Data protection by design e by default

Il Regolamento UE 2016/679 in materia di protezione dei dati personali ha introdotto alcune innovazioni significative e, più in particolare, il concetto di responsabilizzazione o *accountability*, che pone il titolare del trattamento nella condizione di dover dimostrare, tra l'altro, nell'ambito del trattamento dei dati personali, l'adozione delle misure di sicurezza descritte nell'art. 5, paragrafo 1 lettera f) e contestualmente anche di comprovare il rispetto delle prescrizioni contenute nell'art. 5 paragrafo 2 del Regolamento[1]. In particolare la *ratio* sottesa all'introduzione del concetto di *accountability* viene rinvenuta nella necessità di permettere il passaggio dalla teoria dei principi di protezione dei dati alla loro messa in pratica, cosi da tradurre gli obblighi giuridici in misure di protezione dei dati verificabili nei fatti e non solo sulla carta[2]. Ciò premesso, occorre ora individuare il collegamento che intercorre tra il concetto di sicurezza (sotto il profilo tecnologico, giuridico e organizzativo) e quello di adeguatezza delle misure tecniche organizzative ma non prima di aver precisato che la finalità delle adeguate misure tecniche organizzative deve essere individuata nelle protezione dei diritti e delle libertà fondamentali delle persone fisiche mediante la prevenzione delle violazioni dei dati personali degli interessati.

Con il nuovo Regolamento il concetto di misura di sicurezza, complice anche il rafforzamento del concetto di "rischio del trattamento", assume un confine più ampio, infatti, viene meno la classificazione delle misure di sicurezza in "misure minime di sicurezza" e "misure idonee di sicurezza" e, in luogo di quest'ultime, si affermano le "misure di sicurezza adeguate" che devono essere individuate per ciascun trattamento dal

Titolare solo dopo una specifica analisi del rischio ad esso associato. In tale ambito emergono e sono precisati i doveri attribuiti al titolare dagli artt. 24 e 25 del Regolamento quali ad esempio la valutazione del rischio oltre che alla privacy by design e privacy by default.

Sul punto, e per completezza, corre precisare che nel Regolamento sono previste, a presidio delle prescrizioni illustrate, ma non solo, rilevanti e differenziate sanzioni amministrative, in ragione del livello di gravità delle violazioni, come meglio precisato negli artt. 83 e 84 del Regolamento, ai quali comunque si rinvia. Sono in ogni caso fatte salve anche specifiche sanzioni penali e civili ove previste.

Il legame tra il concetto di *accountability* e l'obbligo di dover documentare e comprovare l'adeguatezza delle misure tecniche organizzative assunte, e cioè comprovare che le misure assunte ex ante saranno valide ex post previo riesame ed aggiornamento, se necessario si manifesta con l'istituzione e implementazione del registro delle attività dei trattamenti. Le richiamate misure una volta annotate nel predetto registro saranno "cristallizzate" e utili a dimostrare, in caso di necessità, la conformità dei trattamento al Regolamento.

L'innovazione che ha coinvolto l'applicazione dei principi consiste nella loro valutazione ai fini della responsabilità da attribuire al titolare del trattamento e, pertanto, il merito del Regolamento non risiede tanto nella costruzione di un sistema di principi intorno alla privacy, quanto nell'aver espressamente riconosciuto loro carattere di obbligatorietà. In passato, infatti al principio è stata data un'attuazione limitata sia per la possibilità di deroga, previo consenso, alla misura di minimizzazione sia per la poca chiarezza delle norme introdotte a livello comunitario[3].

Tra le responsabilità attribuite al titolare del trattamento chiaramente descritte nell'art. 24 del Regolamento[4],

nell'ambito del quale sono altresì individuati i principi che saranno di seguito approfonditi nell'ambito della trattazione quali quello di *data protection by design* e quello di *data protection by default*, figurano anche quelle del riesame e dell'aggiornamento delle misure tecniche e organizzative adottate.

Corre infatti precisare che il concetto di *privacy by design* è stato coniato oltre 20 anni fa dalla Dr. Ann Cavoukian quando ha ricoperto l'incarico di "Privacy Commissioner" dell'Ontario con l'indicazione dei sette principi fondanti quali: *a) Proatttivo e non reattivo: prevenire non correggere; b) Privacy come impostazione di default; c) Privacy incorporata nella progettazione; d) Massima funzionalità – valore positivo, non valore zero; e) Sicurezza ad intera protezione del ciclo di vita di un sistema; e) Visibilità e Trasparenza – Mantenere la trasparenza; f) Rispetto per la privacy dell'utente – Centralità dell'utente*. Essi sono stati poi ripresi ed adottati nella conferenza internazionale dei Garanti che si è tenuta a Gerusalemme nel 2010. I principi, *data protection by design* e *data protection by default*, illustrati nell'art. 25[5] del Regolamento non sono, quindi, completamente sconosciuti, di essi, infatti, vi è traccia, tra le altre, nel la Direttiva 2002/58/CE che disciplina il trattamento dei dati personali e la tutela dei dati personali nel settore delle comunicazioni elettroniche oltre che nella newsletter dell'Autorità Garante del 19 giugno 2015 nella quale è inserito anche un parere delle Autorità per la privacy europee riunite nel "Gruppo Articolo 29" in materia di impiego dei droni per gli usi civili.

Il principio di *data protection by design*, prevede a carico del titolare del trattamento l'obbligo di attivare tutte le misure tecniche organizzative adeguate allo stesso con la precisazione però che esse devono essere necessariamente rapportate ad una serie di parametri che sono richiamati nell'art. 25 paragrafo 1. Ovviamente, è opportuno chiarire

all’esito dall’analisi delle misure attuate dal titolare non si deve giungere ad un giudizio di adeguatezza per le misure tecniche organizzative nel loro complesso e non per ciascuna delle misure adottate. E’ agevole osservare come nel Regolamento, e più precisamente in tale ambito, è presente un concetto di neutralità nel quale non sono contenute prescrizioni vincolanti per il titolare del trattamento ma, anzi, viene lasciata piena libertà a quest’ultimo nell’individuazione delle misure tecniche organizzative adeguate al caso concreto. In particolare ciò che la norma richiede con la sua formulazione “neutrale” è la miglior soluzione possibile per soddisfare i requisiti che il Regolamento prescrive per la tutela dei diritti degli interessati e garantire nel tempo la sua applicazione in ragione del progresso tecnico, associando cosi all’elemento di flessibilità quello di un’appropriata attenzione ai diritti dell’interessato. La *privacy by design* è infatti delineata come una metodologia più che una prescrizione specifica nonostante l’individuazione specifica di alcune misure specifiche[6]. Tra le misure individuate dal Regolamento e cui lo stesso conferisce carattere di obbligatorietà figurano invece la pseudominizzazione e la minimizzazione.

Con la pseudominizzazione si verifica l’interruzione momentanea e selettiva del collegamento, e quindi i dati del soggetto interessato non possono essere ad esso associati senza l’uso di informazioni aggiuntive separatamente conservate e protette da misure tecniche organizzative adeguate ed idonee ad evitare l’associazione dell’informazione del dato al soggetto interessato; la minimizzazione è invece una misura strettamente correlata ai principi enunciati dall’art. 5 paragrafo 1 lettera c) del Regolamento ai quali il titolare nell’ambito del trattamento deve uniformarsi[7].

L’art. 25 paragrafo 2 del Regolamento descrive invece il principio di *data protection by default* che si caratterizza per i trattamenti attuati mediante l’impostazione predefinita

e la necessità di predisporre, sin dalla fase di progettazione, le impostazioni idonee ad assicurare il rispetto delle prescrizioni contenute nel Regolamento. A differenza del principio *data protection by design*, le impostazioni devono precedere il singolo trattamento con la conseguenza che ogni qualvolta le regole oppure le modalità del trattamento sono oggetto di modifica, una nuova applicazione del richiamato principio è richiesta per rendere conforme il trattamento alle prescrizioni del Regolamento. La metodologia denominata *data protection by default*, i cui trattamenti sono pertanto definiti per *impostazione predefinita*, richiede la necessità di applicare detta impostazione sin dalla fase antecedente al trattamento. La norma che non si limita ad indicare la tempistica della sua applicazione arricchisce il suo dettato con l'indicazione che oggetto del trattamento possono essere i soli dati necessari e chiarisce che tale obbligo deve valere per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. Le impostazioni predefinite non devono però essere idonee a limitare i soli dati trattati oppure le operazioni consentite, ma devono essere idonee a limitare l'accesso ai dati oggetto del trattamento ad un numero indefinito di persone fisiche senza l'intervento della persona fisica con la conseguenza che un trattamento non riconducibile alle impostazioni predefinite o comunque con esse in contrasto deve necessariamente essere caratterizzato da una forzatura del sistema.

Va infine evidenziato come l'analisi della fattispecie non può essere disgiunta da quello del Considerando 78 che contiene le motivazioni di ausilio per la piena comprensione della disposizione di riferimento. Nel Considerando 78 è descritto l'auspicio di vedere incoraggiati i realizzatori di prodotti e servizi e applicazioni affinché gli stessi possano, nell'ambito dello sviluppo e della progettazione dei prodotti, servizi e applicazioni, tenere in debita considerazione le disposizioni preposte alla tutela dei dati personali. Detto

auspicio poi è più incisivo nella sua parte finale quando sottolinea come le impostazioni di progettazioni e di default dovrebbero essere prese in considerazione, per trovare così adeguato spazio, anche negli appalti pubblici.

Note

[1] *Articolo 5* Principi applicabili al trattamento di dati personali

I dati personali sono:

- f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).

[2] L. Bolognini, E. Pelino e C. Bistolfi in "*Il Regolamento Privacy Europeo, Commentario alla nuova disciplina sulla protezione dei dati personali*" pag. 325. Giuffrè, Milano, 2016.

[3] Principato, *Verso nuovi approcci alla tutela della privacy*: privacy by design e privacy by default settings, in *Contratto e Impresa. Europa*, 2015, pag. 211.

[4] *Articolo 24* Responsabilità del titolare del trattamento

1. Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario.

2. Se ciò è proporzionato rispetto alle attività di trattamento, le misure di cui al paragrafo 1 includono l'attuazione di politiche adeguate in materia di protezione dei dati da parte del titolare del trattamento.
3. L'adesione ai codici di condotta di cui all'articolo 40 o a un meccanismo di certificazione di cui all'articolo 42 può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento.

[5] *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.

3. Un meccanismo di certificazione approvato ai sensi dell’articolo 42 può essere utilizzato come elemento per dimostrare la conformità ai requisiti di cui ai paragrafi 1 e 2 del presente articolo.

[6] Pizzetti, *Intelligenza artificiale, protezione dei dati personali e regolamentazione*, pag 116, Giappichelli, Torino 2018.

[7] *Articolo 5* Principi applicabili al trattamento di dati personali

- c) I dati personali sono: “adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati.

A cura di: **Massimo Ippoliti**

L’articolo Data protection by design e by default proviene da ICT Security Magazine.

https://www.ictsecuritymagazine.com/articoli/data-protection-by-design-e-by-default/