I criteri. Le linee guida dei Garanti europei

Procedura dovuta se c'è monitoraggio dei dipendenti

La valutazione di impatto privacy è obbligatoria tutte le volte in cui il trattamento dei dati comporta rischi elevati per i diritti e le libertà delle persone. L'articolo 35 del regolamento afferma che la Dpia è richiesta quando si verificano:

- una valutazione sistematica e globale di aspetti personali, basata su un trattamento automatizzato, compresa la profilazione;
- il trattamento, su larga scala, di dati personali sensibili;
- la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

L'elenco, tuttavia, non è tassativo. I Garanti della privacy hanno elaborato delle linee guida (aggiornate il 4 ottobre 2017) volte a integrare quanto previsto dal Regolamento, e hanno individuato alcuni trattamenti che richiedono una valutazione di impatto «in virtù del loro rischio intrinseco». I Garanti individuano nove criteri:

1. i trattamenti valutativi o di *scoring*, compresa la profilazione;
2. le decisioni automatizzate che producono significativi effetti giuridici;
3. il monitoraggio sistematico (ad esempio tramite la videosorveglianza);
4. il trattamento di dati sensibili, giudiziari o di natura strettamente personale;
5. il trattamento di dati su larga scala;
6. la combinazione o le corrispondenze di dati;
7. il trattamento di dati relativi a soggetti vulnerabili (ad esempio minori, lavoratori dipendenti e così via);
8. l'uso o l'applicazione di nuove tecnologie (ad esempio il riconoscimento facciale);
9. i trattamenti che impediscono agli interessati di esercitare un diritto o di avvalersi di un servizio (ne è un esempio il caso delle banche per erogare un credito).

Per i Garanti, se un trattamento soddisfa almeno due dei criteri, deve costituire oggetto di una valutazione di impatto privacy. Tuttavia, in base alle linee guida, un titolare può ritenere che si debba procedere con la valutazione anche in presenza di uno solo dei criteri. Per contro, laddove il trattamento soddisfi due dei nove criteri elencati, si può evitare la Dpia, potendo documentare i motivi che hanno spinto il titolare a non effettuare la valutazione di impatto.

L'obbligo della Dpia, secondo le linee guida, si ha tutte le volte in cui si fa un monitoraggio costante delle attività dei dipendenti. Da questo punto di vista, inoltre, si deve ritenere che la valutazione dovrà essere elaborata dal titolare-datore di lavoro tutte le volte in cui tratta dati sensibili (anche su larga scala) di lavoratori o dati personali non sensibili di dipendenti o ancora quando usa un sistema di videosorveglianza.

La scelta ricade sul titolare. Alla luce delle sanzioni previste per la violazione della normativa, però (fino a 10 milioni di euro o al 2% del fatturato globale dell'azienda), indipendentemente dall'obbligatorietà o meno della valutazione di impatto privacy, è sempre preferibile adottare la procedura, perché questa aiuta ad assumere le misure di sicurezza necessarie.

MANCATO ADEGUAMENTO
Chi non si allinea al nuovo Regolamento rischia una sanzione fino a 10 milioni di euro o al 2% del fatturato