Jean Louis a Beccara

La nuova privacy per la Pubblica Amministrazione

Sintesi dell'armonizzazione del Codice italiano al Regolamento europeo

FrancoAngeli
tsm-Trentino School of Management

1801. tsm-Trentino School of Management/Studi e Ricerche

tsm-Trentino School of Management è la Scuola, costituita da Provincia autonoma di Trento, Regione Trentino-Alto Adige/Südtirol e Università degli Studi di Trento, che si occupa di formazione, aggiornamento continuo e ricerca/intervento in particolare per il settore pubblico.

La collana raccoglie materiali inerenti tematiche che contribuiscono ad alimentare con costanza e garanzia di qualità la riflessione sulle problematiche del management, dell'alta formazione e dell'aggiornamento del personale in servizio, in particolare delle Pubbliche Amministrazioni.

Jean Louis a Beccara

La nuova privacy per la Pubblica Amministrazione

Sintesi dell'armonizzazione del Codice italiano al Regolamento europeo

FrancoAngeli
tsm-Trentino School of Management

Responsabilità editoriale: Paola Borz
Con il coordinamento di Stefania Martini

Sommario

A Carla, Giorgio, Anna Paola, Massimiliano e Dana

Presentazione

Dopo la pubblicazione del libro *La privacy nel pubblico. Sntesi dell'integrazione tra Codice italiano e Regolamento europeo per la Pubblica Amministrazione*, tsm-Trentino School of Management e l'Autore completano l'Opera con questo secondo e per ora conclusivo volume. In tal modo, l'esposizione teorica e pratica della materia può dirsi sostanzialmente compiuta, fornendo al lettore e alla lettrice un compendio sistematico e coordinato tra Regolamento europeo e Codice nazionale.

Riprendendo il discorso lasciato in sospeso in chiusura del precedente volume, infatti, l'Autore prosegue – senza soluzione di continuità – lo sviluppo del tema, chiarendo come il Legislatore italiano abbia dato attuazione alla normativa europea (nei margini da quest'ultima consentiti), "armonizzando" il D. Lgs. 196/2003.

In adempimento alla propria *mission*, quindi, tsm svolge attivamente attività di formazione non soltanto attraverso la predisposizione di corsi specialistici per rispondere alla pratica quotidiana, ma anche mediante l'*editing* di materiali, pubblicazioni e monografie sulle più attuali tematiche. È proprio questa "stella binaria" ad orientare l'attività della nostra Società: perché la teoria è in grado di fornire risposte alla pratica, solo quando attinge parte della propria linfa da quest'ultima.

Paola Borz
Direttrice Generale

Prefazione

Il rapporto che esiste tra la disciplina sulla protezione dei dati e l'attività della Pubblica Amministrazione è sempre stato, sin dalle origini, molto delicato.

Da un lato vi era, alla fine degli anni Novanta del secolo scorso (quando fu emanata la prima normativa italiana, la Legge n. 675 del 1996), il timore che il settore pubblico si presentasse (o si dichiarasse) "impermeabile" alle novità legislative. In altre parole, che in un ambito ricco di problemi per molti versi "congeniti" (la mancanza di fondi, l'evidenza di altre priorità, la necessità di efficienza e di sempre più evoluti servizi ai cittadini, l'avvento della trasparenza) l'attenzione alla protezione del dato passasse in secondo piano, sia come "cultura" sia come investimenti in sicurezza.

In realtà, dopo un avvio timido, il tema della protezione dei dati è entrato prepotentemente nel discorso pubblico, grazie anche a interventi ispettivi molto frequenti del Garante per la Protezione dei dati che hanno cercato di fornire delle linee interpretative importanti (come hanno fatto, del resto, in altri settori quali quello bancario e finanziario). Mi vengono in mente, ad esempio, i numerosi interventi del Garante italiano che hanno ordinato a pubbliche amministrazioni di rimuovere dai propri siti web migliaia di dati di cittadini disabili o a basso reddito che potevano generare discriminazione.

Il risultato è stato che in oltre vent'anni di attività si è delineato chiaramente un diritto alla protezione dei dati *nella* Pubblica Amministrazione.

L'avvento del Regolamento Europeo, come è prevedibile, ha ulteriormente connotato questo quadro, per certi versi complicandolo.

Il libro di Jean Louis a Beccara ha, tra i tanti, un grandissimo pregio: quello di cercare di individuare la natura del diritto della protezione dei dati come si è inserito, nel corso degli anni, in un settore così complesso quale quello del pubblico, tentando costantemente di mitigare e armonizzare tutte le norme che già disciplinano il settore (si pensi al delicatissimo tema del diritto all'accesso, o della trasparenza, o dell'anticorruzione, o dell'obbligo di pubblicità di determinati dati e procedimenti) con quelle che mirano alla protezione del dato.

L'aspetto introduttivo/ricognitivo, del libro di a Beccara, è molto interessante perché evidenzia l'incredibile evoluzione che c'è stata nel rapporto tra normativa sulla protezione dei dati personali e settore pubblico.

Il GDPR, che è il provvedimento oggetto della maggior parte delle riflessioni dell'Autore, si mostra chiaramente "diffidente" nei confronti del settore pubblico.

Si notano, in particolare, tre grandi timori del legislatore europeo: che il settore pubblico possa trattare in maniera automatizzata e profilare i cittadini (un'eredità che ci portiamo dietro sin dalla Seconda Guerra Mondiale), il timore di grandi *data breach* nel settore pubblico (con la fuga incontrollata dei dati, anche sanitari, dei cittadini) e, infine, il timore che il cittadino/interessato non riesca a esercitare tutti i diritti che il GDPR prevede e gli garantisce, e che sono stati rafforzati nella normativa più recente.

Ripercorrendo, con metodo, le pagine che seguono, si noterà che l'Autore, approfittando anche della conoscenza diretta di molti dei meccanismi che quotidianamente avvengono nel pubblico, cerca di inquadrare i principali istituti del Regolamento nell'attività tipica di una amministrazione pubblica, affrontando questioni interpretative molto spinose.

Molto interessante, infine, è il costante riferimento alla "giurisprudenza" del Garante, ossia a quelle decisioni che il Garante ha dovuto prendere, o a quelle linee guida che l'autorità di controllo ha dovuto elaborare ed emanare, per porre dei "paletti" normativi a tutela, spesso, dei diritti dei cittadini.

Sicuramente la sfida che il GDPR pone al settore pubblico sarà forse più complessa da gestire della sfida posta alle multinazionali e al sistema produttivo in generale.

Il testo di a Beccara consente, però, di orientarsi senza fatica e di fissare alcuni punti essenziali sia per l'interprete sia per il comune cittadino.

Giovanni Ziccardi
Information Society Law Center
Università degli Studi di Milano

Introduzione

Dopo la prima intenzione di abrogare il D. Lgs. 196/2003 (di seguito, il "Codice"), il Legislatore si è – più opportunamente – risolto per una revisione del Codice stesso, mediante una "armonizzazione" (avvenuta con il D. Lgs. 101/2018) rispetto al Regolamento UE 2016/679 (di seguito, il "Regolamento" o il "GDPR"); fonte normativa, quest'ultima, di rango superiore rispetto a quella nazionale[1]. Pertanto, il Codice andrà integralmente[2] interpretato in conformità alla normativa europea, soccombendo in caso di eventuale contrasto con la stessa.

Ne scaturisce un sistema normativo su due livelli, ove quello di rango inferiore è "legittimo" nel momento in cui quello superiore ne consenta un intervento (una sorta di competenza per materia) e purché la disposizione nazionale sia compatibile con quella europea.

All'operatore, quindi, il difficile compito di interpretare in modo coerente al Regolamento tutta quella normativa italiana che, in qualche maniera, possa fare rinvio alla disciplina nazionale in tema di protezione dei dati, o che disciplini – direttamente – alcuni aspetti della stessa materia (si veda, ad esempio, il D. Lgs. 82/2005, il D.P.R. 445/2000, il D. Lgs. 33/2013 e la L. 241/1990). Oltre a questo doppio binario, restano poi i provvedimenti (Autorizzazioni, Linee guida, Regole deontologiche, che costituiscono una sorta di "*soft law*") del Garante, oltre che – soprattutto – l'interpretazione fornita dal Comitato Europeo (di cui all'art. 64 e ss. del Regolamento) sulla normativa europea[3].

Pur godendo di una propria autonoma compiutezza, il presente volume rap-

[1] Vedi l'art. 22, comma 1, del D. Lgs. 101/2018: "*Il presente decreto e le disposizioni dell'ordinamento nazionale si interpretano e si applicano alla luce della disciplina dell'Unione europea in materia di protezione dei dati personali e assicurano la libera circolazione dei dati personali tra Stati membri ai sensi dell'articolo 1, paragrafo 3, del Regolamento (UE) 2016/679*".

[2] Sia la parte non modificata dal D. Lgs. 101/2018, che quella interessata dalla revisione.

[3] Tant'è che M. Iaselli (in G. Cassano *et alia*, *Il processo di adeguamento al GDPR*, Giuffrè Francis Lefebvre Ed., 2018) si riferisce, giustamente, a un "policentrismo delle fonti".

presenta altresì il *sequel* de *La privacy nel pubblico. Sintesi dell'integrazione tra Codice italiano e Regolamento europeo per la Pubblica Amministrazione* (FrancoAngeli, 2018)[4], ponendosi quale sviluppo evolutivo di tale monografia. Se, però, quel testo prendeva le mosse, volta per volta, dall'esame della normativa nazionale per proseguire con l'esame del Regolamento, sarà ora necessario procedere in senso opposto; in altri termini, dall'analisi della normativa europea si procederà a esaminare come il Codice (rielaborato a seguito del succitato D. Lgs. 101/2018[5]) si innesti sul GDPR, precisandone i contenuti. Una buona conoscenza del precedente volume (in cui si sono già trattati, più dettagliatamente, alcuni argomenti e relative disposizioni che qui si tralasciano, anche perché in gran parte confermate – sia pur con gli opportuni adattamenti – nell'attuale versione del Codice) agevola, quindi, anche la lettura del presente testo.

La presente opera include alcuni dei più recenti provvedimenti del Garante, nonché alcuni passaggi più rilevanti della "Relazione annuale – 2017" della stessa Autorità.

Pur essendo principalmente rivolto ai dipendenti pubblici, per l'analisi di alcuni fondamentali concetti e istituti trasversali della privacy (riguardanti, quindi, anche il mondo delle imprese e dei professionisti), il manuale risulta un utile compendio anche per i soggetti privati.

Ogni manuale, per quanto sia stato oggetto di revisione, può presentare errori e refusi. Pertanto, sarà gradita ogni eventuale segnalazione alla Casa Editrice. Le opinioni e le riflessioni espresse nel presente volume, lungi dal costituire un parere legale, si limitano ad esprimere una considerazione generale e sommaria sulla questione. L'autore, pertanto, declina ogni responsabilità per eventuali comportamenti adottati sulla base di tali considerazioni.

[4] Che, quindi, può rappresentare un utile compendio per la valutazione delle nozioni e degli istituti tutt'ora in vigore, oltre che degli argomenti non trattati nel presente manuale.

[5] Sulla cui bozza, vedasi alcuni interessanti documenti: Parere sullo schema di decreto approvato dalla Camera dei Deputati il 20/06/2018; Parere sullo schema di decreto approvato dal Senato della Repubblica il 20/06/2018; Dossier dd. 21/05/2018 del Servizio Studi del Dipartimento di Giustizia; Dossier del maggio 2018 Servizio bilancio dello Stato; Dossier 18/06/2018 sulla posizione degli auditi; Provv. del Garante n. 312, dd. 22/05/2018, Parere sullo schema di decreto legislativo (doc. *web* n. 9163359).

Parte prima

1. Il diritto alla protezione dei dati personali

Ai sensi dell'**art. 1.2 del GDPR**, il diritto alla protezione dei dati personali costituisce un diritto fondamentale.

Diritto, questo, riconosciuto alla persona fisica (e alle imprese individuali) "*a prescindere dalla loro nazionalità o dalla loro residenza*" (C.2-C.14). Pertanto, il Regolamento si applica anche ai presidenti, agli amministratori delegati e a qualsiasi altra persona che agisca in rappresentanza di società, associazioni o enti in genere.

Diversamente, "*il regolamento non disciplina il trattamento dei dati personali relativi a persone giuridiche*[6]*, in particolare imprese dotate di personalità giuridica, compresi il nome e la forma della persona giuridica e i suoi dati di contatto*" (C.14), nonché ai deceduti (in tal caso, però, "*gli Stati membri possono prevedere norme riguardanti il trattamento dei dati personali delle persone decedute*"; C.27). In forza di tale facoltà, il **Codice** ha oggi previsto, all'**art. 2-***terdecies*, che "*i diritti di cui agli articoli da 15 a 22 del Regolamento riferiti ai dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato, in qualità di suo mandatario, o per ragioni familiari meritevoli di protezione*".

[6] Si ricorda come, in relazione alla Direttiva 2002/58/CE (che estende la sua portata applicativa anche a favore delle persone giuridiche), ai sensi dell'art. 95, "*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 di comunicazione nell'Unione, per quanto riguarda le materie per le quali sono soggette a obblighi specifici aventi lo stesso obiettivo fissati dalla direttiva 2002/58/CE*". Il considerando n. 173 specifica che "*la direttiva 2002/58/CE dovrebbe essere riesaminata in particolare per assicurare la coerenza con il presente regolamento*". Sul punto vedi le *Opinion* 3/2016 (WP 240) e 1/2017 (WP 247). Per taluni autori (vedi G. Scorza in G.M. Riccio *et alia* (a cura di), *GDPR e normativa privacy – commentario*, Wolters Kluwer, 2018) i dati relativi alle società di persone sembrerebbero rientrare nella definizione di "dati personali".

Dal momento che "*il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale*" lo stesso "*va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità*" (C.4). In particolare, il Regolamento, come ribadito all'art. 85, "*rispetta tutti i diritti fondamentali e osserva le libertà e i principi riconosciuti dalla Carta, sanciti dai trattati, in particolare il rispetto della vita privata e familiare, del domicilio e delle comunicazioni, la protezione dei dati personali, la libertà di pensiero, di coscienza e di religione, la libertà di espressione e d'informazione, la libertà d'impresa, il diritto a un ricorso effettivo e a un giudice imparziale, nonché la diversità culturale, religiosa e linguistica*" (C.4).

Ai sensi dell'**art. 1.3 del GDPR** "*la libera circolazione dei dati personali*[7] *nell'Unione non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali*".

Considerato che "*la direttiva 95/46/CE non ha impedito la frammentazione dell'applicazione della protezione dei dati personali nel territorio dell'Unione, né ha eliminato l'incertezza giuridica o la percezione, largamente diffusa nel pubblico, che in particolare le operazioni online comportino rischi per la protezione delle persone fisiche*" (C.9) scopo primario del Regolamento è "*assicurare un livello coerente ed elevato di protezione delle persone fisiche e rimuovere gli ostacoli alla circolazione dei dati personali all'interno dell'Unione, …equivalente in tutti gli Stati membri*". "*È opportuno* – infatti – *assicurare un'applicazione coerente e omogenea delle norme a protezione dei diritti e delle libertà fondamentali delle persone fisiche con riguardo al trattamento dei dati personali in tutta l'Unione*" (C.10).

Pertanto, per assicurare "*un livello coerente di protezione delle persone fisiche in tutta l'Unione e prevenire disparità che possono ostacolare la libera circolazione dei dati personali nel mercato interno, è necessario un regolamento che garantisca certezza del diritto e trasparenza agli operatori economici, comprese le micro, piccole e medie imprese, offra alle persone fisiche in tutti gli Stati membri il medesimo livello di diritti azionabili e di obblighi e responsabilità dei titolari del trattamento e dei responsabili del trattamento e assicuri un controllo coerente del trattamento dei dati personali, sanzioni equivalenti in tutti gli Stati membri e una cooperazione efficace tra le autorità di controllo dei diversi Stati membri*" (C.13).

Resta inteso, peraltro, che "*ove il... regolamento preveda specificazioni o limitazioni delle sue norme ad opera del diritto degli Stati membri, gli*

[7] Seconda, fondamentale, finalità del GDPR. Sulla natura bivalente del Regolamento, vedi G. Scorza in G.M. Riccio *et alia* (a cura di), *GDPR e normativa privacy – commentario*, cit.

Stati membri possono, nella misura necessaria per la coerenza e per rendere le disposizioni nazionali comprensibili alle persone cui si applicano, integrare elementi del presente regolamento nel proprio diritto nazionale" (C.8). Ad esempio, "*per quanto riguarda il trattamento dei dati personali per l'adempimento di un obbligo legale, per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento, gli Stati membri dovrebbero rimanere liberi di mantenere o introdurre norme nazionali al fine di specificare ulteriormente l'applicazione delle norme del presente regolamento*" (C.10).

Di conseguenza, l'**art. 6.2 del GDPR** può stabilire che "*gli Stati membri possono mantenere o introdurre disposizioni più specifiche per adeguare l'applicazione delle norme del presente regolamento con riguardo al trattamento, in conformità del paragrafo 1, lettere c) ed e), determinando con maggiore precisione requisiti specifici per il trattamento e altre misure atte a garantire un trattamento lecito e corretto*" ed il successivo **art. 6.3** può aggiungere che "*la base su cui si fonda il trattamento dei dati di cui al paragrafo 1, lettere c) ed e), deve essere stabilita: a) dal diritto dell'Unione; o b) dal diritto dello Stato membro cui è soggetto il titolare del trattamento. La finalità del trattamento è determinata in tale base giuridica o, per quanto riguarda il trattamento di cui al paragrafo 1, lettera e), è necessaria per l'esecuzione di un compito svolto nel pubblico interesse o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento. Tale base giuridica potrebbe contenere disposizioni specifiche per adeguare l'applicazione delle norme del presente regolamento, tra cui: le condizioni generali relative alla liceità del trattamento da parte del titolare del trattamento; le tipologie di dati oggetto del trattamento; gli interessati; i soggetti cui possono essere comunicati i dati personali e le finalità per cui sono comunicati; le limitazioni della finalità, i periodi di conservazione e le operazioni e procedure di trattamento, comprese le misure atte a garantire un trattamento lecito e corretto*".

"*Il... regolamento prevede anche un margine di manovra degli Stati membri per precisarne le norme, anche con riguardo al trattamento di categorie particolari di dati personali («dati sensibili»). In tal senso, il presente regolamento non esclude che il diritto degli Stati membri stabilisca le condizioni per specifiche situazioni di trattamento, anche determinando con maggiore precisione le condizioni alle quali il trattamento di dati personali è lecito*" (C.10); di qui, la precisazione dell'**art. 9.4 del GDPR**, secondo cui: "*Gli Stati membri possono mantenere o introdurre ulteriori condizioni, comprese limitazioni, con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute*".