La privacy e la regolazione multilivello

Author : Francesco Maldera

Date : 17 Gennaio 2019

Obiettivo finale e principio cardine del GDPR

Perché nasce il Regolamento Europeo per la Protezione dei Dati Personali (GDPR)? Lo dice il Considerando n. 10 dello stesso GDPR:

*"[…] È opportuno assicurare un'applicazione **coerente** e **omogenea** delle norme a protezione dei diritti e delle libertà fondamentali delle persone fisiche con riguardo al trattamento dei dati personali in tutta l'Unione. [...]"*

oltre che il Considerando n. 13:

"Per assicurare un livello coerente di protezione delle persone fisiche in tutta l'Unione e prevenire disparità che possono ostacolare la libera circolazione dei dati personali nel mercato interno, è necessario un regolamento che garantisca certezza del diritto e trasparenza agli operatori economici, [...]"

Quindi, il legislatore europeo ha preso atto che la direttiva 95/46/CE era stata applicata dagli Stati Membri con modalità che, spesso, frenavano la libera circolazione dei dati (iperlegislazione) oppure non garantivano una sufficiente difesa dei diritti e delle libertà delle persone fisiche (ipolegislazione).

E qual è il principio sul quale è imperniato il GDPR? La dottrina si è orientata, ormai, sulla centralità del principio di responsabilizzazione (accountability) esposto al comma 2 dell'art. 5:

"Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo («responsabilizzazione»)"

La maggior parte degli esperti, nella spiegazione di questo principio, si è concentrata sul *refrain* secondo il quale il titolare del trattamento "deve applicare il GDPR e deve essere in grado di comprovarlo". Ovvero, il titolare deve garantire un ciclo continuo di impegno nell'applicazione

del GDPR e deve documentare il suo *percorso*. Questo è certamente vero, ma quasi tutti i commentatori trascurano l'aggettivo *competente* (*responsible* nella versione inglese) che, invece, è centrale nell'interpretazione del singolo articolo oltre che dell'intero GDPR. L'aggettivo *competente*, in italiano, ha una doppia semantica: vuol dire "capace, esperto, professionale, adeguato" ma anche "che ne ha il compito esclusivo, che rientra nella sua peculiare sfera d'azione". Quindi, il titolare del trattamento dei dati personali è il *dominus* nell'applicazione del GDPR secondo una professionalità da acquisire direttamente (molto di rado) o indirettamente (affidandosi a specialisti della materia).

Quando la questione si complica

Su queste basi si può dire che il GDPR fornisce molte indicazioni metodologiche (privacy by desgin, privacy by default, valutazione d'impatto, ecc.) e poche prescrizioni pratiche, induce a comportamenti virtuosi e scoraggia la pedissequa applicazione di formalismi. Spetta al titolare *autovalutare* i propri processi di trattamento ed *autodefinire* le misure di sicurezza adeguate al fine di garantire agli interessati i diritti e le libertà previsti dalla Carta dei diritti fondamentali dell'Unione Europea.

L'approccio, quindi, sembra molto diverso da quello previsto dalla precedente normativa italiana che, invece, regolava in modo molto dettagliato sia l'avvio di alcuni processi di trattamento sia le modalità con le quali i processi dovevano essere condotti. In realtà, a guardare il nuovo testo del Codice privacy italiano (D.Lgs. 196/2003 così come modificato dal D.Lgs. 101/2018) sembra che il titolare del trattamento continui ad essere davvero poco *autonomo* e che debba affrontare un percorso molto accidentato per *inseguire* tutto quello che il quadro normativo prevede.

Infatti, oltre al GDPR ed al Codice privacy, emerge una molteplicità di disposizioni regolatorie secondarie alle quali il titolare deve adeguarsi:

- i codici di condotta (art. 40 del GDPR);
- le regole deontologiche (art. 2?quater del Codice privacy);
- le misure di garanzia per il trattamento di dati genetici, biometrici e relativi alla salute (art. 2?septies del Codice privacy);
- le prescrizioni, contenute nelle precedenti autorizzazioni generali, che risultano compatibili con il GDPR e con il nuovo Codice privacy (art. 21 del D.Lgs. 101/2018).

Com'è facile osservare, gli unici documenti esplicitamente previsti dal GDPR, sono i codici di condotta. Il resto proviene dalla necessità, tutta italiana, di assicurare una transizione che, tuttavia, potrebbe essere molto difficile da gestire.

A questi documenti, si devono aggiungere le linee guida ed i pareri (*opinions*) prodotte dal *vecchio* WP29 ed dal *nuovo* Comitato Europeo per la Protezione dei Dati (EDPB) e che, ad onor del vero, si caratterizzano sempre per la grande utilità esplicativa ed esemplicativa.

Proviamo, quindi, ad approfondire i caratteri della regolazione da applicare in Italia.

I codici di condotta

I codici di condotta, previsti dall'art. 40 del GDPR, sono documenti attraverso i quali una pluralità di titolari (o responsabili), che svolgono trattamenti omogenei, decidono di autovincolarsi per assicurare la conformità al GDPR; i codici diventano operativi solo quando sono approvati dall'Autorità di controllo competente (nel caso italiano dal Garante per la Protezione dei Dati Personali). Tuttavia, se i trattamenti di cui si occupa il codice di condotta non sono esclusivi di un solo Stato membro, l'approvazione avviene da parte della Commissione Europea e prevede il preventivo parere del Comitato Europeo per la Protezione dei Dati.

Finora non sono stati approvati codici di condotta validi in tutta l'Unione Europea né sono stati approvati codici di condotta dal Garante per la Protezione dei Dati Personali. Questi documenti, tuttavia, costituiscono l'approdo finale previsto dall'art. 20 del D.Lgs. 101/2018. Nel frattempo, però, cosa fare dei codici di deontologia e di buona condotta che facevano parte integrante del vecchio testo del Codice privacy?

Le regole deontologiche

In attesa dell'iter di approvazione dei codici di condotta corrispondenti, sempre l'art. 20 del D.Lgs. 101/2018 stabilisce che il Garante per la Protezione dei Dati Personali trasformi i codici di deontologia e di buona condotta (in particolare quelli riportati negli allegati A.1, A.2, A.3, A.4 e A.6 del Codice privacy) in regole deontologiche. Quindi, le regole deontologiche sono documenti di transizione per consentire un adattamento *on fly* dei vecchi codici deontologici.

Per la verità, l'art. 20 stabilisce una procedura *snella* solo per trasformare in regole deontologiche i vecchi codici deontologici. La procedura ordinaria per varare le regole deontologiche è contenuta nell'art. 2?quater nel Codice privacy e prevede che un eventuale schema, proposto da un'associazione di categoria (o da un'altra pluralità rappresentativa di titolari o responsabili) sia posto in consultazione pubblica dal Garante per almeno sessanta giorni per, poi, essere pubblicate in Gazzetta Ufficiale.

Questa procedura ha carattere permanente e ciò fa pensare che, a regime, le regole deontologiche si affiancheranno ai codici di condotta. Con quale differenza? Lo dice l'ultimo comma dello stesso art. 2?quater del nuovo Codice privacy

"[…] Il rispetto delle disposizioni contenute nelle regole deontologiche di cui al comma 1 costituisce condizione essenziale per la liceità e la correttezza del trattamento dei dati personali."

Quindi, le regole deontologiche hanno un carattere fortemente prescrittivo: violarle significa trattare i dati illecitamente. Invece, i codici di condotta nascono per indurre i titolari (o i responsabili) a comportamenti virtuosi nel trattamento dei dati personali.

In ogni caso, nel giorni scorsi il Garante per la Protezione dei Dati Personali ha approvato le

regole deontologiche[i] corrispondenti ai vecchi codici di deontologia e buona condotta secondo la procedura *snella* prevista dall'art. 20 del D.Lgs. 101/2018. In particolare, sono state inviate alla pubblicazione in Gazzetta Ufficiale le seguenti regole deontologiche:

- regole deontologiche relative al trattamento di dati personali nell'esercizio dell'attività giornalistica; le modifiche sono state minime e hanno riguardato, in prevalenza, adeguamenti formali dei riferimenti normativi;
- regole deontologiche relative ai trattamenti di dati personali effettuati per svolgere investigazioni difensive o per fare valere o difendere un diritto in sede giudiziaria; anche in questo caso, gli interventi sono stati perlopiù volti all'allineamento normativo anche se ha destato qualche clamore l'obbligatorietà dell'informativa per dati ed informazioni raccolti presso terzi per la quale, nel vecchio codice, c'era un esonero;
- regole deontologiche per il trattamento a fini di archiviazione nel pubblico interesse o per scopi di ricerca storica; le modifiche, oltre ai riferimenti normativi, sono state piuttosto leggere ed hanno riguardato un articolo che si chiamava "Regole generali di condotta" ridenominato in "Disposizioni generali" (per non creare confusione con i codici di condotta del GDPR) e l'eliminazione dell'informativa semplificata (non prevista dal GDPR) nel caso di acquisizione di dati, nell'ambito di un progetto di ricerca storica, da fonti orali;
- regole deontologiche per trattamenti a fini statistici o di ricerca scientifica pubblicate e regole deontologiche per trattamenti a fini statistici o di ricerca scientifica effettuati nell'ambito del Sistema Statistico nazionale; per queste due regole deontologiche (accomunate da finalità molto simili) l'intervento del Garante è stato più significativo; le modifiche più importanti, tuttavia, hanno riguardato la sostanziale eliminazione di prescrizioni dettagliate sia nella valutazione del rischio (che il GDPR demanda interamente al titolare) sia nelle modalità per consentire l'esercizio dei diritti da parte dell'interessato; peraltro, l'intero ambito statistico ha potuto beneficiare, di recente, della direttiva n. 11 del 7/11/2018[ii] emanata dal Comitato di Indirizzo e Coordinamento dell'Informazione Statistica che disciplina le modalità di presentazione e conduzione dei progetti di ricerca.

Le prescrizioni

Il vecchio Codice privacy prevedeva, all'art. 40 (oggi abrogato), che il Garante potesse procedere a formulare autorizzazioni generali per determinate categorie di titolari o di trattamenti. Alla fine del 2016 il Garante ha provveduto a rinnovare molte autorizzazioni generali già prodotte in passato, in attesa che il Codice privacy fosse adeguato al GDPR; questo è avvenuto, come già detto, con il D.Lgs. 101/2018 che, all'art. 21, ha inteso trasformare le autorizzazioni generali in prescrizioni. Il processo di trasformazione è caratterizzato da una preventiva consultazione pubblica che il Garante ha avviato con provvedimento del 13 dicembre 2018[iii] con il quale sono state pubblicate le prescrizioni riguardanti

- il trattamento di categorie particolari di dati nei rapporti di lavoro (aut. gen. n. 1/2016);
- il trattamento di categorie particolari di dati da parte degli organismi di tipo associativo, delle fondazioni, delle chiese e associazioni o comunità religiose (aut. gen. n. 3/2016);
- il trattamento di categorie particolari di dati da parte degli investigatori privati (aut. gen.

n. 6/2016);
- il trattamento dei dati genetici (aut. gen. n. 8/2016);
- il trattamento dei dati personali effettuato per scopi di ricerca scientifica (aut. gen. n. 9/2016).

È evidente che alcune prescrizioni riguardano gli stessi ambiti considerati dalle regole deontologiche e, anche in questo caso, costituiscono norme vincolanti per i titolari ed i responsabili visto che, l'art. 21 del D.Lgs. 101/2018, al comma 5, stabilisce che

"[…] Salvo che il fatto costituisca reato, le violazioni delle prescrizioni contenute nelle autorizzazioni generali di cui al presente articolo e nel provvedimento generale di cui al comma 1 sono soggette alla sanzione amministrativa di cui all'articolo 83, paragrafo 5, del Regolamento (UE) 2016/679."

Le misure di garanzia

Le prescrizioni, sempre secondo l'art. 21 del D.Lgs. 101/2018, saranno sostituite dalle misure di garanzia previste dall'art. 2?septies del nuovo Codice privacy. Le misure di garanzia

- riguarderanno solo il trattamento dei dati genetici, biometrici e relativi alla salute;
- dovranno essere sottoposte, analogamente alle regole deontologiche, ad una consultazione pubblica della durata non inferiore a sessanta giorni;
- dovranno essere aggiornate ogni due anni tenendo conto dell'evoluzione del contesto di applicazione.

Per il momento, tuttavia, non c'è alcuna ipotesi di adozione delle misure di garanzia.

Conclusioni

Coerenza, omogeneità e responsabilizzazione: tre parole chiave del GDPR alle quali la regolazione secondaria, almeno in Italia, sembra contrapporre specificità e complessità che, certamente, non sono quello che titolari e responsabili auspicavano.

Note

- [i] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9069732
- [ii] http://www.sistan.it/fileadmin/Repository/Home/NORME_E_PROCEDURE/ORGANIZZAZIONE_E_FUNZIONAMENTO/UFFICI_DI_STATISTICA/Direttiva%2011%20del%207%20novembre%202018.pdf
- [iii] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9068972

Articolo a cura di **Francesco Maldera**