RAPPORTO CON GLI ENTI

Privacy, opportuna la divisione tra chi accredita, certifica e controlla

di Rosario Imperiali

Il regolamento generale sulla protezione dei dati personali, cosiddetto Gdpr(regolamento Ue 2016/679), incentiva l'istituzione di meccanismi di certificazione della protezione dei dati «allo scopo di dimostrare la conformità al...regolamento (stesso ndr) dei trattamenti effettuati dai titolari del trattamento e dai responsabili» (articolo 42.1). «La certificazione è volontaria e accessibile tramite una procedura trasparente» (articolo 42.3) ma «lascia impregiudicati i compiti e i poteri delle autorità di controllo competenti» (articolo 42.4). Ciò significa che il rilascio della certificazione Gdpr offre una mera presunzione relativa di conformità che sia il Garante sia l'autorità giudiziaria sono libere di valutare. Inoltre «la certificazione...è rilasciata dagli organismi di certificazione...o dall'autorità di controllo competente in base ai criteri approvati da tale autorità di controllo competente» (articolo 42.5).

Le competenze

La formulazione dell'articolo 42.5 prevede che il potere di rilasciare la certificazione sia riconosciuto alternativamente all'organismo di certificazione accreditato o all'autorità di controllo competente. Analoga disposizione è contenuta nell'articolo 43 del Gdpr in merito al fatto che il potere di accreditamento previsto sia in capo a uno oppure a entrambi gli organismi: dell'Autorità di controllo competente (nel caso dell'Italia, il Garante); dell'organismo nazionale di accreditamento (per l'Italia, Accredia).

Una prima considerazione evidenzia come le formulazioni del Gdpr circa le competenze in materia di certificazione nulla innovano nella parte in cui stabiliscono la potenziale competenza:

• per l'accreditamento, in capo all'organismo nazionale di accreditamento;

• per la certificazione, in capo all'ente di certificazione accreditato (si veda il regolamento 765/2008).

Viceversa, la novità giuridica sembra sussistere unicamente laddove tali competenze vengono riconosciute per la prima volta all'Autorità di controllo competente.

I criteri per la scelta

Mentre la formulazione dell'articolo 42 non dice nulla riguardo alle modalità di opzione di questa alternativa, la previsione dell'articolo 43 rimette la scelta del soggetto legittimato all'accreditamento, secondo una delle opzioni indicate nel regolamento e fondate su un regime di competenze concorrenti. Entrambe le formulazioni adottate sollevano il quesito della natura discrezionale o meno di tale scelta: vale a dire se lo Stato sia libero di decidere secondo una discrezionale valutazione propria oppure se tale decisione debba tener conto di talune considerazioni di principio, come quella di una tendenziale sussidiarietà delle opzioni possibili secondo un preciso ordine logico.

Dall'impostazione generale degli articoli 42 e 43 sembra potersi dedurre che il legislatore comunitario, nell'introduzione e gestione dell'istituto della certificazione Gdpr, abbia inteso fare affidamento al vigente sistema di accreditamento degli organismi di certificazione presente nei diversi Stati membri. Tale volontà viene anche ribadita dal

richiamo operato al regolamento Ue 765/2008 e alla norma En-Iso/Iec 17065/2012, contenuto all'articolo 43, paragrafo 1, lettera b).
Orbene, il regolamento 765/2008 stabilisce chiaramente i principi generali in materia di accreditamento prevedendo che, allo scopo, «ciascuno Stato membro designa un unico organismo nazionale di accreditamento» (articolo 4.1); per l'Italia questo è avvenuto con il decreto interministeriale 22 dicembre 2009 che dà attuazione all'articolo 4 della legge 99/2009 (cosiddetta legge sviluppo) individuando in Accredia l'organismo nazionale.
Sempre il regolamento 765/2008 fornisce una prima possibile risposta alle motivazioni che potrebbero essere alla base regime opzionale previsto in questo ambito dal Gdpr. Precisa il regolamento 765/2008, infatti, che «lo Stato membro che ritenga che, dal punto di vista economico, non abbia senso o non sia sostenibile avere un organismo nazionale di accreditamento o fornire certi servizi di accreditamento ricorre, quanto più possibile, all'organismo nazionale di accreditamento di un altro Stato membro» (articolo 4.2). Ciò significa che il Gdpr ha formulato la previsione dell'alternatività o cumulabilità degli enti preposti all'accreditamento "privacy" (Garante/Accredia per l'Italia) in ragione del fatto che possono esservi Stati membri dell'Unione che decidono di non avere organismi nazionali di accreditamento oppure che tali organismi, pur se esistenti, non prestino servizi del tipo di quelli previsti dal Gdpr.
Nel caso, invece, l'organismo nazionale di accreditamento sia presente e sia in grado di svolgere i servizi preventivati dal Gdpr, non sembra dubbio che esso sia l'ente maggiormente titolato a svolgere la funzione di accreditamento degli organismi di certificazione e che questi ultimi siano, a loro volta, quelli più funzionali al rilascio delle certificazioni. Questa osservazione deriva dalla natura stessa dell'organismo di accreditamento nonché dalla struttura concepita dal legislatore per il sistema di valutazione delle conformità. Quanto al primo punto, la norma europea obbliga gli organismi di accreditamento a istituire e gestire «strutture atte a garantire la partecipazione effettiva ed equilibrata di tutte le parti interessate» per conseguire quel «giusto rapporto fra la responsabilizzazione e il contributo di professionalità dei soggetti privati a vario titolo interessati e il necessario controllo pubblico di un'attività che deve garantire consumatori e utenti» (fonte Mise).

Autonomia e indipendenza

Questa "partecipazione effettiva ed equilibrata" mancherebbe nell'ipotesi dell'adozione di altre soluzioni in quanto si verrebbe a far intervenire in questo ambito, in funzione surrogatoria, enti concepiti per ben altri compiti.
Il sistema di valutazione delle conformità si fonda su una struttura gerarchico-piramidale composta da entità diverse tra loro autonome e indipendenti: l'ente accreditatore; l'organismo di valutazione; il soggetto da certificare. Indipendenza e terzietà di ciascuna di tali parti rappresentano requisiti essenziali per la corretta affidabilità del sistema, considerato che l'affidabilità è l'altra faccia della natura volontaria del medesimo sistema.
L'ente accreditatore è indipendente e terzo, cioè diverso dall'organismo di valutazione e quest'ultimo è, a sua volta, indipendente e terzo rispetto al soggetto da certificare.
Proprio questi requisiti essenziali di terzietà e indipendenza consentono di poter affermare che «l'accreditamento fa parte di un sistema globale, che comprende la valutazione della conformità e la vigilanza del mercato, concepito al fine di valutare e garantire conformità alle norme applicabili.» [Considerando (8) del regolamento 765/2008].

Per questo il legislatore comunitario ha ritenuto di dover intervenire con il regolamento 765/2008 al fine di «elaborare un quadro generale per l'accreditamento e stabilire a livello comunitario i principi per la sua gestione e organizzazione» [Considerando (10)]. E' giusto, quindi, che anche il sistema di accreditamento Gdpr si attenga alle norme di legge europee in ambito.

L'indipendenza dell'ente accreditatore e dell'organismo di valutazione è prescritta da diverse norme del regolamento 765/2008, così come riguardo al requisito della terzietà, nello stesso regolamento si legge:

• «le responsabilità e i compiti dell'organismo nazionale di accreditamento sono chiaramente distinti da quelli di altre autorità nazionali.» (articolo 4.6)

• «l'organismo nazionale di accreditamento non offre o fornisce attività o servizi forniti dagli organismi di valutazione della conformità» (articolo 4.8)

• «gli organismi nazionali di accreditamento non sono in concorrenza con gli organismi di valutazione della conformità.» (articolo 6.1)

• «Gli organismi nazionali di accreditamento controllano gli organismi di valutazione della conformità ai quali hanno rilasciato un certificato di accreditamento.» (articolo 5.3).

I rischi operativi

L'alterazione del delicato equilibrio assicurato dalle disposizioni del regolamento 765/2008 - determinata da una implementazione letterale e non ragionata del disposto degli articoli 42 e 43 del Gdpr - potrebbe condurre a paradossi e a rischi di impraticabilità operativa di questo importante strumento di regolazione volontaria a supporto dei contenuti prescrittivi del Gdpr. Si pensi, ad esempio, a quanto evidenziato nel workshop Fablab tenutosi a Bruxelles il 26 luglio 2016 e organizzato dal Gruppo di lavoro dell'articolo 29, con la partecipazione di 40 rappresentanti delle Autorità di controllo nazionali. In quell'occasione, destinata a una generale riflessione su aspetti pratici e operativi emergenti dall'applicazione del Gdpr, nell'affrontare il tema della certificazione veniva evidenziato che «whether a DPA should do both, accredit and certify was subject to controversy. A conflict of interest was identified as impediment».

E il conflitto di interesse o paradosso può risiedere proprio nella mancanza di quell'alterità di posizioni soggettive che connota il sistema delle valutazioni di conformità e che, al contrario, verrebbe a cancellarsi qualora si optasse per un modello di certificazione in cui accreditatore, organismo di certificazione, fonte dei criteri integrativi e verificatore della sussistenza dei requisiti di accreditamento, si concentrassero nell'unica, onnivora entità dell'Autorità di controllo nazionale. L'assenza di terzietà verrebbe a caducare quel fisiologico sistema di “check and balance” esistente tra ente di accreditamento, organismo di certificazione e soggetto richiedente la certificazione.

Analogamente, è facile prevedere che non poco sarebbe il disagio per un imprenditore nell'aprirsi alla consulenza del Garante in veste di organo di certificazione, essendo consapevole che quello stesso organo è deputato all'irrogazione di pesanti sanzioni in caso di accertate violazioni.

In conclusione, lo stesso Fablab pone come elemento di riflessione il seguente interrogativo: «what happens if a DPA acts as a certifier and the project fails (potential conflict resulting from DPAs being competent for certification and supervisory tasks)?».

Le considerazioni fin qui rappresentate portano a concludere che la scelta dello Stato membro in merito alle competenze per l'accreditamento e per il rilascio delle certificazioni

Gdpr andrebbe orientata sulla falsariga di quanto già previsto dal regolamento 765/2008, con il rinnovato riconoscimento della competenza dell'organismo nazionale di accreditamento per l'accreditamento degli enti certificatori e la competenza di questi ultimi per il rilascio dei certificati di conformità.