

Dal Garante la lista delle fattispecie per cui è obbligatoria la valutazione di impatto

Privacy, 12 i casi sotto la lente

Dai dati di soggetti vulnerabili alle geolocalizzazioni

DI ANTONIO
CICCIA MESSINA

Valutazione di impatto privacy in 12 casi. Tra questi, il trattamento di dati minori e disabili, oppure la videosorveglianza e la geolocalizzazione dei lavoratori o la profilazione online con una app.

I trattamenti sotto i riflettori del Garante della privacy sono elencati nel provvedimento 467 dell'11 ottobre 2018, adottato dall'autorità presieduta da Antonello Soro, in attuazione dell'articolo 35 del Regolamento Ue sulla protezione dei dati n. 2016/679.

L'articolo citato ha affidato alle autorità di controllo dei singoli stati europei il compito di precisare quando un titolare del trattamento (un'impresa, un ente pubblico ecc.) deve stilare, a pena di pesantissime sanzioni amministrative, un documento sulla sicurezza dei trattamenti.

Questo documento si chiama appunto valutazione di impatto privacy, noto anche come data

protection impact assessment (siglato Dpia).

L'obbligo di compilazione scatta a fronte di trattamenti di dati personali fonti di un elevato rischio per le persone.

Si tratta di un adempimento molto delicato, perché si chiede al titolare del trattamento di ponderare bene le misure tecniche e organizzative, che devono costituire barriere idonee a impedire che le persone subiscano danni (ad esempio furti di identità, manipolazione dei dati con effetti negativi, sostituzione di persona e così via).

Proprio per questo, nel corso della stesura del documento deve essere chiesto il parere del responsabile della protezione dei dati (dpo), figura questa da nominare obbligatoriamente nelle pubbliche amministrazioni e nelle imprese, se trattano su larga scala dati sensibili, genetici e biometrici o se fanno monitoraggio su larga scala.

Il regolamento Ue indica alcuni esempi (sono tre) in cui scatta l'obbligo di compilazione della dpia: profilazione, sorve-

glianza sistematica su larga scala di zona accessibile al pubblico, trattamento su larga scala di particolari categorie di dati (ovvero dati sensibili, genetici e biometrici).

Il gruppo dei garanti europei (già Gruppo lavoro articolo 29), nel 2017, ha adottato linee guida, disponibili sul sito del garante italiano. Queste linee guida, fatte proprie dal comitato europeo per la protezione dei dati, hanno indicato nove casi di trattamento a rischio elevato. Ora il garante della privacy italiano, alla luce delle indicazioni del comitato, ha compilato un elenco di 12 tipi di trattamenti da sottoporre a valutazione d'impatto, tra i quali ci sono i seguenti. Il primo riguarda i trattamenti valutativi o di scoring su larga scala, profilazione, attività predittive anche online o attraverso app; decisioni automatizzate che producono effetti giuridici sull'interessato (ad esempio screening dei clienti di una banca attraverso l'utilizzo di dati di una centrale rischi); osservazione, monitoraggio

o controllo degli interessati, trattamento di identificativi univoci in grado di identificare gli utenti di servizi della società dell'informazione (compresi i trattamenti di metadati); trattamenti su larga scala di dati aventi carattere estremamente personale; trattamenti nel rapporto di lavoro mediante sistemi tecnologici (anche con riguardo ai sistemi di videosorveglianza e di geolocalizzazione); trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo); trattamenti effettuati attraverso l'uso di tecnologie innovative (IoT; intelligenza artificiale; assistenti vocali online attraverso lo scanning vocale e testuale; monitoraggi con dispositivi indossabili; tracciamenti di prossimità come il wi-fi tracking); scambio tra diversi titolari di dati su larga scala con modalità telematiche; interconnessione, combinazione o raffronto di informazioni, compresi i trattamenti che prevedono l'incrocio dei dati

di consumo di beni digitali con dati di pagamento (ad esempio mobile payment); trattamenti di categorie particolari e di dati relativi a condanne penali e a reati interconnessi con altri dati personali raccolti per finalità diverse; trattamenti sistematici di dati biometrici; trattamenti sistematici di dati genetici. L'elenco, in corso di pubblicazione nella Gazzetta ufficiale, non è esaustivo. Pa e aziende, infatti, hanno l'obbligo di adottare una Dpia anche quando ricorrano due o più criteri individuati dal Gruppo di lavoro articolo 29 nelle Linee guida del 2017 oppure quando un titolare ritenga che un trattamento che soddisfa anche solo uno dei criteri richieda una valutazione di impatto.



Il testo del provvedimento sul sito www.italiaoggi.it/documenti-italiaoggi