Privacy

Risk assessment e DPIA

di **Pasquale Di Gennaro**

Sommario

Uno degli elementi di maggiore novità introdotti dal Regolamento (UE) 2016/679 sulla protezione dei dati, è la previsione che i titolari del trattamento predispongano una valutazione di impatto (DPIA–*Data protection impact assessment* o anche PIA–*Privacy impact assessment*) ogni qual volta un trattamento presenti rischi elevati per i diritti e le libertà delle persone fisiche. Per determinare se debba essere predisposta la DPIA per uno specifico trattamento, e cioè per accertare se i rischi siano elevati, è implicitamente necessario effettuarne una stima. Il processo di stima del rischio è noto come *risk assessment*, ed è un elemento propredeutico all'avvio di qualunque trattamento. Se all'esito di una prima valutazione il rischio dovesse risultare *elevato*, il processo stesso dovrà essere formalizzato e documentato in una Valutazione di impatto, e ne costituirà una parte fondamentale.

1 La protezione dei dati e il rischio

Il concetto di proporzionare le misure di sicurezza tecnico-organizzative ai *rischi* per i diritti e le libertà delle persone fisiche derivanti dal trattamento dei loro dati personali, non è nuovo nella storia della *data protection*. Infatti, già il Codice italiano in materia di protezione dei dati personali[1], appena novellato dal decreto legislativo n. 101 del 10 agosto 2018 prescriveva, prima di tale ultimo intervento normativo, oltre alle misure di sicurezza *minime* l'adozione di misure di sicurezza cosiddette *idonee* che tenessero conto dei rischi peculiari al trattamento. Nel caso in cui il trattamento avesse presentato un *rischio specifico*, il Codice disponeva con l'art. 17 il ricorso all'istituto della *verifica preliminare* (o *prior checking*) da presentare al Garante affinché potesse prescrivere misure speciali adatte a mitigare i rischi peculiari di quel trattamento. Il nuovo decreto n. 101 del 10 agosto 2018 con l'art. 27 ha abrogato sia gli articoli riguardanti le misure di sicurezza minime e idonee, sia quelli riguardanti il *prior checking*. Tale modifica è stata resa necessaria per adeguare il Codice al GDPR e deriva dal fatto che per il GDPR le misure di sicurezza devono essere sempre proporzionate alle specificità di ciascun trattamento. Difatti, il Regolamento non prevede misure di sicurezza *minime* e puntuali[2], ma individua gli *obiettivi* di sicurezza. E prescrive che i titolari partendo dalla valutazione del rischio insito nel trattamento, lo mitighino individuando responsabilmente misure e accorgimenti adeguati, diminuendo così la possibilità che i dati siano oggetto di violazioni di sicurezza. Il Regolamento oltre a fissare gli obiettivi di sicurezza definisce anche uno schema metodologico per perseguirli. Tale schema, che potremmo definire come *"risk based approach"*, consiste pertanto nel salvaguardare gli obiettivi di

protezione dei dati individuando e mitigando i rischi propri di ciascun trattamento. L'approccio orientato alla valutazione del rischio (*risk based approach*), insieme al principio di responsabilitazione (*accountability*[3]) costituiscono l'ossatura stessa del Regolamento.

2 La scelta delle misure guidata dal rischio

Il *risk based approach*, cioè l'adozione da parte dei titolari di un approccio basato sulla valutazione del rischio propedeutica all'avvio di ciascun trattamento, è così importante per il Regolamento che il termine "rischio" compare ben 75 volte nel testo, in varie espressioni. E tra le varie espressioni, quella che forse più efficamente palesa la *ratio* dell'art. 35, relativo alla "Valutazione d'impatto sulla protezione dati", risalta all'art. 24 sulla responsabilità del titolare, laddove dispone che il titolare tenga "conto [...] dei *rischi aventi probabilità e gravità diverse* per i diritti e le libertà delle persone fisiche [...]". La valutazione dell'impatto che un trattamento può avere sui diritti e sulle libertà, non può prescindere dall'individuazione dei rischi e dalla stima della loro *probabilità e gravità*. Ma cos'è, dunque, un "rischio"? E in cosa consiste la sua valutazione (*risk assessment*)?

3 Cosa si intende per "rischio"

Nonostante il Regolamento citi il termine "rischio" più di 70 volte, non ne fornisce una definizione formale. L'Agenzia europea Enisa[4] nel suo glossario *on-line* sul *risk management* riprende la definizione generica ISO/IEC PDTR 13335-1, qui riformulata e semplificata per calarla nel contesto della protezione dati[5]: rischio.

Con il termine "rischio" si intende la possibilità che una minaccia riesca a sfruttare le vulnerabilità insite in un sistema informativo per il trattamento di dati personali, causando danni agli interessati e all'organizzazione.

La definizione su riportata chiarisce un aspetto fondamentale: il rischio associato al trattamento dei dati personali ha una duplice dimensione: la prima relativa ai rischi per i diritti e le libertà degli interessati dal trattamento dei propri dati; la seconda relativa ai titolari (e responsabili) che si avvalgono di quei dati nell'ambito delle loro attività di impresa. Il GDPR focalizza l'attenzione sui rischi derivanti dai trattamenti per le persone fisiche. Tuttavia, se i rischi per gli interessati non sono opportunamente mitigati ne consegue un aumento del rischio d'impresa. In effetti, i danni derivanti per l'impresa non sono solo le possibili sanzioni motivate dalla *legal un-compliance*. Nella società dell'informazione, infatti, i dati personali sono un *asset* per le imprese, un patrimonio strategico da valorizzare e difendere costruito con fatica e solo dopo aver guadagnato la fiducia dei propri utenti. Si intuisce, pertanto, che le conseguenze per l'impresa derivanti dalla violazione della confidenzialità del proprio patrimonio aziendale, o dalla distruzione anche solo parziale di tale patrimonio, vanno ben oltre l'obbligo di inviare al Garante la notifica di *data breach* (art. 33 del Regolamento), ma hanno a che fare con danni per l'impresa di natura patrimoniale e d'immagine. Assume dunque primaria importanza l'attività di prevenzione mirata a gestire e contenere i rischi (*risk management*) che parte proprio dalla loro individuazione e stima*:* il *risk assessment*.

4 Il risk assessment

L'individuazione e la stima dei rischi connaturati a uno specifico trattamento sono un'attività complessa. Complessa perché richiede un bagaglio di conoscenze multidisciplinari e di esperienze notevole. Oltre che di una conoscenza approfondita del contesto operativo. Tale complessità può essere utilmente gestita partendo proprio dal *rendere consapevoli*. Infatti, la consapevolezza dell'importanza del *risk management* nel processo di adeguamento al GDPR è già un traguardo importante che può influenzare produttivamente l'atteggiamento e la propensione alla collaborazione del vertice decisionale e degli altri *stakeholder* nell'organizzazione. La successiva individuazione e valutazione dei rischi andrà conseguita tenuto conto anche della dimensione e della complessità della realtà in cui si è chiamati ad operare. In realtà più articolate il *risk assessment* è certamente un processo che richiede la sinergia dei vari dipartimenti aziendali, legali e tecnici, e risulterà più efficace se conseguito in maniera sistematica e strutturata, avvalendosi di una metodologia. Ad esempio, Enisa ha recentemente pubblicato un *Handbook on Security of Personal Data Processing*[6] rivolto alle piccole e medie imprese che introduce una metodologia di valutazione del rischio e ne esemplifica l'applicazione discutendo alcuni trattamenti ricorrenti. Nel caso delle micro-imprese si può comunque trarre beneficio dalle esemplificazioni Enisa, perché sono un valido ausilio a una pre-valutazione del rischio che consenta di determinare se lo scenario allo studio richieda o meno il ricorso ad una metodologia più strutturata. Un ulteriore utilissimo strumento sono le indicazioni del gruppo ex art. 29[7], riportate in particolare nella *opinion WP* 248, che fornisce dei criteri per individuare i trattamenti ad elevato rischio e delle esemplificazioni che consentono di inquadrare la rischiosità di alcuni trattamenti "tipo" e comprendere laddove sia necessario o meno procedere con la predisposizione della Valutazione di impatto sulla protezione dati (DPIA).

5 Conclusioni

La gestione del rischio è una delle novità più importanti del GDPR, ma anche forse la più difficile da illustrare e da padroneggiare, perché reca in sé un cambio di mentalità: il passaggio dalla *legal compliance* –in particolare delle misure di sicurezza– intesa come una *check list* da smarcare, vecchio retaggio delle misure minime di sicurezza ormai superate; alla *legal compliance* come un obiettivo di adeguatezza delle misure di sicurezza tecniche e organizzative da perseguire con un metodo guidato dal rischio intrinseco, il *risk based approach*, che necessita dell'individuazione e della stima dei rischi come elementi propedeutici e necessari alla loro mitigazione. Il modo più efficace di conseguire gli obiettivi di protezione dei dati personali, ovvero di protezione delle persone *e* dell'impresa, è infatti *prevenire* i danni grazie all'efficace *mitigazione* dei rischi connaturati all'utilizzo dei dati personali. Dati che, nell'era dell'informazione completamente digitale, sono esposti alle molteplici e mutevoli minacce del cyberspazio.

[1] D.lgs. 30 giugno 2003, n.196

[2] Anche la pseudonimizzazione e la cifratura di cui all'art. 32, par. 1, lettera a) vanno intese

come mere tecniche di ausilio al conseguimento degli obiettivi di confidenzialità, integrità e disponibilità. Ma non misure minime.

[3] Termine che in inglese sintetizza una dimensione soggettiva e una oggettiva della responsabilità: *sento* il peso della responsabilità derivante dalla fiducia che hanno riposto in me i miei clienti quando mi hanno affidato i loro dati personali, ma *devo essere in grado di dimostrare* di trattare tali dati responsabilmente. Ad esempio predisponendo la DPIA.

[4] European Union Agency for Network and Information Security

[5] Per un approfondimento, si veda la definizione di "rischio" nella ISO/IEC 27000:2018 che ha assorbito e sostituito la ISO/IEC 13335

[6] https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing

[7] Sostituito dal Comitato europeo per la protezione dei dati, EDPB - European Data Protection Board