nella UE in materia di regolazione dell'uso dei dati nella *Digital Age*, e i legami che tutto questo ha col GDPR, conviene muovere dalle due Comunicazioni della Commissione UE, presieduta ancora da Junker, presentate il 10 gennaio 2017, dopo che il 16 maggio 2016 era stato definitivamente adottato il GDPR. La prima Comunicazione, intitolata "*Scambio e protezione dei dati in un mondo globalizzato*", dà una lettura dinamica dei trattamenti dei dati, soprattutto personali, e delle regole da rispettare, con particolare riguardo ai trasferimenti di dati all'estero. La seconda, pubblicata lo stesso giorno e intitolata "*Costruire un'economia dei dati europea*", indica già l'ambizione della UE di porsi, grazie alla regolazione

dei trattamenti dei dati, alla guida della globalizzazione digitale, garantendo un ecosistema economico e produttivo rispettoso dei diritti delle persone, ma anche delle regole di una sana e trasparente regolazione della concorrenza e dei trattamenti dei dati non personali. Lo scopo dichiarato è quello di dar vita ad un'economia europea sempre più basata sull'utilizzazione dei dati. In questa prospettiva, già il 25 aprile 2018, la Commissione Junker ha presentato una nuova Comunicazione, intitolata "*Verso uno spazio comune europeo dei dati*", dopo che aveva già presentato, il 13 settembre 2017, quello che poi è divenuto il Regolamento per la libera circolazione dei dati non personali, approvato, in via definitiva, il 14 novembre 2018.

Già in quella Comunicazione la Commissione Junker proponeva e prometteva: a) di rivedere il testo della Direttiva del 96 sulle banche dati (promessa tuttora non mantenuta); b) di promuovere lo sviluppo di tecniche affidabili di identificazione e scambio dati con particolare riferimento alle API (interfacce applicative di programmazione); c) di elaborare note contrattuali minime relative i contratti sui dati, tanto con particolare riguardo ai dati B2B, quanto agli scambi che concernono le relazioni tra fornitori di piattaforme e imprese quando riguardano l'offerta di servizi digitali; d) di regolare l'accesso ai dati per fini scientifici; e) di regolare l'accesso ai dati previo compenso e, ove si tratti di dati personali, previa loro anonimizzazione; f) di definire i diritti dei "produttori di dati non personali". Tutto questo, ovviamente, fermo restando il GDPR. La medesima Comunicazione dava anche molto rilievo alla portabilità dei dati e alla necessità di garantire la interoperabilità delle modalità di trasmissione e di connessione tra le piattaforme.

La Comunicazione "*Costruire un'economia dei dati europea*" era accompagnata da numerosi allegati e da proposte di regolazione di diversi campi. Proprio per questo, del resto, essa era parte integrante del c.d. "Pacchetto dati". In questo senso, non solo l'attività della Commissione van der Leyen può essere considerata come la naturale prosecuzione della strategia europea già affermata dalla precedente Commissione Junker, ma si può, e si deve, riconoscere anche che l'operato della Commissione Junker costituisce tuttora la base dei progetti legati allo sviluppo dell'economia digitale e anche alla utilizzazione da parte degli Stati membri dei fondi europei previsti dal bilancio UE sia per il digitale che per il green.

Essa inoltre poggiava già sul principio base di tutela e sviluppo dei valori che la UE considera non negoziabili e non rinunciabili, e che sono anche strettamente connessi ai diritti fondamentali dei cittadini europei riconosciuti dalla Carta di Nizza e, ora, dal Trattato di Lisbona. Del resto, come costantemente è ripetuto nei saggi contenuti in questo volume, il rispetto dei diritti fondamentali costituisce sempre un limite insuperabile della nuova regolazione, un vincolo comune a tutti gli Stati nell'utilizzazione dei fondi europei e una cornice non negoziabile di qualunque trattato internazionale e globale sui trattamenti dei dati personali, innanzitutto, ma poi, più in generale, anche dei dei dati considerati come nuovo petrolio di un'economia digitale che vive dei dati

relativi alle relazioni interpersonali e alle attività che si svolgono sulla rete globale.

È dunque in questo quadro, molto complesso e per ora ancora in costruzione, che deve essere collocato il contributo che questo volume e i saggi in esso contenuti vogliono offrire al lettore e a chi dei dati e del loro uso si occupa professionalmente.

La tutela dei dati personali e non, sempre meno ha a che fare solo con la tutela del diritto fondamentale alla riservatezza (privacy) considerato giustamente come il fondamento stesso della libertà umana e il presidio del libero arbitrio. Sempre più, invece, questa tutela deve trovare il suo spazio centrale in una galassia di diritti che costituiscono la proiezione giuridica dei princìpi fondamentali sui quali la UE si è costruita, e che sono stati affermati in via strutturata nella Carta di Nizza, poi diventata parte integrante del Trattato di Lisbona.

L'auspicio è che il contenuto di questo volume aiuti chi (per lavoro o per scelta) sta contribuendo alla costruzione di una *Digital Age* rispettosa dei valori dell'uomo e attenta a tutelare la libertà degli esseri umani; ad accrescere la consapevolezza dell'importanza di quanto l'umanità sta facendo; a dare a tutti un panorama più ampio e completo di che cosa significhi e di quali sfide ponga questo difficile passaggio di epoca dalla società industriale a quella digitale per poter svolgere nel modo migliore, e più consapevole possibile, la propria attività.

Merita, infine, sottolineare, a conclusione di questa Introduzione, che il progetto europeo di sviluppo della economia europea digitale è già stato fatto proprio anche dalla Presidenza portoghese che guiderà la UE dal gennaio 2021. Ha dichiarato, infatti, il Presidente António Costa "Il rilancio europeo, equo, verde e digitale è la prima priorità della nostra Presidenza, con l'approvazione di tutti i regolamenti normativi del Recovery Fund e dei piani nazionali per accedervi" (cfr. ANSA, 31 dicembre 2020). Queste dichiarazioni confermano, dunque, il quadro qui delineato e l'utilità di questo Volume.

Infine merita di fare un cenno conclusivo anche all'Accordo economico tra Europa e Cina denominato "*Comprehensive Agreement on Investiment*", stipulato tra la Commissione UE e il Governo cinese il 30 dicembre 2020, giusto un giorno prima che terminasse il mandato della Presidenza tedesca dell'Unione. Particolare rilievo merita dare anche al fatto che alla stipula dell'Accordo fosse presente il Presidente francese Macron, cosa che ha sollevato perplessità negli governi degli altri Paesi UE a partire dal Governo italiano e che l'Accordo in generale ha sollevato malumore anche negli ambienti USA, tanto più che pochi giorni prima il Presidente eletto Joe Biden aveva espresso la sua contrarietà alla firma dell'Accordo.

A parte le tensioni, molto temuto invero, tra USA, UE e Cina, che hanno spinto il governo cinese a dichiarare la propria disponibilità a continuare nello sviluppo di una economia digitale globalizzata inclusiva di tutti gli aspetti legati alla tutela delle concorrenza nel quadro di una competizione globale re-

golata e aperta anche agli USA, non vi è dubbio che l'Accordo intervenuto e la non gradita da tutti partecipazione irrituale alla cerimonia del Presidente Macron, confermano e rafforzano le tesi di fondo sul presente e il futuro della UE che sono alla base del presente volume.

Autori e curatore rinnovano dunque la loro fiducia circa l'utilità degli scritti qui raccolti a offrire alla cultura giuridica italiana uno strumento utile anche a comprendere meglio la materia della protezione dei dati nel mondo di oggi e, ancora di più, in quello di un domani ormai imminente.

Parte Prima

GDPR, Codice italiano e ruolo della Autorità Garante nel mondo dei Big Data e dell'Intelligenza Artificiale

Capitolo I

Il sistema normativo di protezione dei trattamenti di dati personali nel quadro europeo e nazionale

di *Franco Pizzetti*

SOMMARIO: 1. Il quadro normativo della protezione dei trattamenti di dati personali in UE tra fonti europee e leggi nazionali di attuazione. – 2. Le differenti basi normative del GDPR e della Direttiva 2016/680. – 3. Le differenze sistemiche tra GDPR e Direttiva 2016/680. Il "posto" del d.lgs. n. 51/2018. – 4. Il rapporto tra GPDR, delega al Governo contenuta nella legge n. 167/2017 e d.lgs. n. 101/2018. – 4.1. Le conseguenze sistemiche della piena applicazione del GDPR. – 4.2. Il ruolo delle legislazioni nazionali come elemento di flessibilità e variabilità rispetto alla regolazione generale UE. – 4.3. Continua: il ruolo delle legislazioni nazionali come elemento di flessibilità e variabilità. Un *alert* per il presente e per il futuro. – 5. La nuova normativa nazionale e le disposizioni di adeguamento al GDPR. – 5.1. Il quadro sistemico del mutato ruolo degli atti nazionali di adeguamento. – 5.2. Le oggettive difficoltà degli Stati membri nel passaggio dalla Direttiva al GDPR e le ragioni degli "spazi" lasciati alle singole legislazioni nazionali. Il rapporto tra norme nazionali e GDPR e i vincoli che comportano per chiunque debba applicarle. – 5.3. Ancora sul rapporto tra GDPR e competenze assegnate agli Stati membri. Le competenze statali in materia di Autorità di controllo e dei loro poteri: tra GDPR e legislazioni nazionali di adeguamento. – 5.4. Le normative nazionali relative ai poteri sanzionatori delle Autorità e alle procedure relative ai risarcimenti per danno. Il ruolo delle Autorità giurisdizionali. – 6. La delega contenuta nell'art. 13 della legge n. 163/2017 relativa al decreto legislativo di adeguamento. – 6.1. L'art. 13 della legge n. 163/2017 e lo "spazio" lasciato al legislatore delegato: una grande opportunità e una impegnativa responsabilità. – 7. L'attuazione della delega e la necessaria ridefinizione del ruolo del Garante. Primi cenni. – 7.1. L'importanza centrale del ruolo del Garante nel quadro del decreto delegato di adeguamento. – 7.2. Il ruolo del GDPR e quello del Garante in una prospettiva rivolta al futuro. – 7.3. Il futuro della regolazione europea nell'ecosistema digitale e il ruolo del Garante. – 7.4. L'importanza delle Autorità nazionali chiamate ad evitare indebiti comportamenti competitivi tra i diversi Stati dell'Unione. Il ruolo del meccanismo di cooperazione e coerenza.

1. Il quadro normativo della protezione dei trattamenti di dati personali in UE tra fonti europee e leggi nazionali di attuazione

Il quadro normativo in materia di protezione dei trattamenti relativi ai dati delle persone fisiche e alla loro libera circolazione nell'Unione Europea è particolarmente complesso.

Uno degli aspetti più rilevanti riguarda il rapporto tra il Regolamento europeo (UE) 679/2016 e le legislazioni nazionali di adeguamento, che ormai quasi tutti i Paesi dell'Unione hanno adottato nelle materie in cui il GDPR stesso lo consente e, talvolta, lo impone [1].

L'entrata in vigore il 19 settembre 2018 del d.lgs. 10 agosto 2018, n. 101, recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio, con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati" è lo strumento normativo col quale anche l'Italia ha adeguato il suo ordinamento nazionale al nuovo GDPR.

È molto importante avere chiaro quali siano gli effetti giuridici che il d.lgs. n. 101/2018 e, di conseguenza, anche il novellato d.lgs. n. 196/2003, hanno nel sistema delle fonti.

Il rinvio fatto dal GDPR alle leggi nazionali in specifiche materie, o ai fini di dare attuazione a disposizioni puntuali in esso contenute, comporta necessariamente l'integrazione tra il quadro delle fonti UE, costituito dal Regolamento 2016/679, e l'ordinamento nazionale che, soprattutto per la parte relativa alle normative nazionali di adeguamento, si configura, così, come un sistema integrato multilivello.

In questo volume ci occupiamo essenzialmente del quadro regolatorio costituito dal GDPR e dagli atti normativi nazionali di adeguamento. Tuttavia va tenuto presente che le innovazioni introdotte a livello UE rispetto alla normativa relativa alla tutela dei trattamenti dei dati personali non si esauriscono affatto nel raccordo tra GDPR e normative nazionali di adeguamento.

Va sottolineato, infatti, che il 27 aprile 2016 il Consiglio europeo non si è limitato ad approvare in via definitiva il Regolamento 2016/679 "relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali e alla libera circolazione dei dati, che abroga la Direttiva 95/46/CE" (Regolamento ormai generalmente noto come GDPR) [2].

Quel medesimo giorno, e immediatamente dopo l'approvazione del GDPR, il Consiglio ha approvato in via definitiva anche la Direttiva 2016/680/UE "relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati che abroga la Decisone quadro 2008/977/GAI del Consiglio". L'aspetto importante che merita sottolineare è proprio che questa

---

[1] Sul punto si veda il documento "*Data protection as a pillar of citizens' empowerement and the EU's approach to the digital transition – two years of application of the General Data Protection Regulation*", presentato dalla Commissione UE il 24 giugno 2020 in ossequio all'art. 97 del GDPR.

[2] Il Regolamento era già stato approvato dal Parlamento europeo il 14 aprile dello stesso anno, dopo più di quattro anni dalla presentazione del progetto della Commissione, avvenuta il 10 febbraio 2012.

Direttiva era stata adottata in via definitiva dal Parlamento europeo il 14 aprile 2016, subito dopo l'approvazione parlamentare del GDPR.

I due sistemi normativi, quello costituito dal GDPR e quello contenuto dalla Direttiva 2016/680, sono quindi entrati in piena applicazione contemporaneamente, il 25 maggio 2018, determinando: la abrogazione della Direttiva 95/46, il primo; l'abrogazione della Decisione del Consiglio 2008/97, la seconda.

Entrambi questi strumenti, inoltre, prevedono l'intervento dei legislatori nazionali. Una legge o un decreto legislativo di adeguamento dell'ordinamento interno alla nuova regolazione europea, il primo; un intervento legislativo di recepimento della Direttiva nell'ambito dell'ordinamento nazionale, il secondo.

2. Le differenti basi normative del GDPR e della Direttiva 2016/680

Sia il Regolamento 2016/679 che la Direttiva 2016/680 hanno a oggetto la protezione dei trattamenti dei dati personali e la loro libera circolazione nel territorio dell'Unione. Essi hanno basi normative in parte diverse, il che spiega perché siano due strumenti regolatori adottati con due diversi tipi di fonti dell'Unione: con un Regolamento, l'uno, con una Direttiva, l'altro.

Il Regolamento trova il suo fondamento nell'art. 8 della Carta dei diritti fondamentali dell'Unione e nell'art. 16 del Trattato sul Funzionamento dell'Unione Europea, d'ora innanzi TFUE.

La Direttiva 2016/680, invece, deve tener conto della Dichiarazione 21 dell'Allegato l dell'Atto finale della Conferenza Intergovernativa che il 13 dicembre 2007 ha adottato il Trattato di Lisbona. In questa Dichiarazione si è riconosciuto che, nell'ambito delle attività di polizia e giustizia, la tutela dei diritti e la cooperazione che l'art. 16 del TFUE impone rispetto ai trattamenti di dati personali può richiedere regole giuridiche e discipline normative specifiche, in ragione delle caratteristiche proprie di queste materie.

In sostanza, e per essere il più chiari possibile: da un lato, la Carta riconosce la protezione dei trattamenti personali come un diritto fondamentale dei cittadini europei, di cui l'art. 16 del TFUE impone all'Unione di garantire il rispetto in tutte le materie e i settori di sua competenza. Da un altro lato, però, la Dichiarazione 21 prevede la possibilità di regole generali diversificate per quanto riguarda i trattamenti di dati personali nell'ambito delle attività di polizia e giustizia, anche al fine di consentire, pur in un quadro armonizzato, più ampio spazio alle leggi nazionali in materia.

Di conseguenza, come chiariscono i Considerando 10 e 11 della Direttiva 2016/680, è stato ritenuto opportuno differenziare la regolazione europea relativa alla tutela del diritto fondamentale riconosciuto ai cittadini dell'Unione dall'art. 8 della Carta dei diritti e che, in ragione di quanto previso dall'art. 16, paragrafo 1, del TFUE, tocca all'Unione garantire in modo uniforme da quella

relativa alla tutela dei trattamenti di dati personali nei campi specifici della polizia e della giustizia, richiamati dalla Dichiarazione 21.

Per questo motivo la disciplina regolatoria UE in materia di tutela dei dati personali, pur essendo attuativa di un medesimo (e "unico") diritto fondamentale riconosciuto a tutti i cittadini europei, è distribuita in due diversi strumenti normativi e anche gli atti legislativi nazionali di adeguamento, per il GDPR, e di armonizzazione, per la Direttiva 2016/680, sono contenuti in due diversi decreti legislativi: il d.lgs. 8 agosto 2018, n. 101, per l'armonizzazione al GDPR; il d.lgs. 18 maggio 2018, n. 51 per il recepimento della Direttiva [3].

[3] In realtà, nelle intenzioni della Commissione UE, probabilmente il 25 maggio 2018 avrebbe dovuto entrare in vigore, o comunque essere già stato approvato, un terzo importante strumento normativo. Si tratta del Regolamento del Parlamento europeo e del Consiglio "relativo al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettroniche che abroga la direttiva 2002/58/CE (regolamento sulla vita privata e le comunicazioni elettroniche)".

Com'è noto, in materia di protezione dei dati personali, già ben prima del Trattato di Lisbona, nell'ambito CE operavano tre Direttive. La prima, la notissima Direttiva 95/46 adottata nel 1995 relativa in generale alla protezione dei dati personali e alla loro libera circolazione nel Mercato interno (cioè nell'ambito CE); la seconda, la Direttiva 2000/31/CE, "relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno", che peraltro solo molto indirettamente riguardava anche i trattamenti relativi ai dati personali; la terza, la Direttiva 2002/58/CE, specificamente "relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche" detta anche Direttiva relativa alla vita privata e alle comunicazioni elettroniche, successivamente sottoposta nel tempo a significative modifiche.

Il GDPR esplicitamente fa salve entrambe queste Direttive, limitandosi ad abrogare la Direttiva "madre" in questa materia, e cioè la "Direttiva 95/46". Infatti l'art. 2, paragrafo 4 GDPR afferma esplicitamente che il Regolamento non pregiudica la applicazione della Direttiva 2000/31/CE, specialmente rispetto alle responsabilità degli intermediari di servizi, mentre l'art. 95 specifica che: "il presente regolamento non impone obblighi supplementari alle persone fisiche o giuridiche in relazione al trattamento nel quadro della fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche dell'Unione per quanto riguarda le materie per le quali sono soggette a obblighi specifici aventi lo stesso obiettivo fissati dalla Direttiva 2002/58" (cfr. anche Considerando 21 e Considerando 173).

Entrambe le disposizioni citate peraltro sono state inserite nel Regolamento nella convinzione, propria della Commissione e in generale degli operatori, che ormai fosse necessaria in queste materie, e in particolare nell'ambito delle comunicazioni elettroniche, una nuova normativa che tenesse conto delle enormi innovazioni, anche tecnologiche, intervenute in questi anni nel settore delle comunicazioni elettroniche e digitali.

A tal fine la Commissione ha presentato in data 10 gennaio 2017, e quindi dopo la approvazione del GDPR ma prima della sua piena applicazione, una apposita proposta di Regolamento "relativo al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettroniche e che abroga la Direttiva 2002/58".

La scelta fatta dalla Commissione presentando questo Regolamento è stata chiara, come già lo era stata la scelta del GDPR di non abrogare direttamente la Direttiva in questione. Alla base vi è stata, infatti, la consapevolezza che il settore delle comunicazioni elettroniche, che nella proposta della Commissione si amplia al settore delle informazioni nell'ecosistema digitale, richiede necessariamente regole in gran parte specifiche, come del resto già era accaduto con la Direttiva 2002/58 rispetto alla Direttiva 95/46.

In sostanza la scelta è stata quella di mantenere accanto alla legge generale (la Direttiva