3 Articoli

Armando Montemarano

Privacy: in vigore il nuovo Regolamento

«Sebbene i suoi obiettivi e principi rimangano tuttora validi, la direttiva 95/46/CE non ha impedito la frammentazione dell'applicazione della protezione dei dati personali nel territorio dell'Unione, né ha eliminato l'incertezza giuridica o la percezione, largamente diffusa nel pubblico, che in particolare le operazioni on line comportino rischi per la protezione delle persone fisiche».

Con questa affermazione, contenuta nel nono considerando del Regolamento n. 2016/679, il Parlamento europeo e il Consiglio dell'Unione europea hanno riconosciuto la sopravvenuta inadeguatezza, dopo oltre vent'anni, della legislazione sul trattamento dei dati, tracciando indirettamente una linea di cancellazione anche sul codice della privacy italiano (D.Lgs. n. 196/2003), almeno come finora articolato.

Il principio di responsabilizzazione

Si cambia, dunque, registro: non più una normativa basata sul tradizionale principio di legalità, edificato - secondo il brocardo *nullum crimen sine lege, nulla poena sine lege* - sullo schema «ordine del legislatore/sanzione per la disubbidienza», bensì sul principio di responsabilizzazione. Quello stesso, per capirci, cui si ispirano le norme in materia di modelli organizzativi, di certificazione di qualità, di sicurezza del lavoro, di anticorruzione, di antiriciclaggio: di tutti i sistemi, cioè, di gestione dell'impresa che da tempo, ormai, vengono elaborati in sede eurounitaria, i quali sono unificati da una stessa concezione di prassi gestoria e sono unificabili in una organica metodologia di governo aziendale (va infatti ricordato che, quando si parla di privacy, si parla di attività d'impresa, perché la normativa in materia non si applica in mancanza di una connessione con un'attività commerciale o professionale, profit o non profit; non si applica, cioè, al trattamento di dati personali effettuato dalle persone fisiche nell'ambito di attività a carattere personale o domestico, comprese la corrispondenza, gli indirizzari, l'uso dei social network e la pratica delle altre attività on line).

Il principio di responsabilizzazione viene codificato muovendo da alcune premesse:

— sussiste una responsabilità generale del titolare per qualsiasi trattamento di dati personali che abbia effettuato direttamente o che altri abbiano effettuato per suo conto;

— il titolare è tenuto a mettere in atto misure adeguate ed efficaci ed essere in grado di dimostrare la conformità delle attività di trattamento con il Regolamento;

— le misure adottate devono tenere conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche derivanti da trattamenti suscettibili di cagionare un danno fisico, materiale o immateriale;

— la probabilità e la gravità del rischio per i diritti e le libertà dell'interessato vanno misurate dal titolare in base ad una valutazione oggettiva mediante la quale stabilire se i trattamenti di dati comportano un rischio elevato;

— la tutela dei diritti e delle libertà delle persone fisiche richiede l'adozione di misure tecniche e organizzative adeguate e dimostrabili;

— la responsabilità generale dei titolari e dei responsabili del trattamento, anche in relazione al monitoraggio e alle misure delle autorità di controllo, esige una chiara ripartizione interna delle responsabilità.

Il compito fondamentale del RPD o DPR "Data Protection Officer" è esplicitato dal Regolamento che ne prevede il coinvolgimento "tempestivamente e adeguatamente in tutte le questioni riguardanti la protezione dei dati personali" (art. 38 RGPD).

I due pilastri del trattamento

È affidato ai titolari il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali, alla luce di due criteri specifici, indicati nel Regolamento:

1) data protection by default and by design: protezione per impostazione predefinita e per configurazione del sistema prima di procedere al trattamento dei dati e a seguito di un'analisi preventiva e di un impegno attuativo, che deve sostanziarsi in una serie di attività specifiche e dimostrabili;

2) misurazione del rischio di impatti negativi sulle libertà e i diritti degli interessati: tali impatti dovranno essere analizzati attraverso un apposito processo di valutazione, tenendo conto dei rischi noti o evidenziabili e delle misure tecniche e organizzative (anche di sicurezza) che il titolare ritiene di dover adottare per mitigare i rischi.

Su questi due pilastri si reggerà il regime di responsabilità, che consiste principalmente nel fatto che il titolare del trattamento o il responsabile del trattamento dovranno risarcire i danni cagionati ad una persona da un trattamento non conforme al Regolamento, con la possibilità, tuttavia, di essere esonerati da responsabilità dimostrando che l'evento dannoso non era in alcun modo loro imputabile.

Il registro dei trattamenti

La dimostrazione dell'ottemperanza al Regolamento può essere data da un *registro dei trattamenti*, tenuto sotto la responsabilità del titolare o del responsabile i quali, su richiesta, dovrebbero mettere il registro a disposizione dell'autorità di controllo, affinché possa servire per monitorare i trattamenti. L'intervento del Garante avverrà principalmente a posteriori, successivamente alle determinazioni assunte autonomamente dal titolare. Ciò spiega l'abolizione, a partire dal 25 maggio 2018, di alcuni istituti previsti dal codice della privacy, come la notifica preventiva dei trattamenti all'autorità di controllo e la verifica preliminare, sostituiti dagli obblighi di tenuta del registro.

Il registro dei trattamenti deve contenere essenzialmente le seguenti informazioni:

- il nome e i dati di contatto del titolare del trattamento e, se del caso, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;
- le finalità del trattamento;
- una descrizione delle categorie di interessati e delle categorie di dati personali;
- le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
- una descrizione generale delle misure di sicurezza tecniche e organizzative adottate;
- i trasferimenti di dati personali verso un Paese terzo o un'organizzazione internazionale;
- i termini ultimi previsti per la cancellazione delle diverse categorie di dati.

Gli orientamenti per la messa in atto di opportune misure e per dimostrare la conformità da parte del titolare o del responsabile - in particolare per quanto riguarda l'individuazione del rischio connesso al trattamento, la sua valutazione in termini di origine, natura, probabilità e gravità - e l'individuazione di migliori prassi per attenuare il rischio, potrebbero essere forniti mediante:

- codici di condotta approvati;
- certificazioni approvate;
- indicazioni fornite da un responsabile della protezione dei dati;
- linee guida fornite dal Comitato europeo della protezione dei dati.

Le basi giuridiche del trattamento

Le figure individuate dal codice della privacy, a parte il DPO, restano le stesse (titolare, responsabile, incaricato), come pure i fondamenti di liceità del trattamento:

— *consenso*: dev'essere esplicito per i dati sensibili e manifestato attraverso dichiarazione o azione positiva inequivocabile, qual è l'adempimento di obblighi contrattuali;

— *interesse vitale* dell'interessato o di terzi: si può invocare tale base giuridica solo se nessuna delle altre condizioni di liceità può trovare applicazione;

— *obblighi di legge* cui è soggetto il titolare: ad esempio, nel caso dell'esercizio di pubblici poteri (si pensi ad una scuola o ad un ospedale);

— *interesse legittimo* prevalente del titolare o di terzi cui i dati vengono comunicati: l'interesse deve prevalere sui diritti e le libertà fondamentali dell'interessato per costituire un valido fondamento di liceità.

La normativa, però, non detta più le misure di sicurezza da adottare; ne affida l'individuazione al titolare e al responsabile, che devono dimostrare di averle adottate, di averle effettivamente attuate e che erano idonee, in base alla valutazione preventiva del rischio, a tutelare gli interessati.

Accountability e compliance

La parola-chiave, secondo tutti gli interpreti, è ***accountability***; responsabilità o, meglio, responsabilizzazione: assunzione di responsabilità da parte di un soggetto o un gruppo di soggetti (*accountors*) del risultato conseguito da un'organizzazione, sulla base delle proprie capacità e della propria etica. La responsabilizzazione richiede:

- capacità decisionale;
- rispetto dei portatori di interessi (*accountees*);
- premi, se i risultati prefissati sono conseguiti;
- sanzioni, se i risultati prefissati non sono conseguiti.

La definizione degli obiettivi costituisce il mezzo principale per assicurare l'accountability che, a sua volta, presuppone la ***compliance***, cioè il rispetto delle norme sotto un duplice profilo: a) la legittimità dell'azione; b) l'adeguamento dell'azione proattiva agli standard stabiliti da leggi, regolamenti, linee guida o codici di condotta. L'accountability, dunque, per quanto concerne il trattamento dei dati personali:

- si riferisce all'obbligo di rendere conto delle proprie decisioni e di essere responsabile per i risultati conseguiti nell'esercizio della libertà di scelta dei mezzi;
- si fonda sulla realizzazione di comportamenti proattivi, vale a dire di iniziative tali da comprovare la concreta attuazione delle misure finalizzate ad assicurare l'applicazione del Regolamento.

Il DPO - Data Protection Officer

Se la *compliance* diventa essenziale, la figura interna cui fare riferimento è individuata dal Regolamento nel *Responsabile della protezione dei dati* (RPD o DPO, *data protection officer*), la cui nomina è obbligatoria ogni qual volta:

- il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico;
- il trattamento dei dati personali su larga scala costituisce una componente inscindibile delle attività aziendali; vale a dire quando le attività principali del titolare o del responsabile consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati oppure consistono nel trattamento, su larga scala, di categorie di dati sensibili.

Allo stato attuale, in attesa di migliori esemplificazioni del Garante, **la nomina del DPO, per quanto concerne specificamente le attività degli Enti ecclesiastici, è da ritenere obbligatoria nelle seguenti opere:**

Ospedali, case di cura, Rsa e simili

In base al secondo capoverso della FAQ 3 sul responsabile della protezione dei dati in ambito privato, pubblicata sul sito del Garante il 26 marzo 2018, sono tenuti alla nomina, tra gli altri, le «società operanti nel settore della cura della salute, della prevenzione/diagnostica sanitaria, quali ospedali privati, terme, laboratori di analisi mediche, centri di riabilitazione».

Scuole

In base al par. 2.1.1 delle linee guida elaborate dal «Gruppo Articolo 29», premesso che la nomina di un DPO è obbligatoria per i trattamenti effettuati da un'autorità pubblica o da un organismo pubblico, sono autorità pubbliche o organismi pubblici le autorità nazionali, regionali e locali ma, a seconda del diritto nazionale applicabile, anche tutta una serie di altri organismi di diritto pubblico; **al riguardo è indubbio che le scuole statali devono nominare il DPO e che le scuole paritarie sono da considerare esercenti un servizio pubblico.**

Altre attività di utilità sociale

In base al secondo capoverso della FAQ 4 del Garante, in ogni altro caso resta comunque **raccomandata**, anche alla luce del principio di accountability che permea il Regolamento, la designazione del DPO.

L'art. 83, comma 4, Reg. (CE) n. 2016/679/UE stabilisce che la mancata nomina del DPO è soggetta a sanzioni amministrative pecuniarie fino a 10 milioni di euro o, per le imprese, fino al 2 % del fatturato totale annuo dell'esercizio precedente.

Il DPO va designato, secondo il Regolamento, in funzione delle qualità professionali, dunque deve essere un giurista o, comunque, una persona esperta del diritto; può essere un dipendente oppure assolvere i suoi compiti in base ad un contratto di servizi ma:

- non può essere rimosso o penalizzato per l'adempimento dei propri compiti;
- deve riferire direttamente al vertice gerarchico del titolare o del responsabile;
- può essere contattato direttamente dagli interessati;
- è tenuto al segreto d'ufficio;
- può svolgere altri compiti, purché non ricorra un conflitto di interessi.

Il DPO è incaricato almeno dei seguenti compiti: a) informare e fornire consulenza al titolare o al responsabile, nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dalla normativa; b) vigilare sull'osservanza della normativa nonché delle politiche del titolare o del responsabile in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo; c) cooperare con l'autorità di controllo.

I codici di condotta e la certificazione

La conformità al Regolamento dei trattamenti potrà essere asseverata da meccanismi di certificazione, con particolare riguardo alle esigenze specifiche delle micro, piccole e medie imprese.

La certificazione è volontaria e non riduce la responsabilità del titolare o del responsabile; è rilasciata dagli organismi di certificazione accreditati dall'ente unico italiano, Accredia, o dall'autorità di controllo competente, il Garante, in base ai criteri approvati da tale autorità; è accordata per un periodo massimo di tre anni e può essere rinnovata alle stesse condizioni, purché continuino ad essere soddisfatti i requisiti pertinenti.

Gli organismi di certificazione possono essere accreditati se:

— hanno dimostrato all'autorità di controllo di essere indipendenti e competenti e, dunque, che i compiti e le funzioni da essi svolti non danno àdito a conflitto di interessi;

— si sono impegnati a rispettare i criteri di certificazione approvati dall'autorità di controllo;

— hanno istituito procedure che gli consentano di valutare l'idoneità dei titolari e dei responsabili ad applicare il codice di condotta eventualmente adottato, di controllare che detti titolari e responsabili ne rispettino le disposizioni e di riesaminarne periodicamente il funzionamento;

Principio di accountability

"Con il nuovo Regolamento viene definito un principio già riconosciuto dal Garante: quello che prevede che sia responsabilità del possessore dei dati sensibili conservarli in maniera corretta". Il principio di accountability sancisce dunque che sarà onere dell'azienda o dell'ente che ha i nostri dati dimostrare un "atteggiamento proattivo nella salvaguardia del dato personale dell'utente".

— hanno istituito procedure per il rilascio, il riesame periodico e il ritiro delle certificazioni, dei sigilli e dei marchi di protezione dei dati, nonché i reclami relativi a violazioni della certificazione.

Il Regolamento prospetta, come esposto, la possibilità di redigere codici di condotta, destinati a contribuire alla sua corretta applicazione, in funzione delle specificità dei vari settori di trattamento e delle esigenze delle micro, piccole e medie imprese. I codici possono essere elaborati dalle associazioni e dagli altri organismi di rappresentanza delle categorie di titolari o dei responsabili allo scopo di dettagliare l'applicazione del Regolamento. Il codice di condotta dovrà contenere, quindi, i meccanismi che consentono all'organismo accreditato di effettuare il controllo obbligatorio del rispetto delle norme da parte dei titolari o dei responsabili che si impegnano ad applicarlo.

Le associazioni e gli altri organismi che intendono elaborare un codice di condotta tenendo conto delle caratteristiche specifiche dei trattamenti effettuati in alcuni settori, o modificare o prorogare un codice esistente, devono sottoporre il progetto di codice, la modifica o la proroga, all'autorità di controllo, che esprime un parere sulla conformità al Regolamento e approva il progetto se ritiene che offra garanzie adeguate.

Il modello di organizzazione

La logica che permea il Regolamento europeo, si è detto, è quella del modello organizzativo. Per farsi intendere, con un'approssimazione che però rende bene la sostanza ultima delle cose, il DPO sta alla privacy come l'Organismo di vigilanza sta al modello organizzativo, come il Responsabile del servizio prevenzione e protezione sta alla sicurezza sul lavoro, come il Responsabile della qualità sta alla certificazione di qualità, come il Responsabile della prevenzione della corruzione sta all'anticorruzione. O, ancora, il registro dei trattamenti sta alla privacy come il modello organizzativo sta alla responsabilità amministrativa da reato, come il documento di valutazione dei rischi sta alla sicurezza sul lavoro, come il manuale della qualità sta alla certificazione.

Nulla vieta (anzi, tutto lo suggerisce) che, avendone requisiti e professionalità, stante anche la sussunzione della sicurezza sul lavoro nel modello organizzativo imposta dall'art. 30 D.Lgs. n. 81/2008, uno stesso soggetto, collegiale o monocratico, possa riassumere in sé i ruoli apicali previsti dalle diverse disposizioni nelle suindicate materie, in modo che il compendio di tutta la documentazione costituisca l'evidenza e la prova della procedimentalizzazione delle attività, elevando così il rating di legalità dell'Organizzazione.

Quando il costo della prevenzione si stima maggiore del danno che si può ricevere dall'accadimento dell'evento dannoso, si è portati a non apprezzarne l'utilità. E allora, per contenere quanto più possibile questo costo, si ricorre ad interventi di facciata: si scopiazzano da internet o dai formulari codici etici e piani di sicurezza; si designano anziani pensionati o sprovveduti dipendenti e collaboratori a presidenti degli Organismi di vigilanza o a fungere da RSPP. Tutto ciò costa poco ma, ovviamente, non rende nulla, non apporta alcun reale beneficio; seppure contenuto, il costo resterà sempre un peso.

Se si pensasse invece di realizzare, magari proprio a partire dalla «nuova» privacy, veri protocolli di formazione delle decisioni, che consentissero la verificabilità delle operazioni, l'individuazione delle singole responsabilità, la documentazione delle azioni; se si attuasse, cioè, un sistema di controllo interno efficiente, non più affidato alla buona volontà dei singoli presenti in loco, che consentisse davvero alle funzioni apicali di monitorare costantemente le attività e, quindi, di prevenire i fattori di rischio, il costo potrebbe diventare investimento. Soprattutto per gli Enti ecclesiastici, messi di fronte al coinvolgimento crescente dei laici nella gestione delle opere e nella conseguente necessità di affidare ai religiosi, oltre alla custodia e all'interpretazione del carisma, i ruoli di direzione e di controllo della gestione delle attività.

D'altronde, dovrebbe dare da riflettere la constatazione che sono le economie e le imprese più avanzate del pianeta - e non certo quelle più retrive - a costruirsi proprio su quei sistemi di gestione che da noi sono talvolta considerati insopportabili fonti di spesa, insostenibili balzelli.