I Garanti della protezione dei dati personali hanno anche un ruolo di indirizzo dello sviluppo digitale?

Augusta Iannini
Vicepresidente Autorità Garante per la protezione dei dati personali

Le prime applicazioni concrete del Regolamento UE 2016/679 pongono intriganti interrogativi rispetto alla disposizione che obbliga i titolari del trattamento ad attuare il principio di protezione dei dati fin dalla progettazione e la protezione dei dati per impostazione predefinita, comprensivi entrambi anche della "security by design and default".

Nel parere n. 5/2018 il GEPD[1] ha distinto tra il "privacy by design", emblema di una dimensione visionaria ed etica, e quello propriamente giuridico, inteso come "data protection by design e data protection by default" nel quale il "by design" riguarda quell'approccio proattivo che parte dalla fase della progettazione sino a tutto il ciclo di vita dei dati trattati, senza dirimerne la funzionalità, mentre il "privacy by default" può essere semplicemente declinato nel senso che il singolo non deve esplicare alcuna azione per proteggere la propria vita privata perché questa protezione è integrata nel sistema, per impostazione predefinita, in modo automatico.

Poste queste nozioni di base, nella valutazione della conformità al GDPR di

[1] European Data Protection Supervisor, Opinion 5/2018, Preliminary Opinion on privacy by design, https://edps.europa.eu/sites/edp/files/publication/18-05 31_preliminary_opinion_on_privacy_by_design_en_0.pdf

sistemi che utilizzano dati personali per fornire servizi, sono emerse numerosi rilevanti questioni, tuttora irrisolte.

In particolare, con tre provvedimenti del 2018[2], il Garante ha impartito una serie di prescrizioni ad un fornitore di servizi di geolocalizzazione, nominato dai titolari, in entrambi i casi, responsabile del trattamento che è risultato essere anche produttore dei dispositivi interessati.

Tra le prescrizioni imposte, il Garante, sul presupposto che "*la versione standard dei servizi forniti... comporta trattamenti di dati personali relativi alla posizione geografica accentuatamente dettagliata (anche per la periodizzazione temporale assai ravvicinata: 30, 60 o 120 secondi)...*", ha ingiunto al fornitore, ai sensi dell'articolo 58, paragrafo 2, lettera d) del Regolamento (UE) 2016/679, non solo di informare i propri clienti della possibilità di modificare il sistema rispetto all'impostazione standard ma – ed è l'aspetto più problematico – in base ai principi di minimizzazione dei dati e di rispetto dei parametri di *privacy by design e by default* espressamente richiamati dall'articolo 5, paragrafo 1, lettera c) e dall'articolo 25 del Regolamento (UE) 2016/679, di configurare la versione "standard" con modalità proporzionate rispetto al diritto di riservatezza degli interessati, in particolare proprio con riferimento alla periodizzazione temporale della rilevazione geografica.

Le altre prescrizioni imposte dal Garante sono state onorate dai titolari ma rispetto all'indicazione relativa alla modifica dell'impostazione standard del sistema sono insorte una serie di problematiche, la più rilevante delle quali riguarda il pregiudizio irreparabile che la società, responsabile del trattamento su indicazione dei titolari ma anche produttrice del sistema, incontrerebbe sul mercato, offrendo un prodotto privo della capacità di rilevare i dati di geolocalizzazione con quell'accuratezza medio-alta richiesta dai clienti ed offerta da altre imprese concorrenti non colpite, per ora, dalle prescrizioni del Garante.

In sintesi: nessuna difficoltà ad offrire ai clienti titolari dei trattamenti la possibilità di modulare i servizi secondo la giurisprudenza del Garante, ma indisponibilità a ridurre la potenzialità del proprio prodotto, per non uscire dal mercato.

Dunque il quesito che si pone, in linea generale, per la geolocalizzazione ma anche per altri servizi è se l'Autorità possa e, in caso affermativo, con quali provvedimenti, intervenire nella valutazione del rispetto dei principi *di privacy by design e/o by default*, e – soprattutto – nei confronti di quali soggetti.

[2] https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9023246; https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9039945; https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9084531&zx=z5bh4d4zwy0

Uno dei cardini del nuovo Regolamento europeo e dei contenuti del principio di "*accountability*" che grava sul titolare e, in certi casi, sul responsabile del trattamento, è il rispetto dei principi di *privacy by design e by default*, sinteticamente definiti come la necessità che qualunque sistema tratti dati personali deve, sin dall'origine, essere impostato in modo da rispettare i consolidati principi di proporzionalità, minimizzazione, etc.

Dunque non vi è dubbio che il titolare e il responsabile che utilizzano, nel nostro caso, un sistema di geolocalizzazione devono impiegare quel prodotto secondo le indicazioni contenute nella giurisprudenza del Garante.

Ma il produttore di un sistema che ne disegna le potenzialità secondo le regole del mercato, che ambisce a collocarlo in Paesi dalle tradizioni più diverse rispetto alla normativa sulla tutela dei dati personali e che nel momento in cui lo progetta non riveste né il ruolo di titolare né quello di responsabile, deve preoccuparsi che la versione "standard" risponda alle regole contenute nel nuovo Regolamento europeo?

La risposta, in una logica di mercato, sarebbe intuitiva ma le norme sulla tutela dei dati personali non depongono per un'interpretazione così scontata.

L'articolo 25 del Regolamento (UE) 2016/679, al primo comma, impone al titolare, al momento di determinare i mezzi del trattamento e all'atto del trattamento, di adottare misure tecniche e organizzative adeguate, quali (ma non solo) pseudonimizzazione e minimizzazione.

Alla valutazione di adeguatezza non sono estranei anche i parametri dello stato dell'arte, dei costi di attuazione, della natura, dell'ambito di applicazione, del contesto e della finalità del trattamento, pur dovendosi il giudizio finale relazionare comunque con la valutazione dei rischi per i diritti e le libertà delle persone fisiche. E in questa complessa operazione, il titolare del trattamento può essere supportato dalle indicazioni rinvenibili dalle migliori prassi, da codici di condotta approvati, da certificazioni, da linee guida offerte dal comitato o da suggerimenti forniti dal Responsabile della Protezione Dati. Ma la questione non può dirsi definita solo con queste indicazioni perché al secondo comma dell'articolo 25, nella prima parte, il Regolamento impone che le misure tecniche ed organizzative per essere ritenute "adeguate" devono garantire, "per impostazione predefinita", solo il trattamento dei dati personali necessari per ogni finalità. Qui la novità sta nell'espressione "per impostazione predefinita", che viene descritta nel considerando 78 come un onere del titolare fin dalla progettazione di un sistema di raccolta dati. Tanto che, subito dopo la parte del "considerando" dedicata agli obblighi del titolare, si specifica che "*in fase di sviluppo, progettazione, selezione ed utilizzo di applicazioni, servizi e prodotti basati sul trattamento di dati personali o che trattano dati personali, i produttori dei*

prodotti, dei servizi e delle applicazioni dovrebbero essere incoraggiati a tener conto del diritto alla protezione dei dati allorché sviluppano e progettano tali prodotti, servizi ed applicazioni e, tenuto debito conto dello stato dell'arte, a far sì che i titolari ed i responsabili del trattamento possano adempiere ai loro obblighi di protezione dati".

Dunque nei confronti dei produttori, il Regolamento sembra limitarsi ad una specie di "*moral suasion*". Tuttavia, se un produttore costruisce un sistema non "compliant" rispetto alla tutela dei dati personali, potrebbe non avere mercato, almeno all'interno dell'Unione europea, per l'impossibilità dei titolari di rispettare gli obblighi contenuti nell'articolo 25 GDPR. E questo approccio è confermato dalla nostra normativa nazionale di adeguamento, introdotta con il decreto legislativo 10 agosto 2018 n. 101.

Il Regolamento UE 2016/679, all'articolo 58, ha descritto il potere delle Autorità nazionali. In particolare, al comma 2 del medesimo articolo 58, alla lettera d), ha conferito ai Garanti il potere di ingiungere al titolare del trattamento o al responsabile di conformare i trattamenti alle disposizioni del regolamento, se del caso, in una "determinata maniera...", ovvero con indicazioni specifiche.

Inoltre, il comma 6 dell'articolo 58 ha conferito agli Stati Membri la facoltà di accrescere i poteri delle Autorità previsti nei paragrafi 1, 2 e 3 del medesimo articolo. E il legislatore nazionale non si è lasciato sfuggire l'occasione. Infatti all'articolo 154 bis del Codice Privacy, introdotto dal decreto legislativo 10 agosto 2018 n. 101, al comma 1, ha chiarito che, in applicazione proprio della facoltà concessa dal Regolamento, il Garante può adottare linee guida di indirizzo riguardanti le misure organizzative e le tecniche di attuazione dei principi del GDPR, anche per singoli settori e in applicazione dei principi di cui all'articolo 25 del Regolamento, ovvero, del *privacy by design* e *privacy by default*, con tutti i conseguenti corollari richiamati nei considerando 77 e 78.

Dunque le linee guida certamente conterranno e costituiranno veri e propri obblighi per i titolari e per i responsabili del trattamento ma anche suggerimenti persuasivi per i produttori su come impostare i sistemi che trattano dati personali, secondo le indicazioni del considerando 78. Ma se questi produttori fornissero anche i servizi relativi al trattamento per conto del titolare, assumendo il ruolo formale di responsabili, le linee guida del Garante si applicherebbero anche ai sistemi da loro prodotti (in virtù del ruolo successivamente assunto) e quindi anche alle "impostazioni standard" di un sistema progettato in via astratta per una serie infinita di situazioni, di finalità, di opportunità?

Dunque, mi pare fondamentale che alcuni concetti frettolosamente declinati

con formule di stile siano esaminati con estrema attenzione per elaborare riflessioni sul ruolo delle Autorità Garanti, e in particolare sulle conseguenze che un'interpretazione della normativa europea e nazionale, come quella sopra descritta, potrebbe comportare.

In estrema sintesi il legislatore ha inteso disegnare per le Autorità di protezione dati, quando valutano la conformità di un trattamento ai principi indicati nell'articolo 25 GDPR, anche un ruolo di programmatore e decisore delle modalità di sviluppo dell'economia digitale?