

## 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](#)<sup>1</sup>.

Nell’articolo immediatamente successivo della stessa Carta viene riconosciuto con altrettanta importanza e pienezza **il diritto alla protezione dei dati personali**<sup>2</sup>, 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<sup>3</sup>), 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 temperato 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 pa-

reti 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<sup>4</sup>, fossero già presenti in uno stato embrionale nell'art. 3 del Codice della protezione dei dati<sup>5</sup>. 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'*accountability***, 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<sup>6</sup> 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 presidi 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<sup>7</sup> 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