Cristina Vicarelli
Avvocato

La piattaforma ODR: un caso di privacy by design

Ho già parlato della piattaforma ODR e degli obblighi connessi, ora è entrata in funzione ed è già possibile, per consumatori e commercianti (per seguire la terminologia presente sulla piattaforma stessa) presentare una richiesta volta al componimento stragiudiziale di una controversia insorta a seguito di un acquisto operato on line. La procedura è piuttosto semplice, e la presentazione dell'istanza è assistita da un breve percorso a domande e risposte, che ne rende agevole il completamento.

Il funzionamento della piattaforma è stato quasi integralmente disciplinato dal Regolamento 524/2013. Stavolta vorrei soffermarmi su una annotazione che ho tralasciato nel precedente post, per non sovraccaricarlo di informazioni che potevano apparire marginali.

L'Articolo 5 del Regolamento ora citato ("Istituzione della piattaforma ODR") prevede:

"1. La Commissione sviluppa la piattaforma ODR ed è responsabile per quanto riguarda il suo funzionamento, comprese tutte le funzioni di traduzione necessarie ai fini del presente regolamento, la sua manutenzione, il suo finanziamento e la sicurezza dei dati. La piattaforma ODR è di facile impiego. Lo sviluppo, il funzionamento e la manutenzione della piattaforma ODR assicurano, nei limiti del possibile, la tutela della vita privata fin dalla fase di progettazione («privacy by design») e l'accessibilità e l'utilizzabilità della piattaforma stessa da parte di tutti, comprese le persone vulnerabili («design for all» – progettazione universale). (…)."

Privacy by design: cos'è?

Quello della Privacy by design è un principio introdotto nell'emanando Regolamento Generale sulla Protezione dei Dati, in ragione del fatto che, per garantire il rispetto delle disposizioni del Regolamento stesso, poste a tutela dei diritti e delle libertà delle persone fisiche con riguardo al trattamento dei dati personali, è necessario adottare misure tecniche ed organizzative adeguate. Al fine di poter dimostrare la conformità con il Regolamento, si è ritenuto opportuno obbligare il

Titolare del trattamento ad adottare politiche interne e ad attuare misure che soddisfino in particolare i principi della protezione dei dati fin dalla progettazione (privacy by design), e, per rafforzare la tutela, tali obblighi sono stati connessi al dovere di configurare la protezione dei dati come impostazione predefinita (privacy by default). Tali misure potrebbero consistere, tra l'altro, nel ridurre al minimo il trattamento dei dati personali, pseudonimizzare i dati personali il più presto possibile, offrire trasparenza per quanto riguarda le funzioni e il trattamento di dati personali, consentire all'interessato di controllare il trattamento dei dati e consentire al Titolare del trattamento di creare e migliorare le caratteristiche di sicurezza. In fase di sviluppo, progettazione, selezione e utilizzo di applicazioni, servizi e prodotti basati sul trattamento di dati personali o che trattano dati personali per svolgere le loro funzioni, i produttori dei prodotti, dei servizi e delle applicazioni dovrebbero essere incoraggiati a tenere conto del diritto alla protezione dei dati allorché sviluppano e progettano tali prodotti, servizi e applicazioni e, tenuto debito conto dello stato dell'arte, a far sì che i Titolari del trattamento e i Responsabili del trattamento possano adempiere ai loro obblighi di protezione dei dati.I principi della protezione dei dati fin dalla progettazione e di default dovrebbero essere presi in considerazione anche nell'ambito degli appalti pubblici (cfr considerando 61). La norma che canonizza tali obblighi è l'art. 23 del Regolamento (secondo la numerazione seguita nella Proposta) "Articolo 23 – Protezione dei dati fin dalla progettazione e protezione di default

"1. 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 responsabile 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 presente regolamento e tutelare i diritti degli interessati.

2. Il responsabile 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.

2 bis. Un meccanismo di certificazione approvato ai sensi dell'articolo 39 può essere utilizzato come elemento per dimostrare la conformità ai requisiti di cui ai paragrafi 1 e 2."

La genesi

L'idea di informare l'ICT con misure di tutela della privacy, non è del tutto nuova. Nella Direttiva 95/46/CE è possibile rinvenire alcune previsioni che obbligano i Titolari dei dati a implementare cautele nella progettazione e messa in opera dell'ICT: l'art. 17, ad esempio, obbliga il Titolare ad "attuare misure tecniche ed organizzative appropriate", che il considerando 46 pone "sia al **momento** della progettazione che a quello dell'esecuzione del trattamento", mentre l'articolo 16 della Direttiva stabilisce l'obbligo di riservatezza dei trattamenti, riservatezza speculare a quella che presiede alla regolamentazione della sicurezza IT. Oltre ciò rilevano anche i principi sanciti all'art. 6 della Direttiva (liceità, finalità, pertinenza e non eccedenza, ecc.).

Il quadro normativo ora delineato, però, se collocato in ambito ICT, non garantisce che la tutela dei dati personali sia tenuta in conto sin dalla progettazione: soprattuto se si osserva la sproporzione che spesso contraddistingue la posizione contrattuale degli utenti e dei fornitori dei servizi ICT, si comprende come gli utenti siano impossibilitati ad adottare, da soli, le misure che sarebbero necessarie anche solo a proteggere i loro propri dati personali. Invece, dovrebbero poter usufruire di strumenti che garantiscano la tutela già di default.

Sulla scorta di tali considerazioni il WP29, (cfr WP168) ha ritenuto che fosse opportuno introdurre nel nuovo quadro normativo previsioni che traducessero tutti questi requisiti in un più ampio principio, quello, appunto della privacy by design, un principio che avrebbe dovuto essere vincolante per coloro che progettano e producono tecnologie, tanto quanto per i Titolari ai quali spetta la scelta sulla soluzione tecnologica da acquistare o adottare. Essi avrebbero dovuto essere obbligati a tener conto della protezione dei dati offerta dalla tecnologia sin dal momento della pianificazione delle procedure e dei sistemi. E sia i fornitori che i Titolari avrebbero dovuto dimostrare di aver adottato tutte le misure necessarie a garantire la rispondenza a questi requisiti.

Secondo il WP 29 una corretta implementazione di privacy by design e privacy by default avrebbe dovuto aver riguardo non solo del trattamento dei dati in sé e per sé considerato ma avrebbe dovuto portare alla progettazione di sistemi che evitassero di trattare dati personali se non necessario o, comunque, minimizzassero i trattamenti.

L'attuazione dei principi di Privacy by Design e by Default avrebbe rappresentato uno strumento indispensabile per consentire agli utenti di proteggere meglio i propri dati, e avrebbe dato alle DPA uno strumento in più per applicare in concreto la protezione dei dati personali.

A ben guardare, se si confronta con la normativa nazionale, si tratta anche di una rivisitazione e riattualizzazione del principio di necessità, fissato dall'art. 3 del Codice della Privacy.

Conclusione

Sebbene le indicazioni emerse nel corso degli anni siano state accolte dal testo licenziato dal trilogo e canonizzate all'art. 23 della Proposta di Regolamento (che ormai si trova in una fase molto avanzata del suo iter di approvazione), il Regolamento Generale sulla Protezione dei Dati non è ancora in vigore. il Regolamento su ODR, quindi, in ordine alla privacy by design, anticipa quello sulla protezione dei dati, con una prescrizione espressa, che si coordina con quadro normativo che verrà.

Trattandosi di una delle prime applicazioni in materia, sarebbe stato interessante se la Commissione avesse pubblicato un qualche tipo di report per spiegare come ha attuato la progettazione rispettosa della privacy. Alcuni elementi possono infatti essere tratti dall'informativa, come il tempo di conservazione semestrale, ma sarebbe stato utile sondare altri aspetti, magari più tecnici, in modo da trarne spunto.