I codici di condotta: un’occasione da cogliere

Author : Francesco Maldera

Date : 8 Aprile 2019

L’inquadramento normativo

Ci siamo già occupati, almeno in parte, dei codici di condotta[i] previsti dall’art. 40 del Reg. UE 2016/679 (GDPR) e li abbiamo collocati nella normativa secondaria che i titolari ed i responsabili del trattamento dei dati personali saranno chiamati a rispettare.

Sinora nessun codice di condotta è stato varato a livello nazionale ed europeo, perché il Comitato Europeo dei Garanti per la Protezione dei Dati Personali (EDPB) non aveva prodotto le relative linee guida per l’uniforme applicazione dell’istituto in tutta l’Unione Europea.
Le ***Linee guida sui Codici di Condotta e sugli Organismi di Monitoraggio***[ii] (d’ora in poi “linee guida”) sono state avviate alla consultazione pubblica nella settima riunione plenaria, tenutasi il 13 febbraio 2019: ciascuno ha potuto esprimere le proprie considerazioni su questo documento dal 19 febbraio al 2 aprile 2019.

Una volta consolidate le linee guida, potranno essere avviati ad approvazione i codici di condotta. In questo momento, almeno in Italia, la normativa che detta il percorso per renderli operativi è contenuta nell’**art. 20 del D.Lgs. 101/2018** che ha modificato e integrato il D.Lgs. 196/2003 (Codice privacy). Il punto di partenza sono i codici di deontologia e buona condotta (previsti dal vecchio Codice privacy e ad esso allegati): questi documenti non esistono più, almeno in questa denominazione. Sono stati sostituiti dalle **regole deontologiche** pubblicate sulle Gazzette Ufficiali del 3 gennaio 2019 (quelle relative all’attività giornalistica), del 14 gennaio 2019 (quelle relative alla ricerca scientifica e statistica) e del 15 gennaio 2019 (quelle riguardanti le attività investigative e l’archiviazione ai fini storici). Tuttavia, le regole deontologiche (non previste dal GDPR) costituiscono solo un *ponte* verso i più omogenei (a livello europeo) codici di condotta. Infatti, lo stesso art. 20 prevedeva (e prevede) che, entro il 19 marzo 2019, le associazioni e gli altri organismi rappresentanti le categorie interessate avrebbero dovuto presentare all’attenzione del Garante italiano i rispetti codici di condotta e che la loro procedura di approvazione sarebbe durata, al massimo, ulteriori sei mesi.

Purtroppo, il termine del 19 marzo non si è potuto rispettare visto che, come si diceva, l’EDPB

non ha concluso per tempo la necessaria divulgazione delle relative linee guida finalizzate a definire criteri uniformi per la redazione e l'approvazione dei codici di condotta.

Cosa sono i codici di condotta

I codici di condotta costituiscono uno strumento messo in campo dal legislatore europeo per indurre le associazioni di titolari (o responsabili) del trattamento a definire un **quadro di comportamenti omogenei**, diretti alla corretta applicazione del GDPR per specifici trattamenti di dati personali. L'esempio più classico, peraltro non nuovo nel contesto italiano, riguarda la nozione di *dato aggregato* (quindi anonimo e fuori dal campo di applicazione del GDPR) nell'ambito di ricerca statistica: quando un insieme di valori assunti da variabili statistiche può definirsi aggregato? La risposta (presente nelle regole deontologiche tutt'ora in vigore) è che viene considerato aggregato l'insieme di valori che *conta*, al minimo, tre unità statistiche; al di sotto di questa soglia l'insieme di valori assunti dalle variabili può condurre alla identificazione dei soggetti e, quindi, a potenziali rischi per i relativi dati personali. Questo è un esempio di elementi di interesse da inserire nei codici di condotta (nello specifico riguarda la ricerca statistica).

Un altro esempio di raggio d'azione dei codici di condotta potrà essere la definizione, in via generale, dell'applicazione del legittimo interesse come base giuridica di specifici trattamenti. Com'è noto, l'impiego di questa base giuridica richiede un test di bilanciamento che potrebbe essere utile eseguire *una volta per tutte* con l'approvazione del Garante.

Quindi, si tratta di un'autoregolamentazione *sorvegliata* (perché approvata dall'autorità di controllo) da parte delle associazioni qualificate di titolari (o di responsabili): l'adesione ai codici di condotta e la relativa applicazione dimostrano che il titolare ha adeguato il proprio comportamento ai fini della protezione dei dati personali.

Chi prende l'iniziativa

L'iniziativa per l'elaborazione di un codice di condotta viene assunta da associazioni o organismi che rappresentano un insieme *qualificato* di soggetti omogenei (p.e. organismi rappresentanti delle imprese edili, associazioni delle società di igiene ambientale, ecc.). Le linee guida specificano che chi elabora il codice di condotta deve essere **qualificato**, cioè deve dimostrare la rappresentatività (che l'autorità di controllo verificherà) attraverso alcuni indicatori: la percentuale di membri aderenti rispetto al totale dei soggetti che rientrano nella categoria e la durata dell'esperienza nel settore che si vuole rappresentare.

Per rafforzare la significatività del codice di condotta, l'associazione deve dimostrare di averlo preliminarmente sottoposto ad esame (consultazione) da parte di tutti i portatori di interesse. In particolare, il codice deve accogliere integrazioni e modifiche proposte sia dagli associati (che svolgeranno il ruolo di titolari o responsabili del trattamento) sia dai soggetti di cui si tratteranno i dati personali (interessati).

Ogni codice di condotta, inoltre, deve avere una struttura minima rilevabile dal paragrafo 2

dell’**art. 40 del GDPR**, definendo:

a) il trattamento corretto e trasparente dei dati;
b) i legittimi interessi perseguiti dal responsabile del trattamento in contesti specifici;
c) la raccolta dei dati personali;
d) la pseudonimizzazione dei dati personali;
e) l'informazione fornita al pubblico e agli interessati;
f) l'esercizio dei diritti degli interessati;
g) l'informazione fornita e la protezione del minore e le modalità con cui è ottenuto il consenso dei titolari della responsabilità genitoriale sul minore;
h) le misure e le procedure di cui agli articoli 24 e 25 e le misure volte a garantire la sicurezza del trattamento di cui all'articolo 32;
i) la notifica di una violazione dei dati personali alle autorità di controllo e la comunicazione di tali violazioni dei dati personali all'interessato;
j) il trasferimento di dati personali verso paesi terzi o organizzazioni internazionali; o
k) le procedure stragiudiziali e di altro tipo per comporre le controversie tra titolari del trattamento e interessati in materia di trattamento, fatti salvi i diritti degli interessati ai sensi degli articoli 77 e 79.

In ogni caso, le linee guida, nell’Allegato 3, presentano una check?list per arrivare ad una elaborazione corretta del codice e ad avviare un corretto iter di approvazione.

Chi decide sul codice di condotta

L’associazione che predispone la bozza di codice di condotta potrà essere **nazionale o internazionale** (comprendendo associati presenti in più Paesi membri dell’UE). Nel primo caso il codice opererà, qualora approvato, solo nell’ambito di un Paese mentre, nel secondo caso, avrà valore transnazionale. Questa differenza incide molto sull’iter di approvazione e, quindi, su chi concretamente decide sul codice.

Quando il codice di condotta intende operare solo a livello nazionale, l’iter di approvazione riguarda solo l’autorità di controllo del singolo paese (detta CompSA che, sul territorio italiano, è il Garante per la Protezione dei Dati Personali).

Se il codice di condotta intende operare a livello transnazionale, l’associazione lo presenta in bozza all’autorità di controllo competente per la nazione dove ha sede legale (CompSA). Tuttavia, la CompSA non decide da sola ma deve coinvolgere, in prima battuta, tutte le altre autorità competenti dei Paesi nei quali il codice intende operare affinché possa avviarsi una cooperazione volta a verificare che il codice non confligga con specifiche disposizioni normative nazionali. L’ultima parola, in ogni caso, spetta al Comitato Europeo per la Protezione dei Dati (EDPB) che esprime un’opinione formale rispetto alla bozza di codice e determina l’eventuale approvazione o la modifica da parte della CompSA. In caso di approvazione di un codice transnazionale la Commissione Europea fornirà la corrispondente decisione dandone opportuna pubblicità legale nell’ambito della Gazzetta Ufficiale Europea.

Chi controlla l’applicazione del codice di condotta

All’interno della bozza del codice di condotta le associazioni proponenti devono specificare chi è l’organismo che ne verificherà l’applicazione nell’ambito degli associati. Tale organismo, disciplinato dall’**art. 41** del GDPR, deve essere preventivamente accreditato dall’autorità di controllo competente. Le linee guida dedicano a questo aspetto un apposito capitolo che è utile soprattutto alle autorità di controllo per procedere al preventivo accreditamento di questi soggetti. Ai soggetti che si proporranno per l’accreditamento e per il successivo controllo dell’applicazione dei codici di condotta vengono richieste:

- indipendenza e assenza di conflitti di interesse;
- esperienza nell’attività di verifica dell’efficacia delle misure tecniche e organizzative adottate;
- organizzazione significativa e strutturata in grado di adempiere allo scopo (soprattutto quando il codice di condotta è transnazionale);
- capacità di risolvere eventuali situazioni di conflitto derivanti dall’applicazione dei codici di condotta, anche attraverso un proficuo rapporto con l’autorità di controllo.

Come si evolve il codice di condotta

Il GDPR è una normativa che induce titolare e responsabile all’applicazione del classico **ciclo di Deming: Plan?Do?Check?Act**. Questo vuol dire che la compliance alla normativa non è raggiunta una volta per tutte ma che è necessario prevedere procedure che consentano l’adeguamento dei comportamenti al mutare del contesto del trattamento.

Per questo, anche i codici di condotta devono prevedere specifici meccanismi per la loro revisione che coinvolgano gli associati, gli interessati e l’organismo accreditato che ne sorveglia l’applicazione. Senza la definizione di queste specifiche procedure, il codice di condotta non ha alcuna speranza di poter essere approvato.

Conclusioni

I codici di condotta, quindi, costituiscono un’occasione da cogliere per dare all’applicazione del GDPR una concretezza che molti operatori economici, soprattutto quelli più piccoli, cercano da tempo. Le linee guida dell’EDPB costituiscono un passo importante rispetto all’obiettivo di fare chiarezza nei percorsi di adeguamento e, soprattutto, di diffusione della cultura della protezione dei dati personali.

Note:

[i] https://www.ictsecuritymagazine.com/articoli/la-privacy-e-la-regolazione-multilivello/

[ii]

https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-20190219_guidelines_coc_public_consultation_version_en.pdf

Articolo a cura di **Francesco Maldera**