InterLex®
RIVISTA DI DIRITTO TECNOLOGIA INFORMAZIONE

Una lettura disincantata del GDPR: qualche dubbio e qualche problema interpretativo

FORUM20 - Alessandro Dario Cortesi* - 7 dicembre 2017

Manca un semestre prima che il GDPR (reg. UE 2016/679) trovi pratica applicazione ma il numero e l'autorevolezza dei suoi commentatori, gli snodi problematici su cui si è appuntata la riflessione degli operatori pratici, alcuni interventi dell'Autorità garante e del Legislatore, ci consentono di formulare dei primi giudizi e qualche previsione.

Sia consentito innanzitutto distinguere la nostra voce dal coro dei *laudatores* che dipingono la disciplina in esso contenuta come fortemente innovativa.

La direttiva 95/46/CE (in continuità con quanto prevedeva la Convenzione del 28 gennaio 1981 del Consiglio d'Europa, citata nel suo considerando 11) assumeva che la libera circolazione delle merci, delle persone, dei servizi e dei capitali, così come i progressi registrati dalle tecnologie dell'informazione, avrebbero aumentato i flussi transfrontalieri dei dati (considerando 5). Si proponeva, quindi, di armonizzare le discipline privacy dei paesi membri, affinché la loro diversità non rappresentasse una barriera al libero scambio.

Il fatto stesso che, a distanza di oltre vent'anni, si sia scelto di riformare la materia attraverso un regolamento (fonte che, a differenza della direttiva, non necessita della mediazione dei singoli Stati, ma si impone direttamente nei loro ordinamenti) prova che la desiderata uniformazione non si sia compiutamente raggiunta, il che è del resto ammesso nel considerando 9 dello stesso GDPR.

Il Regolamento avrà maggiori possibilità di successo? Pare lecito avanzare dei dubbi, su cui torneremo a breve.

Secondo alcuni Autori il Regolamento attuerebbe un netto cambio di prospettiva, dal momento che verrebbe finalmente riconosciuto un "diritto alla protezione dei dati di carattere personale" (considerando n. 1) quale "diritto fondamentale" a tutti i cittadini europei.

Anche questa enfasi mi pare eccessiva.

Innanzitutto perché il Regolamento ha sul punto una portata solo ricognitiva dellaCarta di Nizza, proclamata il 7 dicembre 2000 e nuovamente proclamata il 12 dicembre 2007 a Strasburgo, a cui è stato attribuito il medesimo valore giuridico dei trattati dal Trattato di Lisbona del 13 dicembre 2007) in cui convergono le tutele predisposte dall'art. 7, rispetto della vita privata e familiare, e dall'art. 8, protezione dei dati di carattere personale (profili sempre più compenetrati, secondo la giurisprudenza della Corte di Giustizia).

Ma soprattutto perché, come già la Direttiva, anche il GDPR è molto chiaro nel suo considerando 4 laddove specifica che "il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità".

Anche il Regolamento, quindi, riconosce l'esistenza di interessi pubblici confliggenti (cfr. ad es. considerando 16 e 19) e la necessità di operare un bilanciamento, entro degli spazi in cui si concretizzano le scelte politiche nazionali (cfr. art. 2, comma 2 GDPR). Questa la ragione per cui permangono nel testo del Regolamento frequenti rinvii al diritto degli Stati membri (si vedano, e senza pretese di esaustività, i considerando 8, 10, 19, 121, 129, 142, 146, 152, 153, 154, 155, 163 e gli artt. 6, 8, 9, 14, 15, 28, 29, 32, 36, 37, 38, 39, 40, 42, 43, 49, 53, 54, 62, 80, 85).

A tacer d'altro l'inasprimento delle sanzioni (che ai sensi degli artt. 83 e 84 dovranno essere effettive, proporzionate e dissuasive), la previsione della figura del Responsabile della protezione dei dati (artt. 37 e ss.), l'esplicitazione dei principi di *accountability* (considerando 57 e art. 5 c. 2), di protezione dei dati fin dalla progettazione e per impostazione predefinita (*rectius* il principio di minimizzazione, come ho chiarito in un precedente contributo in questo Forum) hanno ridestato l'interesse delle imprese, sensibilizzate al riconoscimento di questi diritti ai cittadini europei in quanto tali (a prescindere dalla nazionalità o dalla residenza).

È prevedibile che ciò faciliterà la circolazione dei dati in ambito sovranazionale, ma è lecito dubitare che si raggiungerà, anche tramite il Regolamento, il traguardo di una disciplina davvero uniforme e ciò nonostante il ruolo sempre più forte che sono chiamate a svolgere le Autorità garanti, il Gruppo di lavoro ex articolo 29 (della direttiva 95/46/CE), il Garante Europeo della protezione dei dati e nonostante l'attività degli Organismi di certificazione di cui all'art. 43 del GDPR e la redazione dei codici di condotta di cui all'art. 40 GDPR.

Ostacola il raggiungimento di questi obiettivi il dato letterale del GDPR che risulta assai farraginoso, ripetitivo e talvolta oscuro (problema a cui si aggiunge la complessa traduzione in lingua italiana di alcuni sintagmi che complica l'attività dell'interprete), tanto che sono sorti dubbi persino in ordine alla sua sfera applicativa.

Per esigenze di spazio si indicano solo alcuni esempi.

Oggetto di tutela da parte del GDPR sono i dati delle persone fisiche (considerando 14, artt. 1 e 2) salvo che siano trattati da "una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico" (cfr. il poco chiaro considerando 18 e l'art. 2, comma 2, lett. c); non i dati delle persone giuridiche per cui valgono logiche diverse (e a cui è dedicata ad es. la direttiva 2016/943 del Parlamento europeo e del Consiglio, dell'8 giugno 2016 sulla protezione del *know-how* riservato e delle informazioni commerciali riservate/segreti commerciali contro l'acquisizione, l'utilizzo e la divulgazione illeciti).

Alcuni Autori propendono per un'interpretazione restrittiva, che fa in sostanza coincidere la definizione di "persona fisica" con quella di "consumatore". Si ritengono così esclusi dalla tutela i dati delle persone fisiche imprenditori individuali (ma potrebbe estendersi il ragionamento ai liberi professionisti ex art. 2238 c.c., imprenditori non sono, alle imprese familiari ex art. 230-bis c.c., ai titolari di partita iva in genere).

Tale lettura non mi pare condivisibile, per la considerazione, invero banale, che l'imprenditore individuale prima di divenire tale è una persona fisica, per cui valgono le medesime esigenze di tutela di coloro che non svolgono attività d'impresa, essendo ad entrambi applicabili gli artt. 7 e 8 della Carta dei Diritti Fondamentali dell'Unione Europea.

Ma questa considerazione non esaurisce i problemi interpretativi: laddove l'attività economica venga svolta dall'imprenditore individuale, dalla impresa familiare, dal libero professionista nei medesimi locali ove la persona fisica risiede, alcuni dati (come ad es. l'indirizzo della sede legale dell'impresa, il nome del titolare) non potranno rimanere riservati. L'attenzione dovrà essere quindi posta più sui dati che sui soggetti. E del resto lo stesso Garante per la protezione dei dati personali con il provvedimento 20 settembre 2012 n. 262 si interrogava sull'interpretazione da darsi alle modifiche apportate dalla legge 22 dicembre 2011 n. 214 al codice in materia di protezione dei dati personali (d. lgs. 30 giugno 2003 n. 196), dal momento che persino l'esclusione dei dati delle persone giuridiche, introdotta nel 2011, aveva segnato un'inversione di tendenza del legislatore nazionale che aveva lasciato insoddisfatti.

Un altro tema che ha acceso il dibattito attiene ai dati dei defunti, che il considerando 27 del GDPR esclude dal campo di applicazione. La scelta appare formalmente coerente con la volontà di attribuire tutela alla persona fisica, dal momento che, com'è ovvio, con la morte, essa viene meno. Sennonché alcuni legislatori nazionali, come ad esempio quello italiano, si sono spinti da tempo oltre.

Già l'art. 13, comma 3 della legge L. 31/12/1996, n. 675 consentiva l'esercizio dei diritti del defunto da parte di chi dimostrasse interesse. L'art. 9, comma 3 del Codice privacy ha adottato una formulazione ancor più esaustiva, prevedendo la legittimazione a "chi ha un interesse proprio, o agisce a tutela dell'interessato o per ragioni familiari meritevoli di protezione".

Ebbene, atteso che il GDPR, anche su questo tema, rinvia alle scelte dei legislatori nazionali, si auspica che questa apertura permanga: che il Regolamento non segni cioè un arretramento delle tutele.

Altri articoli del GDPR, che (questi sì) hanno introdotto delle importanti innovazioni, necessitano di disposizioni attuative. Mi riferisco in particolare:

- alla pseudonimizzazione dei dati (considerando 26 e art. 4 GDPR), che risulta centrale, ex art. 6 u.c. lett. e) del GDPR, per considerare lecito il trattamento dei *big data* per finalità diverse da quelle per cui è stato raccolto il consenso (in assenza di una norma di copertura);

- al diritto alla portabilità (considerando 68 e art. 20 GDPR), dal momento che occorrerà fare chiarezza su cosa si intenda per "formato strutturato, di uso comune e leggibile" e in quali casi potrà ritenersi "non tecnicamente fattibile" la trasmissione diretta da un titolare di trattamento all'altro;
- al diritto di opposizione ad un processo decisionale automatizzato (art. 21 e ss. GDPR) poiché, in tanto potrà esservi vero consenso, in tanto avrà senso richiedere l'intervento umano, si potrà esprimere la propria opinione e contestare la decisione, in quanto venga rivelato all'interessato l'algoritmo in funzione del quale la decisione automatica viene operata: è facile preconizzare che tale ostensione, in difetto di una previsione normativa esplicita, ben difficilmente troverà attuazione.

Un utile approfondimento di questi aspetti potrebbe giungere anche dalla pubblicazione del regolamento europeo e-privacy che dovrebbe abrogare la direttiva 2002/58/CE del 12 luglio 2002 relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche. Questo regolamento è atteso, secondo quanto riferisce il Garante europeo, entro il mese di maggio 2018.

Nel frattempo gli interventi del legislatore nazionale, non offrono chiarimenti su questi temi, ma destano ulteriori perplessità.

Con l'art. 13 della legge 25 ottobre 2017 n. 163 (legge di delegazione europea 2016/2017), il Governo è stato delegato ad adottare entro sei mesi dal 21 novembre 2017, uno o più decreti delegati legislativi per adeguare la disciplina della privacy interna con la direttiva. In considerazione del fatto che, come è noto, le sorti del Governo Gentiloni sono in bilico, rappresenterebbe un buon risultato riuscire ad esercitare tempestivamente la delega ricevuta. Ritengo in altre parole remota l'eventualità che gli operatori pratici ricevano indicazioni in tempo utile rispetto al termine del 25 maggio 2018 in cui diverrà applicabile il GDPR. Questo termine non sarà certamente prorogato e quindi possiamo al più attenderci che il Garante diluisca nel tempo le attività ispettive più invasive o quanto meno mitighi le sanzioni comminate in relazione alla "novità" della disciplina.

Ma, mentre fervono gli sforzi delle imprese per adeguare i propri sistemi informativi al GDPR, in un'ottica di minimizzazione, il legislatore con la legge 20/11/2017, n. 167, Legge europea 2017, "al fine di garantire strumenti di indagine efficace in considerazione delle straordinarie esigenze di contrasto al terrorismo, anche internazionale", ha innalzato il termine di conservazione dei dati di traffico telefonico e telematico nonché dei dati relativi alle chiamate senza risposte da rispettivamente due anni, un anno e trenta giorni (art. 132 codice della privacy) a ben 72 mesi!

In sede applicativa immaginiamo che susciti importanti riflessioni, da ultimo, il tema della notifica delle violazioni dei dati personali all'autorità di controllo ex art. 33 GDPR.

Contrariamente a quanto è stato sostenuto da alcuni Autori, la formulazione dell'art. 33 è chiara. Si dovrà inviare una tempestiva notificazione al ricorrere di entrambe le condizioni: a) che si verifichi una certa "violazione dei dati personali"; b) che la violazione (certa) renda "non improbabile" la sottoposizione a rischio dei "diritti e delle libertà delle persone fisiche". In altre parole in caso di incerta *data breach* non sarà dovuta la notificazione. Essa non sarà dovuta nemmeno nel caso in cui possano razionalmente escludersi rischi per i diritti e le libertà delle persone fisiche.

Sennonché il codice della privacy italiano punisce all'art. 168, salvo che il fatto costituisca più grave reato, con la reclusione da sei mesi a tre anni (*inter alia*) la falsità nelle comunicazioni di cui all'art. 32-bis, commi 1 e 8, ovvero la notificazione della violazione dei dati.

Giacché la legge 163/2017 delega il Governo anche all'aggiornamento delle sanzioni, è possibile, ed anzi probabile, che venga mantenuta la scelta della comminatoria di reato. Se così fosse, occorrerebbe prestare ossequio al divieto di autoincriminazione (*nemo tenetur se detegere*), principio basilare del processo penale, di cui sono espressione fra gli altri gli artt. 63 comma 1, 191 comma 1 e 198 comma 2 c.p.p. e l'art. 384, comma 2 c.p., ma che, seppure con diverse sfumature, si ritiene ben presente nelle fonti europee, come corollario del principio del giusto processo e del giusto procedimento.

* Professore a contratto di Informatica giuridica presso l'Università Cattolica del Sacro Cuore di Milano.

Per intervenire nel Forum, clicca qui
Inizio pagina Indice del Forum Home

Pubblicazione iscritta nel registro della stampa del Tribunale di Roma con il n. 585/97 - Direttore responsabile Manlio Cammarata - P. IVA 13001341000