

# Privacy 4.0 al via, tra vecchi e nuovi adempimenti per aziende e professionisti

*Giovanni Ziccardi - Professore Associato di Informatica Giuridica presso la facoltà di Giurisprudenza dell'Università degli Studi di Milano*

Con il Regolamento Europeo per la Protezione dei Dati (GDPR) si delinea un nuovo quadro di adempimenti per aziende e professionisti, più adatto ad un'era in cui il dato personale digitale viaggia oltre i confini territoriali e, con estrema facilità, sulle piattaforme di social network e nel cloud. Molti adempimenti non sono nuovi, ma "ereditati" dal Codice Privacy. E' il caso, ad esempio, dell'informativa e del consenso. Rivoluzionato invece il sistema delle misure di sicurezza ed introdotto, infine, una nuova e importante figura aziendale: il Data Protection Officer (DPO). Con quali funzioni?

Il Regolamento Europeo per la Protezione dei Dati (**GDPR**), già in vigore dal maggio del 2016 e che sarà presto attuato (il 25 maggio 2018) in tutti i Paesi dell'Unione Europea, prevede, nel testo dei suoi 99 articoli, numerosi **adempimenti** di diversa entità che necessitano, in un'ottica di adeguamento normativo, di una riflessione sistematica e di una programmazione accurata sul da farsi nelle prossime settimane.

Molti adempimenti non sono nuovi, ma sono "ereditati" dal Codice Privacy in vigore (D. Lgs. n. 196/03) e, addirittura, erano già previsti nella Direttiva 96/45 che ha originato, più di vent'anni fa, l'attuale quadro di protezione dei dati.

Le **realità aziendali** e gli **enti pubblici** che nei decenni appena trascorsi avevano fatto un lavoro serio di adeguamento normativo, non soffriranno troppo nel passaggio a un nuovo regime che è, comunque, profondamente radicato nel passato, pur mantenendo un volto ben rivolto al futuro e all'era dei social network, della profilazione automatizzata, del cloud e delle reti.

## Informativa e consenso nell'era delle nuove tecnologie

L'informativa e il consenso sono i due adempimenti "tradizionali" che sono rimasti al centro del sistema e che necessiteranno di un "lifting" per adeguarli ai cambiamenti tecnologici dell'era moderna.

Dovranno, sempre di più, **essere chiari**, informare e rendere trasparente l'intero processo di trattamento dei dati anche online, dove è estremamente difficoltoso sia chiarire con precisione tutti gli aspetti del trattamento sia tenere traccia delle manifestazioni di volontà quando il consenso è dato con un click o selezionando un menù a tendina.

Il timore del legislatore è quello che non si possa più assicurare un "**tracking**" **preciso del dato**, una rilevazione costante del percorso che le informazioni fanno in una società sempre più informatizzata: da dove sono raccolte, a chi sono vendute, che tragitti percorrono, dove sono conservate e se e quando "moriranno" o se rimarranno negli archivi e nei database in eterno.

## Diritti dell'interessato

Anche i diritti che l'interessato (la persona fisica cui si riferiscono i dati) può esercitare nei confronti di chi tratta i suoi dati si sono potenziati, e cercano di permettere a ogni persona di controllare – meglio, "governare" – il proprio dato.

Accanto a **diritti di accesso, rettifica e integrazione** sono apparsi i nuovi, e interessanti, diritti alla **portabilità dei dati** (l'utente potrà portarsi con sé le informazioni se cambierà servizio o piattaforma) e all'oblio (con aumentate possibilità di cancellazione delle informazioni), che richiederanno una maggior attenzione (e capacità di reazione) in capo ai titolari che trattano dati.

## Misure di sicurezza

L'intero sistema delle misure di sicurezza è stato rivoluzionato. L'abbandono delle misure minime di sicurezza (che erano elencate con cura) ha portato a un "vuoto" dove è colui che tratta i dati a dover analizzare il rischio per i dati che processa, a elaborare un piano di sicurezza, a metterlo in opera e a doverlo in ogni momento dimostrare e renderlo verificabile. Si tratta di un approccio alla sicurezza dei dati basato sull'**idea di "accountability"**, una strategia già nota in ambito di information security e di certificazioni.

## Nuove figure aziendali

Sarà un nuovo soggetto, il **Data Protection Officer (DPO)**, a fare da "sceriffo" all'interno di molte grandi realtà che trattano i dati per garantire l'applicazione di tutte le disposizioni del Regolamento, per dialogare con il Garante in caso di problemi e per fare da punto di contatto con gli interessati. La nomina di un DPO, insieme alla tenuta di un **registro dei trattamenti** aggiornato e a una corretta gestione di eventuali data breach (esfiltrazioni di dati dall'archivio dell'azienda) sono considerati da molti come **i primi tre adempimenti più urgenti** da mettere in opera per garantire un buon approccio alla nuova idea di sicurezza.

## Regime sanzionatorio

Le sanzioni previste sono **tra le più alte** mai stabilite in una normativa privacy: non solo sanzioni "fisse" (fino a 20 milioni di euro) ma anche sanzioni stabilite in percentuale con riferimento al fatturato mondiale annuo dell'azienda (fino al 4%). Queste nuove sanzioni, così elevate, hanno causato una corsa alla compliance che nelle settimane prima del 25 maggio 2018 risulterà ancora più evidente.

## Considerazioni e prospettive per le aziende

Il Regolamento dovrebbe portare **maggiore uniformità normativa** nei Paesi dell'Unione Europea – consentendo anche, a volte, di dialogare con le autorità di altri Paesi – anche se sono già stati annunciati provvedimenti normativi, in Italia, che cercheranno di disciplinare la transizione da un quadro legislativo ventennale a un nuovo approccio per molti versi differente.

L'idea di fondo è che il **nuovo quadro di adempimenti** sia più adatto per affrontare un'era dove il dato personale digitale viaggia oltre i confini con estrema facilità, sulle piattaforme di **social network** e nel **cloud**, o che è "addosso" alla persona fisica, negli smartphone, nei braccialetti fitness, nell'Internet delle Cose. Un dato che può facilmente profilare l'individuo non solo con riferimento alle sue preferenze commerciali e d'acquisto ma, anche, monitorando le sue performance sul lavoro o il suo stato di salute. Particolare attenzione è dedicata ai **minori di 16 anni**, che sono utenti dei servizi della società dell'informazione già dalla giovane età e che il Regolamento vuole proteggere con una specifica cura.

E questo, per la prima volta, è fatto tramite un Regolamento che dalla "piccola" Europa si presenta come una norma con un'influenza, e un'applicazione, che tocca tutto il mondo, **tutte le aziende** anche non europee o senza sede in Europa che, comunque, trattano dati di europei o offrono servizi a consumatori del Vecchio Continente.

Gli adempimenti sono di diversa complessità: alcuni puntano essenzialmente a tenere traccia di fatti (registro e mappatura dei trattamenti, studi preliminari per valutare l'impatto dei trattamenti, istruzioni pensate per chi tratta i dati e piani di formazione), altri richiedono invece un **nuovo approccio organizzativo** (la nomina del DPO, la creazione di un punto di ricezione per l'esercizio dei diritti, la gestione corretta di un data breach).

Diventerà essenziale, in ogni momento, sapersi orientare in questa **mappa di adempimenti** adeguando sempre le misure di sicurezza al rischio concreto che si presenta in ogni singola situazione, con una costante attenzione ai costi ma anche allo stato dell'arte e alle migliori tecnologie disponibili. Si vedrà, in questo senso, che l'utilizzo della **crittografia**, del mascheramento dei dati e dei database e di una pseudonimizzazione accorta delle informazioni potrà fare la differenza.