KnowIT

Rivista scientifica per i manager della governance digitale e della privacy

Operazione DATA PROTECTION

IL FUTURO DELLA PROTEZIONE DEI DATI SECONDO IL REGOLAMENTO 679/2016

KnowIT. Periodico trimestrale. Anno II N. 1 - Marzo 2017 - ISSN 2532-1684

Indice

KnowIT. Rivista scientifica trimestrale gratuita per i manager della governance digitale e della privacy.

Anno 2 - Numero 1 - Marzo 2017 - Testata iscritta al n. 6/2016 del Registro della Stampa del Tribunale di Lecce il 23 maggio 2016 - ISSN 2532-1684

Direttore responsabile: Silvia Riezzo

Direttore editoriale: Andrea Lisi

Editore: Clio S.p.A. Via 95° Rgt. Fanteria n°70 - 73100 Lecce. Tel. +39 0832 344041 - Fax +39 0832 340228 - www.clio.it - info@clio.it

EDITORIALE: La protezione del dato si evolve e concretizza sui binari del cambiamento digitale

Andrea Lisi - *Direttore Editoriale KnowIT, Presidente ANORC Professioni*

Xiaolu Guo (scrittrice e regista cinese) si è posta recentemente questi interessanti interrogativi: "Perché la gente ha bisogno di privacy? Perché la privacy è importante? In Cina, ogni famiglia vive insieme coi nonni, genitori, figlie, figli e parenti più prossimi. Mangia insieme e condivide tutto, parla di tutto. La privacy rende le persone sole. La privacy fa cadere a pezzi la famiglia". Effettivamente, **se nel mondo "analogico" eravamo sempre più gelosi della nostra riservatezza, in quello digitale** sembriamo essere più vicini alla vita collettiva cinese e **cediamo frammenti di noi stessi ogni giorno**, spesso senza saperlo. Anche la normativa ormai ha preso atto di questo cambiamento sociale, infatti è indispensabile prima di tutto ricordare un concetto: **il Regolamento 679/2016 non si occupa di privacy**, il che è anche ovvio se si pensa che in una società ormai costantemente partecipata e trasparente come quella digitale è difficile, se non impossibile, poter affermare con forza il proprio diritto al rispetto della vita privata e familiare, diritto che ogni giorno, in modo consapevole e inconsapevole, noi stessi calpestiamo navigando on line. Eppure quel diritto rimane solennemente proclamato nell'art. 7 della Carta dei diritti fondamentali dell'Unione Europea[1].

Nell'articolo immediatamente successivo della stessa Carta viene riconosciuto con altrettanta importanza e pienezza **il diritto alla protezione dei dati personali**[2], il quale viene sintetizzato nei suoi punti essenziali. Tale diritto è qualificato come fondamentale per l'individuo anche dal nuovo Regolamento europeo (considerando n. 1[3]), ma allo stesso tempo al considerando n. 4 si precisa che esso **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. Del resto, nel successivo considerando n. 9, lo stesso legislatore europeo esprime consapevolezza del fatto che la rapidità dell'evoluzione tecnologica e la globalizzazione comportino nuove sfide per la protezione dei dati personali: la portata della condivisione e della raccolta di dati personali è aumentata in modo significativo e la tecnologia attuale consente, tanto alle imprese private quanto alle autorità pubbliche, di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività. Il considerando si conclude prendendo atto del fatto che sempre più spesso le persone fisiche rendono disponibili al pubblico, su scala mondiale, informazioni personali che le riguardano e che pertanto la tecnologia ha irrimediabilmente trasformato l'economia e le relazioni sociali, facilitando inevitabilmente la libera circolazione dei dati personali all'interno dell'Unione e il loro trasferimento verso paesi terzi e organizzazioni internazionali, a cui si deve però accompagnare sempre la garanzia di un loro elevato livello di protezione. Leggendo i primi considerando al Regolamento appare quindi chiaramente come anche secondo il legislatore europeo quella vecchia concezione del diritto alla privacy, definito in passato come *the right to be alone*, si stia andando a schiantare ogni giorno contro le pareti liquide della società dell'informazione e si avverte così tra le pieghe della normativa dell'Unione quasi una rassegnata resa alla situazione odierna. **Ma se la privacy rischia di non esistere più e anche il *the right to be forgotten*** (cioè il famoso "diritto all'oblio", di cui tanto si parla per la sua evanescenza in ambito digitale e che oggi comunque si ritrova almeno citato nell'art. 17 del Regolamento) **non se la passa bene, il diritto alla protezione del dato invece ritrova una sua ragione per sopravvivere e addirittura per rafforzarsi**, pur se le sue radici organizzative sono state profondamente ridisegnate rispetto a quanto previsto nella precedente direttiva 95/46/CE, ormai abrogata.

Del resto lo stesso legislatore europeo, nel considerando n. 9 del Regolamento, sottolinea che, sebbene i suoi obiettivi e principi rimangano tuttora validi, 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. Insomma, **per il legislatore europeo il mondo è cambiato e occorre prenderne atto e il diritto alla protezione dei dati va così adeguato alle nuove esigenze di una società completamente diversa**.

Cosa è cambiato allora rispetto alla direttiva e allo stesso Codice della protezione dei dati personali (D.Lgs. 196/2003) che ne costituisce il recepimento? Va riferito prima di tutto che il Codice italiano è andato ben al di là della direttiva europea di recepimento, rimanendo così, ancora oggi, piuttosto attuale in molti suoi punti che sembrano costituire quasi una sorta di anticipazione di ciò che oggi il Regolamento riferisce. Il Codice, va detto, è inevitabilmente invecchiato e risente di un'impostazione molto formale e rigida nelle sue elencazioni e regole, rispetto a un **Regolamento che guarda**

invece alla sostanza della protezione dei dati, attribuendo ai titolari del trattamento prima di tutto delle precise responsabilità e non vuoti formalismi da rispettare. Quindi non dobbiamo stupirci se i rivoluzionari principi della *privacy by design* e *privacy by default*, che si ritrovano espressi con forza nei commi 1 e 2 dell'art. 25 del Regolamento[4], fossero già presenti in uno stato embrionale nell'art. 3 del Codice della protezione dei dati[5]. Ma la loro attuazione nel Regolamento non è lasciata a un elenco di misure minime, necessarie e idonee e a precisi provvedimenti delle Authority (i quali si spera siano d'aiuto per un adempimento formale e ossequioso delle regole); oggi il mondo è sempre più complesso e mutevole, il contesto di riferimento varia ogni giorno e le regole occorre costruirsele da soli in base a una accurata seduta di autoanalisi realizzata con l'aiuto del proprio DPO (Data Protection Officer)!

Insomma, **il cuore del Regolamento è l'*accountabilty***, intesa come responsabilizzazione piena dei protagonisti del trattamento dei dati (titolari e responsabili del trattamento dei dati), i quali devono cooperare costantemente tra loro e con i loro auditor indipendenti (i DPO – *Data Protection Officer*) per dare forma e soprattutto sostanza adeguata alle politiche di trattamento portate avanti dalle loro strutture. Questa è la reale innovazione nella normativa. Infatti, è **proprio l'approccio organizzativo al trattamento che è cambiato in modo radicale**, non tanto per la previsione obbligatoria di quel Registro delle attività di trattamento dei dati contenuta nell'art. 30 del Regolamento[6] e che per noi costituisce una sorta di riedizione del DPS (Documento Programmatico per la Sicurezza) - improvvidamente abrogato in passato nonostante le critiche di chi, come il sottoscritto, ripeteva che sarebbe rientrato come obbligo con questo Regolamento -, quanto per l'impatto organizzativo che tale Regolamento contiene, sia a livello di presìdi anche archivistici da predisporre, sia per le competenze che occorre indispensabilmente formare all'interno di ogni organizzazione per adeguarsi allo stesso.

Del resto, l'articolo 2 del Regolamento, precisando l'ambito di applicazione della normativa, sottolinea che lo stesso "si applica al trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio[7] o destinati a figurarvi", in qualche modo facendoci cogliere sin dall'inizio della lettura che l'unico modo per adeguarsi ai suoi dettami è sviluppare una strategia appropriata, che abbia un'impostazione anche archivisticamente coerente e che consenta così di documentare opportunamente le scelte fatte, di verificare l'impatto di ogni trattamento, di selezionare le varie tipologie di dati trattati e le relative tempistiche di trattamento e di garantire, quindi, un'organizzazione in linea con i rischi effettivi (e adeguatamente verificati) che i dati trattati corrono, presidiata da misure coerenti con quanto rilevato e documentato. Solo in questo modo si possono evitare le pesantissime sanzioni previste nel Regolamento.

Del resto, se mancasse in un'azienda o pubblica amministrazione un'adeguata organizzazione atta a presidiare i trattamenti dei dati personali sviluppati dalla struttura risulterebbe impossibile concretizzare le previsioni contenute, ad esempio, negli articoli 20 (in base al quale l'interessato ha il diritto di ricevere, in un formato strutturato, di uso comune e leggibile da dispositivo automatico, i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti) o 13 (che precisa come lo stesso interessato abbia anche il diritto di conoscere sempre il periodo di conservazione dei dati che lo riguardano). Per concludere queste brevi considerazioni, appare indubbio che la vera innovazione nel Regolamento è l'approccio alla protezione del dato personale: i titolari del trattamento dovranno sempre più fare i conti con il passaggio da un approccio "formalmente regolare" a un approccio "effettivamente conforme", finalizzato a rendere effettivi principi e regole generali da applicare attraverso la predisposizione di modelli organizzativi validati dallo sforzo pervasivo e programmatico di preparati team multidisciplinari.

Note

1. Articolo 7 - Rispetto della vita privata e della vita familiare - Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle proprie comunicazioni.
2. Articolo 8 - Protezione dei dati di carattere personale -
   1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.
   2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica.
   3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente.
3. Considerando n. 1 al Regolamento 679/2016: la protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale. L'articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea («Carta») e l'articolo 16, paragrafo 1, del trattato sul funzionamento dell'Unione europea («TFUE») stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.
4. Articolo 25 - Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita
   1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.
   2. Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e

l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.

5. Art. 3 - Principio di necessità nel trattamento dei dati

1. I sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità.

6. Articolo 30 - Registri delle attività di trattamento

1. Ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità. Tale registro contiene tutte le seguenti informazioni:
   a) il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;
   b) le finalità del trattamento;
   c) una descrizione delle categorie di interessati e delle categorie di dati personali;
   d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
   e) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;
   f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
   g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1 […]

7. Art. 4 (definizioni) comma 1 punto 6) «archivio»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico.

L'eziologia dell'archivio nell'ambito di applicazione materiale del Regolamento

Francesca Cafiero - *Consulente archivista Digital&Law Department*

L'assenza di un dato, è un dato anch'esso. Questo è uno degli insegnamenti cardine delle discipline legate ai beni culturali e più in generale alla ricerca storica, che fondano la loro epistemologia attorno alla ricostruzione di dati, antichi di secoli e talvolta di millenni[1].

Come per quelle antiche, **anche per le moderne basi di dati il problema della possibile perdita del contenuto resta uno dei nodi fondamentali**, la cui entità aumenta proporzionalmente in relazione alla stessa capacità di ritenzione, accresciuta esponenzialmente negli ultimi decenni, per merito del processo di dematerializzazione e di successiva digitalizzazione del flusso informativo e documentale.

Tale monito può rivelarsi parimenti prezioso se rapportato al contesto digitale, nel quale è stato necessario pensare e adottare nuove metodologie e strumenti volti alla corretta progettazione e gestione delle basi di dati.

Nondimeno tale esigenza è stata debitamente presa in considerazione dal nuovo Regolamento Europeo sulla privacy, il cui ambito di applicazione ai sensi dell'articolo 2, comma 1 è stato circoscritto ai «dati personali contenuti in un archivio o destinati a figurarvi». Il Regolamento affronta dunque il tema della protezione delle persone fisiche, con riguardo al trattamento dei dati personali, imponendo un approccio razionale e sistematico alle singole attività, **presupponendo che gli stessi dati oggetto di protezione debbano necessariamente essere strutturati secondo criteri specifici**. Dal momento che non è più la semplice raccolta di dati, ma **l'archivio, a costituire il contesto di riferimento**, sembrerebbe altrettanto opportuno presupporre che i c.d. criteri specifici, debbano logicamente essere quelli archivistici.

Procedendo con ordine, è opportuno anzitutto affrontare la rivalsa dell'archivio attraverso l'enucleazione degli aspetti sostanziali e formali che attengono strettamente al corretto trattamento dal dato. Un ragionamento di tipo induttivo sembrerebbe adatto ad abbracciare i contenuti del nuovo Regolamento Europeo che non pretende di fornire un'introspezione sulle regole dell'archivistica "pura", al fine di condividere a livello Europeo anche i criteri di organizzazione e strutturazione degli archivi stessi, ma piuttosto cerca di attingere dalla disciplina, nelle sue diverse declinazioni funzionali, quanto basta affinché la gestione archivistica del dato diventi la *conditio sine qua non* della *compliance* normativa.

Specularmente l'introduzione del Regolamento sembra incidere significativamente sulla tradizionalissima prospettiva archivistica attraverso una "sana" contaminazione, che ne prevede l'applicazione nei confronti dei depositi costituiti da dati, *sic et simpliciter*.

Non a caso la definizione contenuta nell'art.4 del nuovo Regolamento («qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico») connota l'archivio in base a criteri di strutturazione "determinati", sebbene non meglio specificati, finalizzati a garantire sostanzialmente l'accessibilità al dato.

Tuttavia proprio i criteri di strutturazione differenziano un archivio di dati personali da una semplice raccolta di tipo domestico: mentre quest'ultima, come nel caso di una rubrica telefonica o di una bacheca di un social network, contiene dati - certamente personali - che si accumulano in maniera sostanzialmente accidentale, senza la precisa intenzione di costituire un complesso documentale che risponda a determinate procedure organizzative, l'archivio invece dovrebbe nascere propriamente dalla sedimentazione del tutto spontanea e naturale della documentazione prodotta/ricevuta nel corso dell'attività di un soggetto produttore e sono i documenti e le loro aggregazioni a costituirne le cellule fondamentali. Oltretutto la sedimentazione dell'archivio è basata sul c.d. "vincolo naturale", che implica non già l'assenza di criteri organizzativi, ma di quella premeditazione dei legami che si instaurano tra i documenti, così come tra loro aggregazioni.

L'apparente contrasto tra base di dati e archivio sembrerebbe trovare tuttavia una soluzione in uno dei considerando, il n.15, che approfondisce ulteriormente i confini del Regolamento, escludendo dall'ambito di applicazione i dati contenuti in «fascicoli o serie di fascicoli non strutturati secondo criteri specifici, così come le rispettive copertine». Tralasciando il riferimento un po' nostalgico alle "copertine" dei fascicoli – dal quale trapela il sentore di una connotazione dell'archivio ancora analogica - è importate considerare l'accenno ad architetture strutturate secondo "criteri specifici", in fascicoli e serie di fascicoli, sconosciute alle basi di dati, verosimilmente di matrice archivistica.

Tuttavia l'approccio archivistico percepibile nel Regolamento coincide con l'esigenza di organizzazione siste-

matica dei dati personali, piuttosto che con l'archivio nella sua accezione tradizionale e in tale prospettiva sembrerebbero sostanziarsi i principi della privacy *by design e della privacy by default*. È opportuno a tal proposito ribadire l'importanza che la fase progettuale aveva assunto parimenti per la costituzione di archivi digitali: prima ancora della gestione, è la progettazione che necessita di essere curata per consentire la corretta sedimentazione della documentazione all'interno di un ambiente adeguato, basato su sistemi integrati.

Di fatto la dimensione dell'archivio, applicata al contesto digitale, può garantire l'adozione di architetture e modelli di riferimento, fondati su metodologie di antica tradizione, in grado di assicurare, anche alla luce delle recenti contaminazioni, una solidità per la protezione non solo formale delle persone fisiche, ma anche effettiva e sostanziale. Alla luce di tali considerazioni il nesso tra trattamento organizzato dei dati personali e ambito di applicazione materiale del Regolamento potrebbe essere letto alla luce di una nuova prospettiva: in sostanza, l'archivio non fungerebbe soltanto da strumento di protezione (a trattamento iniziato), ma anzitutto da criterio di interpretazione dell'ambito materiale della protezione.

L'inedita attenzione agli aspetti di organizzazione archivistica è uno degli elementi di maggior rilievo del Regolamento europeo, che imprese, enti e PA dovranno tenere nella dovuta considerazione.

Note

[1] Lo stesso principio può essere ammantato di significato giuridico, tanto più pregnante se l'assenza del dato è da relazionare a un documento informatico.

Le obbligazioni di *compliance* previste nel nuovo Regolamento europeo in materia di protezione dei dati personali

Franco Cardin - *Team privacy del D&L Department e coordinatore del Direttivo ANORC*

Premessa

Dopo una lunga gestazione durata più di quattro anni, il 4 maggio 2016 è stato pubblicato sulla GUCE il nuovo Regolamento europeo 2016/679, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali. Pur essendo entrato in vigore il 25 maggio 2016, il Regolamento diventerà applicabile, per espressa previsione dell'art. 99, paragrafo 2, a partire dal prossimo 25 maggio 2018[1].

Le ragioni che hanno spinto il legislatore europeo ad approvare questo nuovo strumento normativo sono da ricercarsi nella necessità non solo di adeguare le disposizioni contenute nella direttiva 95/46/CE al nuovo contesto della società dell'informazione - caratterizzata da un sempre maggiore utilizzo delle tecnologie informatiche e telematiche - assicurandone nel contempo un livello di applicazione coerente ed elevato in tutti gli stati membri dell'Unione europea, ma anche e soprattutto di **garantire che gli obblighi giuridici in materia di protezione dei dati personali si traducano in meccanismi efficaci** che consentano una protezione reale dei medesimi dati.

In considerazione delle peculiarità del nuovo contesto della società dell'informazione, caratterizzato dal continuo aumento della quantità di dati personali trattati (e, quindi, anche dal possibile aumento dei rischi per i diritti e le libertà fondamentali delle persone fisiche), ma anche del fatto che la direttiva 95/46/CE non è pienamente riuscita a garantire la traduzione degli obblighi giuridici in materia di protezione dei dati personali in meccanismi efficaci in grado di consentire una reale protezione degli stessi, il legislatore europeo ha ritenuto opportuno e necessario introdurre una nuova architettura giuridica che consenta il passaggio dalla teoria dei principi di protezione dei dati personali alla loro messa in pratica.

In questa nuova architettura giuridica contenuta nel Regolamento europeo 679/2016, **il motore** per l'attuazione efficace dei principi di protezione dei dati personali è rappresentato dall'introduzione del cosiddetto principio di responsabilità (***accountability***), il cui scopo è quello di incoraggiare i titolari del trattamento ad adottare, in funzione dei rischi intrinseci in ogni specifico trattamento, misure organizzative, tecniche e politiche adeguate che consentano da un lato di rendere effettivi i principi di protezione dei dati personali e, dall'altro, di assicurarne l'efficacia e di dimostrarne il rispetto.

Il principio di responsabilità (*accountability*) e le obbligazioni di *compliance*

Tra le diverse novità introdotte dal Regolamento europeo 679/2016, quella che maggiormente impatta sul piano culturale, organizzativo e tecnico è **l'introduzione del predetto principio di responsabilità[2]**, che si concretizza non solo nel rispetto degli altri principi generali del trattamento dei dati personali - previsti nel paragrafo 1 dell'art. 5 del medesimo regolamento - ma anche nella capacità del titolare del trattamento di dimostrare di averli osservati[3].

Spetta, infatti, al titolare del trattamento, come specificato nel successivo art. 24, paragrafo 1, l'onere di mettere in atto - tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi per i diritti e le libertà delle persone fisiche - misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al regolamento, nonché di aggiornarle qualora sia necessario.

È opportuno ricordare, inoltre, che il paragrafo 2 del medesimo art. 24 precisa che le predette misure tecniche e organizzative includono, qualora ciò sia ritenuto proporzionato rispetto alle specificità delle attività di trattamento e ai particolari rischi a esse collegati, l'attuazione da parte del titolare del trattamento di politiche interne adeguate[4].

Costituiscono, in particolare, misure obbligatorie di attuazione del principio di responsabilità:

- la predisposizione dell'accordo interno tra due o più contitolari del trattamento previsto nell'art. 26;
- la stipula dei contratti o di altri atti giuridici relativi alle designazioni a responsabile e subresponsabile del trattamento prevista nell'art. 28;
- l'effettuazione, nei casi in cui i trattamenti comportino un rischio elevato per i diritti e le libertà fondamentali delle persone fisiche, della valutazione d'impatto sulla protezione dei dati personali, prevista nell'art. 35;
- la designazione del Responsabile della protezione dei dati personali (DPO) nei casi previsti nell'articolo 37, paragrafo 1;
- l'adozione delle norme vincolanti d'impresa nei casi previsti nell'art. 47;
- l'adozione delle misure atte a soddisfare i principi della protezione dei dati personali fin dalla progettazione (*privacy by design*) e della protezione dei dati di *default* (*privacy by default*).

Oltre alle predette misure obbligatorie, il nuovo Regolamento europeo ne prevede altre che possono essere volontariamente adottate dal titolare del trattamento allo scopo di consentire un'ulteriore garanzia del rispetto dei principi fondamentali di protezione dei dati personali.

Tra queste ultime meritano di essere ricordate, in particolare, l'effettuazione di adeguati piani di formazione di tutto

il personale coinvolto in operazioni di trattamento di dati personali, l'adesione ai codici di condotta e ai meccanismi di certificazione, la realizzazione di audit interni o esterni che consentano di verificare periodicamente l'applicazione corretta delle misure di sicurezza organizzative e tecniche, la definizione di procedure interne per la gestione dei reclami inoltrati dagli interessati, la predisposizione di regole interne che consentano di gestire prontamente e in modo efficace gli eventi di *data breach*.

Conclusioni

Se la scadenza del 25 maggio 2018 può apparire non immediata, non bisogna sottovalutare che l'attuazione delle obbligazioni di *compliance* previste nel nuovo Regolamento europeo 679/2016 comportano - in particolare per i soggetti pubblici e privati che trattano rilevanti quantità di dati personali o che svolgono attività che implicano, per loro natura, ambito di applicazione e finalità perseguite, particolari rischi per i diritti e le libertà fondamentali delle persone fisiche - un significativo impegno non solo sul piano culturale e organizzativo, ma anche probabilmente su quello economico, a causa dei necessari investimenti finalizzati, da un lato, a garantire un adeguato livello di sicurezza dei dati personali e, dall'altro, a non incorrere nelle pesanti sanzioni introdotte dal nuovo Regolamento europeo.

È **fortemente consigliato, pertanto, che si inizi già da ora il percorso di adeguamento ai nuovi obblighi di *compliance*** previsti dal nuovo Regolamento europeo che, come si è visto, impone ai titolari del trattamento, con l'introduzione del principio di responsabilità, non solo l'adozione di misure tecniche e organizzative finalizzate a garantire un livello di sicurezza adeguato al rischio, ma anche l'onere di dimostrare, in caso di controlli, la conformità delle stesse. Considerata la complessità delle attività da svolgere è opportuno che questo percorso di adeguamento sia gestito da una **squadra multidisciplinare**, nella quale sia garantita la presenza di diversi professionisti (giurista, informatico, esperto di organizzazione, esperto di processi, ecc.) e preveda almeno le seguenti azioni:

1. mappatura di tutti i trattamenti in corso o programmati;
2. individuazione, tramite l'effettuazione di una *gap analysis*, delle criticità individuate e dei trattamenti maggiormente esposti a rischi per i diritti e le libertà fondamentali degli interessati;
3. predisposizione di un piano di transizione che individui ciò che deve essere modificato/integrato;
4. designazione, qualora sia obbligatorio o comunque ritenuto opportuno, del Responsabile della protezione dei dati personali (DPO);
5. effettuazione, se ritenuto necessario a seguito dell'analisi dei rischi, della valutazione d'impatto sulla protezione dei dati;
6. revisione delle informative e dei consensi;
7. revisione degli incarichi, con particolare riferimento a quelli dei fornitori nella loro qualità di responsabili del trattamento;
8. predisposizione di procedure atte a garantire e facilitare l'esercizio dei diritti degli interessati;
9. impostazione e redazione delle nuove documentazioni obbligatorie finalizzate a dimostrare l'adeguatezza e l'efficacia delle misure organizzative e tecniche adottate (registro dei trattamenti, eventi di *data breach*, valutazione d'impatto ecc.);
10. predisposizione di un piano di sicurezza dei dati e dei sistemi;
11. predisposizione delle procedure finalizzate a garantire l'obbligo di notifica all'Autorità di controllo e, nei casi ritenuti necessari, di comunicazione agli interessati, degli eventi di *data breach*;
12. definizione delle modalità necessarie a garantire un presidio continuativo, sia legale che informatico, su tutte le attività di trattamento dei dati personali.

Al fine di garantire l'efficacia delle predette azioni di adeguamento si ritiene, infine, che sia indispensabile coinvolgere tutti i soggetti che sono preposti a effettuare operazioni di trattamento dei dati personali in **un adeguato piano di formazione** finalizzato a far conoscere le più importanti novità introdotte dal nuovo Regolamento europeo 679/2016.

Note

[1] Trattandosi, infatti, di un regolamento non sarà necessario, come nel caso delle direttive, che venga recepito da una legge nazionale, ma diventerà applicabile direttamente in tutti gli Stati membri della Comunità Europea.

[2] L'introduzione di tale principio era stato caldamente suggerito dal Gruppo di lavoro ex art. 29 nel parere n. 3/2010, nel quale si evidenziava la necessità di riaffermare e rafforzare la responsabilità dei titolari del trattamento prevedendo l'obbligo di adottare misure organizzative e tecniche adeguate ed efficaci, non solo per attuare i principi di protezione dei dati personali, ma anche per dimostrare che le stesse misure siano state effettivamente implementate, fornendone la prova nel caso venga espressamente richiesto.

[3] Il paragrafo 2 del medesimo articolo 5, infatti, precisa che: "Il titolare del trattamento è competente per il rispetto del paragrafo1 e in grado di comprovarlo ("responsabilizzazione")".

[4] È opportuno sottolineare che l'adeguatezza delle misure organizzative e tecniche e delle eventuali politiche interne adottate deve essere valutata caso per caso, non solo prima che il trattamento venga effettuato ma anche successivamente con riferimento alla loro effettiva efficacia.

Data protection by design and by default nella PA: la trasparenza dei "dati ulteriori"

Alessandra Foschetti – *Semplificazione amministrativa e promozione della cittadinanza attiva presso il Comune di Bologna*

Il Regolamento sulla privacy 2016/679 del Parlamento europeo e del Consiglio introduce, accanto al principio di *privacy by design*, il concetto ulteriore di *privacy by default*, in considerazione del fatto che l'approccio alla protezione dei dati personali e alla privacy non può essere basato esclusivamente su una valutazione di conformità normativa, ma vada applicato il principio di "tutela della vita privata per impostazione predefinita" in qualsiasi processo.
La normativa italiana sulla trasparenza amministrativa e le diverse modulazioni dell'accesso ai dati/documenti (al momento in Italia ne abbiamo tre: accesso civico, accesso civico generalizzato – cd. Foia – accesso e L. 241/90, cui potremmo aggiungere l'accesso "ai dati" in regime di interoperabilità tra pubbliche amministrazioni) **rendono particolarmente complesso il processo di progettazione delle applicazioni a garanzia della trasparenza e del rispetto dei principi sulla privacy**.
Infatti, a seconda che l'interessato vanti un diritto soggettivo o un interesse legittimo, diverso è il grado di ostensibilità dei dati personali qualora si tratti di documenti da pubblicare obbligatoriamente oppure richiesti ai sensi della L. 241/90.

Il D.lgs. n. 33/2013 (Decreto Trasparenza), nelle indicazioni operative per la pubblicazione dei dati nelle sezioni "Amministrazione Trasparente" aveva indicato, nella sua formulazione originale – tale è restata fino alla riforma del D.lgs. 97/2016 - la pubblicazione di schede sintetiche di taluni provvedimenti che ne riportino il contenuto, l'oggetto, l'eventuale spesa prevista, oltre le informazioni che rendono il documento identificabile (data, numero di protocollo, ufficio o soggetto che lo ha formato).
L'obbligo riguardava quindi la pubblicazione, ma non in forma integrale. Secondo quanto previsto dall'art. 23 c. 1 del Decreto Trasparenza, le amministrazioni erano tenute a pubblicare gli elenchi (ovvero delle schede) dei provvedimenti finali dei seguenti procedimenti:

a) autorizzazione o concessione;

b) scelta del contraente per l'affidamento di lavori, forniture e servizi, anche con riferimento alla modalità di selezione prescelta ai sensi del codice dei contratti pubblici, relativi a lavori, servizi e forniture, di cui al D.lgs. n. 163/2006;

c) concorsi e prove selettive per l'assunzione del personale e progressioni di carriera di cui all'art. 24 del D.lgs. n. 150/2009;

d) accordi stipulati dall'amministrazione con soggetti privati o con altre amministrazioni pubbliche.

Questi stessi provvedimenti pubblicati in forma sintetica nella sezione apposita, rientravano però anche tra quelli a pubblicazione obbligatoria in altre sezioni di Amministrazione Trasparente o comunque sul sito istituzionale dell'ente (si pensi, ad esempio, all'obbligo di pubblicazione in materia di concorsi o di contratti pubblici, in materia di affidamento di lavori, servizi o forniture previsto pure dal nuovo Codice degli Appalti).
Gli enti, chiamati a ripensare alle proprie modalità di gestione dei documenti per permettere la pubblicazione in modo tempestivo e automatico delle tipologie dei provvedimenti indicati dalla normativa, hanno in molti casi integrato l'interfaccia web dei siti istituzionali con i sistemi informatici gestionali interni.
In considerazione dell'esigenza di pubblicare un dato "necessario" ad adempiere gli obblighi previsti, le modalità organizzative e i sistemi erano stati progettati (*privacy by design*) per rispondere alle esigenze di controllo diffuso previsto dalla normativa sulla trasparenza.
L'art. 22 del D.lgs. n.97/2016 di modifica degli obblighi di Trasparenza ha abrogato le disposizioni dell'art. 23 sulla pubblicazione degli elenchi dei provvedimenti finali dei procedimenti relativi ad autorizzazioni e concessioni, concorsi, prove selettive del personale e progressioni di carriera.
Secondo quanto precisato dalle Linee guida ANAC (Del. 1310/2016), "pur rilevandosi un difetto di coordinamento con la legge 190/2012, che all'art. 1, co. 16, lett. a) e d), continua a fare riferimento alla trasparenza dei suddetti procedimenti, tali obblighi devono ritenersi abrogati. Resta ferma la possibilità di esercitare il diritto di accesso civico generalizzato ai provvedimenti sopra indicati, ai sensi degli artt. 5, co. 2 e 5-bis del d.lgs. 33/2013".
In considerazione delle caratteristiche degli stessi, quali provvedimenti in grado di ampliare la sfera giuridica soggettiva (con o senza effetti economici diretti), è elevata la possibilità che essi siano oggetto di "accesso civico generalizzato".
Proprio in ragione di tali considerazioni, in coerenza con le finalità del D.lgs. n. 150/2009 e della legge n. 190/2012 **è data facoltà alle amministrazioni di pubblicare i c.d. "dati ulteriori" ossia dati, informazioni e documenti per i quali non sussista uno specifico obbligo di trasparenza**.
Con l'abrogazione dell'obbligo di pubblicazione e il venire meno dell'esigenza di controllo diffuso (rimandato a istanze di accesso civico), molti enti si trovano oggi a pubblicare,

quindi, dati "ulteriori", in quanto, avendo già predisposto i sistemi per la trasparenza online e non essendo essi incompatibili con la nuova disciplina, la pubblicazione dei provvedimenti sui siti è rimasta integrale.
Non tutti però hanno rilevato che nel pubblicare dati ulteriori rispetto a quelli per i quali è prevista la pubblicazione obbligatoria occorre modulare diversamente la sicurezza dei dati personali relativamente alla disciplina sulla privacy.

L'Autorità Nazionale Anticorruzione-ANAC, d'intesa con il Garante, ha emanato le "Linee guida recanti indicazioni operative ai fini della definizione delle esclusioni e dei limiti all'accesso civico di cui all'art. 5 co. 2 del d.lgs. 33/2013" (Determinazione n. 1309 del 28/12/2016, cfr. anche Provvedimento del Garante recante "Intesa sullo schema delle Linee guida ANAC recanti indicazioni operative ai fini della definizione delle esclusioni e dei limiti all'accesso civico" n. 521 del 15/12/2016, in www.gpdp.it).
Nelle citate Linee guida è indicato che "laddove l'esigenza informativa, alla base dell'accesso generalizzato, possa essere raggiunta senza implicare il trattamento dei dati personali", alla luce dei "principi generali sul trattamento e, in particolare, a quelli di necessità, proporzionalità, pertinenza e non eccedenza, in conformità alla giurisprudenza della Corte di Giustizia Europea, del Consiglio di Stato, nonché al nuovo quadro normativo in materia di protezione dei dati introdotto dal Regolamento (UE) n. 679/20168 […] il soggetto destinatario dell'istanza, nel dare riscontro alla richiesta di accesso generalizzato, dovrebbe in linea generale scegliere le modalità meno pregiudizievoli per i diritti dell'interessato, privilegiando l'ostensione di documenti con l'omissione dei "dati personali" in esso presenti".
Di contro, l'accesso civico (applicabile, a parere di chi scrive, anche ai "dati ulteriori") è rifiutato "se il diniego è necessario per evitare un pregiudizio concreto alla tutela [della] protezione dei dati personali, in conformità con la disciplina legislativa in materia" (art. 5-bis, comma 2, lett. a) del Decreto Trasparenza.)
Resta la possibilità che i dati personali per i quali sia stato eventualmente negato un accesso civico o civico generalizzato possano essere resi ostensibili laddove l'istante dimostri l'esistenza di "un interesse diretto, concreto e attuale, corrispondente ad una situazione giuridicamente tutelata e collegata al documento al quale è chiesto l'accesso" ai sensi degli artt. 22 ss. della L. 241/1990.
La normativa europea sulla tutela dei dati, con il principio della *privacy by default*, da un lato ci viene in soccorso in presenza di una normativa sulla trasparenza così frastagliata. D'altro canto ci pone un problema operativo, in quanto, già in fase di progettazione, approvvigionamento o sviluppo di sistemi per la pubblicazione dei dati occorreva darsi delle *policy* conformi alla tutela oggi indicata dal Regolamento Europeo: **in questo momento la rincorsa agli adeguamenti diventa costosa e foriera di errori, soprattutto perché si va a inserire su piattaforme nelle quali, per la maggioranza dei casi, non è ben chiaro quali dati siano effettivamente trattati**.
La progettazione delle applicazioni, mettendo al centro la tutela del dato e della persona, sia esso destinato alla pubblicazione obbligatoria, facoltativa, per estremi o integrale, è la sola possibilità di garantire una tutela idonea col passare del tempo e delle norme.

Privacy by design: il giusto approccio di fronte al progresso tecnologico

Michele Iaselli - *Presidente ANDIP*

Il progresso tecnologico avanza rapidamente e ormai sono tanti i prodotti o i servizi che si fondano su evolute tecnologie. Ma le nuove tecnologie hanno spesso effetti dirompenti, imponendo cambiamenti radicali nello stile di vita, nell'economia e nel comportamento sociale delle persone, per cui la discussione sui benefici e sui pericoli delle nuove tecnologie è sempre molto accesa. La tecnologia solitamente viene definita neutrale, ma è l'uomo che decide se usarla per scopi buoni o cattivi.

Esiste, quindi, un problema anche di educazione e consapevolezza sociale, che non serve solo a indirizzare il comportamento umano nella direzione corretta, ma anche a mantenere alta l'attenzione sui pericoli che non sono intrinseci a una tecnologia in sé ma che possono derivare dai suoi utilizzi impropri o effetti inattesi.

In tale ambito un contesto normativo trasparente è visto come un elemento chiave per lo sviluppo della tecnologia e di sistemi autonomi di mercato, in cui prodotti e servizi possono essere distribuiti senza problemi. C'è il forte timore da parte di molti che una legislazione prematura e invadente possa ostacolare il progresso scientifico e annullare potenziali vantaggi o peggio ancora causare inefficienze economiche o altro. Allo stesso tempo, in qualche modo paradossalmente, si ammette che la mancanza di un ambiente giuridico affidabile e sicuro possa ugualmente ostacolare l'innovazione tecnologica. Tale difficile situazione mina sicuramente la certezza del diritto e induce la gente ad agire in un settore ambiguo in cui i diritti e le responsabilità non sono preventivamente individuabili.

Un problema spesso sottolineato quando si affronta la tematica del rapporto tra tecnologia e regolamentazione è la lentezza della legge, nel senso che **l'innovazione tecnologica è molto più rapida del legislatore, che interviene con notevole ritardo** a regolare l'introduzione di determinati prodotti o servizi di alto contenuto tecnologico (si pensi ad esempio ai droni). Il problema giuridico si pone non solo quando nasce una nuova tecnologia, ma anche quando ci troviamo di fronte a profonde trasformazioni di tecnologie già esistenti. In questo caso nasce l'esigenza di adattare un quadro normativo preesistente al continuo evolversi del progresso tecnologico.

Gli obiettivi concorrenti di proteggere i consumatori e più in generale gli utenti finali da effetti pregiudizievoli e promuovere contemporaneamente l'innovazione devono comunque diventare propri del legislatore. A questo proposito, **il sistema normativo più efficace deve combinare più strumenti: norme giuridiche, norme e standard tecnici, codici di condotta e *best practices***. In questo modo sarà possibile garantire la certezza, la flessibilità, la precisione e anche l'interpretazione più corretta di fronte a determinati dubbi.

Proprio per superare, almeno in parte, tali difficoltà, nel campo specifico della privacy **sarebbe opportuno affrontare e risolvere sin dall'inizio qualsiasi problematica nel rispetto del principio della *privacy by design***.

Tale principio richiede che la tutela dei diritti e delle libertà degli interessati, con riguardo al trattamento dei dati personali, comporti l'attuazione di adeguate misure tecniche e organizzative al momento sia della progettazione che dell'esecuzione del trattamento stesso, onde garantire il rispetto delle disposizioni del Regolamento UE 2016/679.

Al fine di garantire e dimostrare la conformità con il Regolamento, il titolare del trattamento deve adottare politiche interne e attuare misure adeguate, che soddisfino in particolare i principi della *privacy by design* e della *privacy by default*.

Il principio della *privacy by design* prevede che la protezione dei dati sia integrata nell'intero ciclo di vita della tecnologia, dalla primissima fase di progettazione fino alla sua ultima distribuzione, all'utilizzo e all'eliminazione finale.

Il principio della *privacy by default* prevede che le impostazioni di tutela della vita privata relative a servizi e prodotti rispettino i principi generali della protezione dei dati, quali la minimizzazione dei dati e la limitazione delle finalità.

In considerazione di tali principi, il Regolamento comunitario prevede che al momento di determinare le finalità e i mezzi del trattamento e all'atto del trattamento stesso, il titolare del trattamento, tenuto conto dell'evoluzione tecnica e dei costi di attuazione, deve mettere in atto adeguate misure e procedure tecniche e organizzative, in modo tale che il trattamento sia conforme al Regolamento e assicuri la tutela dei diritti dell'interessato**.** In particolare, se all'interessato

è lasciata facoltà di scelta relativamente al trattamento dei dati personali, il titolare del trattamento garantisce che siano trattati, di *default*, solo i dati personali necessari per ciascuna finalità specifica del trattamento e che, in particolare, la quantità dei dati raccolti e la durata della loro conservazione non vadano oltre il minimo necessario per le finalità perseguite. In particolare, detti meccanismi garantiscono che, di *default*, non siano resi accessibili dati personali a un numero indefinito di persone e che gli interessati siano in grado di controllare la distribuzione dei propri dati personali.

Anche gli incaricati del trattamento e i produttori devono attuare le misure e le procedure tecniche e operative adeguate per garantire che i loro servizi e prodotti consentano ai responsabili del trattamento, di *default*, di conformarsi al Regolamento.

La *privacy by design* può essere definita la nuova dimensione della privacy che trae le sue origini dall'innovazione tecnologica e dal progresso delle comunicazioni elettroniche.

L'evoluzione, quindi, tocca anche il settore della privacy rispetto alla tradizionale e primaria configurazione, con il riferimento alle PET (acronimo di *Privacy Enhancing Technologies*) che costituiscono le tecnologie utilizzate per migliorare il diritto alla privacy. Ovviamente tali tecnologie vengono considerate in maniera neutra, ovvero senza alcuna connessione con specifiche fattispecie. Tale espressione fu utilizzata per la prima volta nel report pubblicato nel 1995 dal titolo *Privacy-enhancing technologies: the path to anonymity*, della *Data Protection Authority* olandese in collaborazione con il Commissario dell'Ontario (Canada).

Il concetto di *privacy by design* trova spazio nella trilogia di applicazioni: 1) *IT systems*; 2) *accountable business practices*; 3) *physical design and infrastructure*. In sostanza:

1) **Tecnologia dell'informazione;**
2) **Pratiche commerciali responsabili;**
3) **Progettazione delle strutture.**

In particolare, con riferimento alla tecnologia dell'informazione si afferma, come già evidenziato, che la tecnologia non può costituire una minaccia per la privacy, ma un ausilio per la riduzione dei rischi. Per le pratiche commerciali responsabili, viene evidenziato come la privacy non va interpretata come un onere, un costo che appesantisce l'attività imprenditoriale ma, al contrario, come un vantaggio per una migliore competitività.

Infine, l'elemento della progettazione delle strutture assume rilevanza, poiché molto spesso siamo costretti a vedere esposti i dati personali in aree pubbliche mal progettate come, ad esempio, le sale d'attesa degli ospedali o degli uffici, ove è possibile che vengano – illecitamente – divulgate le informazioni personali.

Con questa nuova concezione della privacy si è così maggiormente diffusa l'esigenza di assicurare una forte tutela dei diritti e delle libertà delle persone, con particolare riferimento all'identità personale e alla vita privata degli individui che utilizzano le reti telematiche.

Tale tutela trova il suo fondamento nel principio di necessità consacrato dall'art. 3 del Codice per la protezione dei dati personali, ma questo principio va inteso in duplice senso. **Non solo necessità di ricorrere all'utilizzo del dato personale solo in casi estremi, ma necessità anche di strutturare i servizi che utilizzano nuove tecnologie in modo tale da garantire il rispetto della riservatezza degli utenti**. Insomma, finalmente si fa strada la necessità di concepire una "coscienza della privacy" da parte di tutti che possa prevenire, laddove sia possibile, successivi interventi sanzionatori delle Autorità preposte.

Il principio è recepito dall'art. 25 del Regolamento UE 2016/679, il quale sancisce che, tenuto conto dello stato dell'arte e dei costi di attuazione, nonché della natura, del campo di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi di varia probabilità e gravità per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare i principi di protezione dei dati, quali la minimizzazione, in modo efficace e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del Regolamento e tutelare i diritti degli interessati.

Lo stesso titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, di *default*, solo i dati personali necessari per ogni specifica finalità del trattamento; ciò vale per la quantità dei dati raccolti, l'estensione del trattamento, il periodo di conservazione e l'accessibilità. In particolare dette misure garantiscono che, di *default*, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.

La posizione dei Garanti europei sul *Data Protection Officer*

Enrico Pelino - *Grieco Pelino Avvocati*

Il Gruppo di lavoro *ex* art. 29, ossia l'organismo consultivo che raccoglie (tra l'altro) i Garanti europei, ha reso pubblico nel dicembre 2016 un primo gruppo di linee guida e di FAQ su tre importanti istituti del regolamento UE n. 2016/679 (Regolamento generale sulla protezione dei dati, in breve "RGPD") tra questi figura il *data protection officer*, o DPO (responsabile della protezione dei dati), cui sono dedicate le concise riflessioni che seguono.

Core activity (artt. 37.1.b), 37.1.c)) – Definire la *core activity* è essenziale ai fini dell'obbligo di designazione del DPO da parte di soggetti privati. Orbene, i Garanti europei, confermando i primi orientamenti dottrinali, non le identificano necessariamente nell'attività primaria del titolare o del responsabile di trattamento, è invece sufficiente che ne siano «parte inestricabile». Per chiarire meglio: attività tipica di una struttura sanitaria è la fornitura di prestazioni sanitarie, *core activity* è il trattamento dei dati sanitari dei pazienti, che non può essere disgiunto dalla prima.
Difficile per l'interprete sottrarsi alla suggestione di collegare idealmente il concetto di «parte inestricabile» (*inextricable part*) all'analoga espressione presente in CGUE, *Google Spain*, C-131/12, § 56 (*inextricably linked*).

Monitoraggio «regolare e sistematico» (art. 37.1.b)) – Altrettanto essenziale ai fini dell'obbligo di designare il DPO è che le *core activities* consistano (tra l'altro) in un monitoraggio regolare e sistematico degli interessati su larga scala. Ad avviso dei Garanti europei, è «regolare» il monitoraggio periodico e ripetuto, non occorre necessariamente che sia anche continuo. «Sistematico» va inteso nel senso di conforme a un piano o a un programma, dunque non casuale né estemporaneo.
Esempi proposti sono la fornitura di servizi di telefonia, la geolocalizzazione (come quella resa possibile da applicazioni per smartphone), i programmi fedeltà, la raccolta di dati sanitari attraverso apparecchi di *wellness* indossabili, la videosorveglianza.

«Su larga scala» (artt. 37.1.b), 37.1.c)) – Terzo elemento fondamentale per l'integrazione del precetto normativo è la sussistenza di un'attività (di monitoraggio o di trattamento di dati sensibili o giudiziari) su larga scala. Qui la soluzione è più lontana. Nelle linee guida si ammette l'esistenza di un'«area grigia» nella quale l'applicazione della categoria è controversa. Ciò solleva perplessità in termini di certezza del diritto, anche perché l'omessa designazione del DPO è sanzionabile (art. 83.4 a)).
Le poche sicurezze sono limitate alle indicazioni rintracciabili nel considerando 91: l'avvocato o il medico che trattano individualmente dati personali degli assistiti non lo fanno su larga scala. Può inferirsi, in linea generale, che altrettanto valga per qualsiasi altro professionista. È una base, ma non è neppure lontanamente sufficiente a scolpire il concetto. I Garanti aggiungono, quasi incidentalmente, a questa zona franca anche il trattamento svolto da una piccola impresa familiare (cfr. § 2.2 linee guida). Più controverso invece il caso della media impresa.
Il riferimento alle dimensioni societarie sembrerebbe promettente per l'interprete. La nozione di PMI è infatti normata a livello europeo con riferimento a specifici parametri dimensionali, cfr. raccomandazione n. 2003/361/CE.
Ugualmente, la nozione di impresa familiare (a prescindere dalle dimensioni) è stata messa a punto dall'Expert Group on Family Business nel rapporto finale 2009.
La tentazione di collegarsi ai parametri dimensionali rinvenibili in fonti europee extra-privacy non trova tuttavia espresso conforto nelle linee guida, che anzi enunciano parametri del tutto diversi, riferiti piuttosto all'attività di trattamento, non alla massa economica e organizzativa del soggetto che vi procede, ossia: numero degli interessati coinvolti dal trattamento; volume dei dati personali trattati e/o ampiezza della loro tipologia; durata del trattamento; contesto geografico di quest'ultimo.
Tra gli esempi di trattamento su larga scala figurano quelli di un ospedale (privato), di un'assicurazione o una banca, di un servizio di trasporto pubblico su abbonamento, di fornitori di telefonia o di servizi Internet.
Ci si potrebbe domandare se una grande farmacia, un'associazione tra professionisti o uno studio medico particolarmente strutturati possano rientrare concettualmente nell'alveo della nozione di «larga scala».

Esclusione di automatismi nella designazione del DPO
L'obbligo di designazione del DPO non si trasmette automaticamente dal titolare del trattamento al responsabile e viceversa. È un chiarimento utile: se cioè il titolare del trattamento deve per legge dotarsi di un DPO, ciò non produce effetto a catena sul responsabile.

Estesi obblighi di documentazione – Il Regolamento dà

ampio spazio ai profili documentali e organizzativi. Non vi sfugge certamente la figura del DPO. Gli obblighi di documentazione sono estesi e riguardano:

- innanzitutto la stessa scelta di designare/non designare il DPO. Come emerge infatti dai rilievi appena svolti, non è sempre auto-evidente la sussistenza dell'obbligo di designazione. In caso negativo, si impone lo svolgimento di un'analisi preliminare, da conservare per consultazione e verifica, riportando i fattori considerati e la loro ponderazione.
  Quanto rilevato riguarda naturalmente il settore privato. Ad avviso di chi scrive, non può tuttavia escludersi l'opportunità di provvedere all'analisi preliminare (e di documentarla) anche in ambito pubblico, rispetto alla decisione di una pubblica amministrazione di dotarsi di un proprio DPO oppure di fruirne in condivisione con altre amministrazioni, cfr. art. 37.3. L'esigenza di condivisione va naturalmente inserita all'interno di scelte organizzative più ampie e dipende anche da considerazioni economiche, tuttavia non può prescindere dalle peculiarità del singolo caso e dall'attenzione a profili funzionali.
- La scelta di distaccarsi dal parere del DPO. Ciò vale sia in generale sia, più specificamente, a proposito della valutazione di impatto (*DPIA, data protection impact assessment*): il dissenso rispetto alla posizione del DPO deve lasciare traccia. Ad opinione di chi scrive, sono qui prevedibili resistenze e conflitti né può escludersi il condizionamento dovuto a rapporti di forza e dinamiche organizzative (soprattutto nel caso di DPO interno).
- I pareri del DPO. Lo si deduce logicamente da quanto appena detto: se della posizione del DPO bisogna tenere espressamente conto, essa andrà documentata.
- Operazioni riportate nei registri di trattamento. La tenuta dei registri, prescritta dagli artt. 30.1 e 30.2, è di competenza del titolare o del responsabile del trattamento. Osservano tuttavia i Garanti europei che nella prassi applicativa potrà ben essere richiesta al DPO (né ciò sarà illegittimo) la gestione degli aspetti operativi di tali attività, senza ovviamente che ciò muti l'attribuzione e la responsabilità previste per legge.

Coinvolgimento nella struttura del titolare o del responsabile di trattamento – Il coinvolgimento del DPO nella struttura che svolge il trattamento deve essere pervasivo. Questo è uno degli aspetti più delicati dell'intero istituto: tendenzialmente il DPO, attraverso la conoscenza dei flussi di dati personali, acquisisce una visione profonda e dettagliata dell'intera attività e dei progetti di un'azienda, di un gruppo di aziende, di una pubblica amministrazione o perfino di più pubbliche amministrazioni. È un punto di osservazione privilegiato e strategico, ovviamente presidiato da segreto. Del resto, la stessa natura dei compiti che il Regolamento impone al DPO rende imprescindibile questo assetto.
I Garanti europei sono molto precisi sul punto e mettono in chiaro che il DPO:

- va coinvolto fin dall'inizio in ogni questione concernente il trattamento di dati personali (dunque pressoché in tutte);
- deve essere invitato a partecipare regolarmente alle riunioni con ruoli manageriali di medio e alto livello;
- deve essere coinvolto tempestivamente nel caso di incidenti che determinino violazione dei dati (data breach).

Dotazione di risorse – La pervasività del ruolo del DPO sarebbe vanificata dalla mancanza di risorse, che devono perciò essere adeguate. Il Gruppo di lavoro sottolinea che va garantita al DPO:

- disponibilità di strumenti finanziari, umani, fisici e operativi, formativi e conoscitivi;
- accesso e relazione con altri settori organizzativi (risorse umane, IT, ufficio legale, management, ecc.);
- disponibilità di tempo adeguato ai compiti richiesti.

Ruolo essenziale nella valutazione d'impatto (DPIA) – Il DPO svolge un ruolo chiave in materia di valutazione d'impatto. In proposito, i Garanti europei non aggiungono particolari novità al quadro desumibile dall'articolato regolamentare. Tuttavia, giovano le seguenti precisazioni:

- il DPO deve innanzitutto valutare se occorra o no procedere alla DPIA;
- quale metodologia seguire;
- se la DPIA vada effettuata all'interno o esternalizzata;
- quali misure di sicurezza porre in essere per ridurre i rischi per gli interessati di trattamento.

Inoltre il DPO deve effettuare una valutazione finale sulla correttezza della DPIA svolta e sulla sua coerenza con il Regolamento.

In conclusione, va notato che le linee guida registreranno un ulteriore affinamento entro il mese di aprile 2017, recependo commenti e osservazioni pervenute alla data del 15 febbraio 2017. Dunque potrebbero prodursi nell'immediato futuro alcuni scostamenti rispetto al testo commentato, fatto comunque salvo il suo nucleo centrale.

LAND

Firmiamo da sempre, non eravamo ancora maggiorenni
e già firmavamo digitalmente in Cloud
per circa 200 milioni di volte l'anno.

ORA CHE NE ABBIAMO 24 VI FAREMO DIVERTIRE...

SIGN DIFFERENT
HAPPY SIGN

L'applicazione di verifica mobile raddoppia ed aumentano le funzionalità:

HONOS

Verifica documenti
Verifica Firma
FEA Glifometrica

HAPPY SIGN

Verifica documenti
Verifica Firma
FEA Glifometrica
Firma Digitale Remota
Firma Digitale Glifometrica
Libro Firma
Archivio Documenti Firmati
Notifiche in tempo reale
dello stato dei documenti

LAND S.r.l.
Via di Affogalasino, 40
00148 ROMA
info@land.it - www.land.it

Know IT è la piattaforma di formazione e informazione dedicata ai professionisti dell'era digitale. Il percorso di digitalizzazione, anche se a piccoli passi, sta rivoluzionando gli scenari di mercato, aprendo nuove prospettive e nuove criticità per la privacy, il commercio elettronico, il diritto d'autore e la conversione in digitale di processi prima analogici, come la fatturazione, la gestione documentale, la firma. Tutto ciò avrà un impatto sempre maggiore su molti aspetti organizzativi, coinvolgendo PA, aziende, professionisti e cittadini.

Know IT si propone di diffondere una conoscenza digitale che si allarghi dall'area prettamente tecnica a quella normativa e gestionale, implementando la capacità degli utenti di valutare e condurre i nuovi processi e modelli organizzativi, ottimizzandoli e fornendo valore aggiunto al contesto in cui si trovano a operare.

Il nostro programma formativo affronta in particolare le seguenti macrotematiche: e-commerce, diritto d'autore, privacy e sicurezza, firme elettroniche e biometria, e-government, e-health, document management e, in generale, tutti i principali aspetti dell'ICT law.

Corsi on demand dedicati a PA, aziende e professionisti

SCOPRI L'OFFERTA FORMATIVA

www.knowit.clioedu.it

Digital & Law Department
www.studiolegalelisi.it

CLIOEDU®