GDPR perché certificarsi - La vera ragione economica e il fenomeno della selezione avversa

Date : 25 gennaio 2018

Le certificazioni previste dall'art.42 del GDPR e gli organismi di certificazione art.43 sono specifiche previsioni normative che il GDPR introduce nell'ultima Sezione del Capo IV dedicato alle figure titolari del trattamento e responsabili del trattamento. Il posizionamento della sezione relativa alle certificazioni in coda al Capo IV, è di per sé indicazione della maggiore rilevanza che il legislatore attribuisce alle tematiche introdotte nelle precedenti quattro sezioni: Obblighi generali, Sicurezza dei dati personali, Valutazione d'impatto sulla protezione dei dati e consultazione preventiva, Responsabile della protezione dei dati (DPO).

Al fine di non alimentare ambiguità o indurre false aspettative è bene precisare da subito che **ad oggi nessuno può rilasciare certificazioni, bollini, marchi o sigilli validi ai sensi del GPDR** né tanto meno conformemente alla legislazione privacy italiana. Non esiste, ad oggi, la possibilità di poter rilasciare alcunché, da parte di nessuno, che possa avere una qualsivoglia valenza a norma del GDPR o del Codice Privacy.

Fatta questa doverosa precisazione, analizzeremo ora cosa sono le certificazioni a norma GDPR, a cosa servono, dove risiede il beneficio delle certificazioni e perché sarebbe utile certificarsi. In questa trattazione non si affronteranno tematiche relative a certificazioni, bollini, marchi o sigilli **non conformi al GDPR** e che da tempo vengono commercializzati da società e associazioni private.

Organismi di certificazione

Gli organismi di certificazione, per poter essere accreditati in conformità all'art.43.1, devono:

- dimostrare in modo convincente all'autorità di controllo di essere indipendenti e competenti riguardo al contenuto della certificazione (art. 43.2. let. a);
- impegnarsi a rispettare i criteri di cui all'articolo 42, paragrafo 5, e approvati dall'autorità di controllo o dal comitato (art. 43.2. let. b);
- avere istituito **procedure e strutture atte a gestire i reclami relativi a violazioni della certificazione** o il modo in cui la certificazione è stata o è attuata dal titolare del trattamento o dal responsabile del trattamento e a **rendere dette procedure e strutture**

trasparenti per gli interessati e il pubblico (art.2. let. b);
- aver dimostrato in modo convincente all'autorità di controllo competente che i compiti e le funzioni da loro svolti non danno adito a conflitto di interessi;
- altre prescrizioni indicate dalla normativa.

Certificazioni

Le certificazioni ai sensi art.42 UE 2016/679 sono uno **strumento volontario** (art. 42.3), che si affianca a tutti quelli obbligatori e a quelli consigliati indicati nel regolamento; come ad esempio il *Registro delle attività di trattamento* (art. 30); strumento questo non obbligatorio in alcuni casi[1], ma del quale, vista la sua enorme rilevanza ai fini della dimostrabilità ex post della compliance, ne viene consigliata l'adozione anche nei casi in cui non sarebbe obbligatorio[2].

L'applicazione di un meccanismo di certificazione approvato può essere utilizzato come elemento (tra i tanti e non il solo) per dimostrare il rispetto degli obblighi da parte del titolare del trattamento (art. 24.3)[3].

Il semplice possesso di **una certificazione**, rilasciata a norma GDPR, **non è dimostrazione di conformità** del proprio trattamento e tanto meno della propria organizzazione, ai dettami del GDPR.

La certificazione ai sensi del GDPR **non riduce la responsabilità del titolare** del trattamento o del responsabile del trattamento riguardo alla conformità al regolamento e **lascia impregiudicati i compiti e i poteri delle autorità** di controllo competenti (art. 42.4).

Beneficio economico

La certificazione consente di poter ottenere uno **sconto sanzionatorio** in caso di accertamento di violazione. Questo rappresenta il vero beneficio economico delle certificazioni, espressamente previsto dal GDPR (art. 83.2 let. J; art. 83.4 let. b). Infatti, al momento di infliggere una sanzione amministrativa pecuniaria e fissare l'ammontare della stessa affinché questa risulti, per ogni singolo caso, effettiva, proporzionata e dissuasiva, si potrà tenere in debito conto anche dell'adesione ai meccanismi di certificazione approvati ai sensi dell'articolo 42.

Appare quindi subito evidente che il vero e più rilevante beneficio derivante dall'ottenimento di una certificazione a norma GDPR è il beneficio economico derivante dallo sconto sanzionatorio.

Ma chi è che potrebbe avere maggior interesse a poter beneficiare di uno sconto sanzionatorio? Forse chi si è più che diligentemente e responsabilmente conformato al GDPR, mettendo in atto tutti gli strumenti necessari a poterne garantire la dimostrabilità ex post, oppure tutti coloro che già sanno che molto probabilmente potrebbero incorrere in una sanzione? Evidentemente non i primi.

Selezione avversa

Questo meccanismo potrebbe portare ad una distorsione del sistema e al concretizzarsi dei fenomeni di *selezione avversa*. Si avrebbe così l'attrazione di soggetti non sempre affidabili che potrebbero perseguire anche scopi non leciti e finalizzati al perseguimento di reati. Il mescolamento di questi soggetti non affidabili con soggetti diligenti renderebbe molto difficile capire chi nel gruppo è 'buono' e chi è 'cattivo'.

Questo tipo di effetto è stato evidenziato da uno studio di Benjamin Edelman, dal titolo "Adverse selection in online 'trust' certifications and search results", che trattava del fenomeno della selezione avversa nel mercato dei certificati SSL[4].

Siti che richiedevano e ottenevano certificazioni SSL erano in realtà meno affidabili di altri e avevano più del doppio delle probabilità di non essere attendibili o addirittura dannosi rispetto ai siti non certificati.

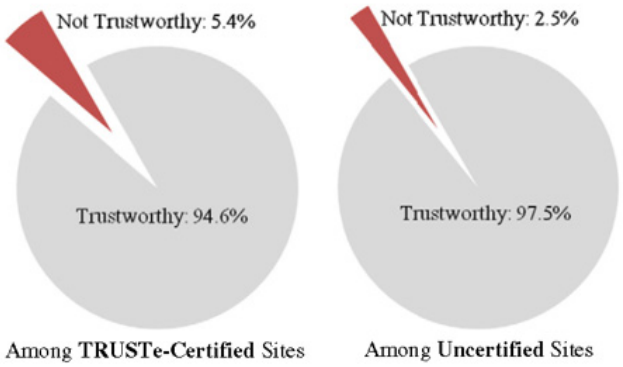

Fig. 1. Comparing TRUSTe-certified and uncertified sites.

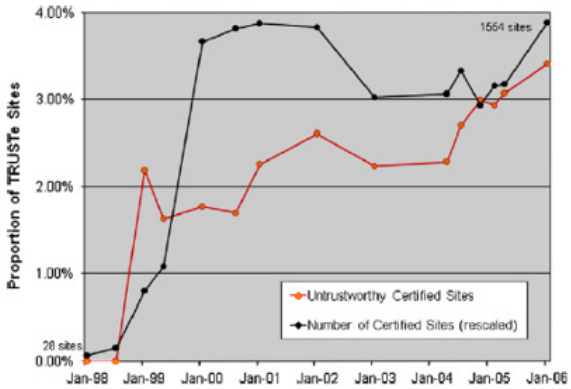

Fig. 3. Historical analysis of trustworthiness of TRUSTe-certified sites.

Sarebbe interessante realizzare a distanza di un certo tempo, esempio dodici mesi, dall'attivazione del sistema di certificazione previsto dal GDPR uno studio analogo per verificare, sulla totalità dei soggetti sanzionati dal Garante negli ultimi due-tre mesi, quale sarà la distribuzione rispetto al possesso o meno di una certificazione ex art.42 e quale sarà la distribuzione dei soggetti sanzionati in possesso di una certificazione rispetto agli organismi che tali certificazioni hanno rilasciato. Anche senza un apposito studio, questi dati li potremo certamente avere anche dalle relazioni annuali del Garante.

Risulta quindi chiaro che già dall'andamento di questo tipo di risultati si potrà avere una prima misura sulla validità e sull'efficacia del meccanismo delle certificazioni GDPR, che potrebbe a questo punto risultare già perfetto, oppure perfettibile, attraverso l'adozione di opportune azioni correttive.

Un primo accorgimento, che potrebbe migliorare l'efficacia dei meccanismi di certificazione e attenuare uno dei vari 'vizi' originari dei sistemi di certificazione, consisterebbe nel **disaccoppiare le funzioni Approvare e Vigilare** sui certificatori.

Sarà inoltre necessaria, da parte dell'autorità di controllo, attivare un'adeguata attività volta ad

effettuare anche un riesame delle certificazioni rilasciate in conformità dell'articolo 42.7, come previsto dall'art.58.1 lettera C[5]. Si evidenzia che gli eventuali controlli ispettivi da parte del Garante si svolgono anche attraverso il supporto della struttura della Guardia di Finanza guidata del Col. Marco Menegazzo, denominata Nucleo Speciale Privacy[6], che durante le proprie attività può operare avvalendosi anche del supporto degli altri reparti speciali della G.d.F[7].

Inoltre, in merito alle certificazioni, l'autorità di controllo ha tutti i poteri correttivi per revocare la certificazione o ingiungere all'organismo di certificazione di ritirare la certificazione rilasciata a norma degli articoli 42 e 43, oppure ingiungere all'organismo di certificazione di non rilasciare la certificazione se i requisiti per la certificazione non sono o non sono più soddisfatti (art.58.2 lettera h)[8].

Tutto questo dovrebbe contribuire a scoraggiare l'abitudine di alcuni soggetti, che in alcuni contesti, sono avvezzi al rilascio di certificazioni 'facili' o non veritiere, che in maniera forse un po' troppo disinvolta, sono sempre pronti a sostenere di essere in grado di giustificare il proprio operato asserendo che al momento della verifica e del rilascio tutto era conforme.

Quello che tutti dovrebbero sempre aver presente è che nel nuovo contesto della protezione dei dati personali, come previsto dal GDPR, sono in gioco e si devono proteggere e tutelare le libertà e i diritti fondamentali dei cittadini dell'UE, avendo concreta consapevolezza di cosa tutto questo implichi. Tralasciando 'cartari' e 'venditori di fumo', troppo spesso invece il GDPR viene ancora percepito e affrontato per i soli aspetti burocratici e securitari previsti dalla normativa.

Note

1. Art.30 2016/679 - "*Registri delle attività di trattamento*" - **1.** Ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità. … ...
   5. Gli obblighi di cui ai paragrafi 1 e 2 non si applicano alle imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10.
2. Per estratto dalla *'Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali' del Garante - "*La tenuta del registro dei trattamenti non costituisce un adempimento formale bensì parte integrante di un sistema di corretta gestione dei dati personali. Per tale motivo, si invitano tutti i titolari di trattamento e i responsabili, a prescindere dalle dimensioni dell'organizzazione, a compiere i passi necessari per dotarsi di tale registro e, in ogni caso, a compiere un'accurata ricognizione dei trattamenti svolti e delle rispettive caratteristiche – ove già non condotta.
   URL: http://www.garanteprivacy.it/approccio-basato-sul-rischio-e-misure-di-accountability-responsabilizzazione-di-titolari-e-responsabili, ultima consultazione 02/01/2018.
3. Art. 24 com. 3 GDPR - Responsabilità del titolare del trattamento – 3. L'adesione ai

codici di condotta di cui all'articolo 40 o a un meccanismo di certificazione di cui all'articolo 42 può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento.

4. Edelman, B. Adverse selection in online ‘‘trust” certifications and search results. Electron. Comm. Res. Appl. (2010),
   URL: http://www.benedelman.org/publications/advsel-trust-se.pdf, ultima consultazione 02/01/2018.
5. GDPR - CAPO VI - Autorità di controllo indipendenti - Sezione 2 - Competenza, compiti e poteri - Art. 58 - "Poteri" **- 1.** Ogni autorità di controllo ha tutti i poteri di indagine seguenti:
   ...
   c) effettuare un riesame delle certificazioni rilasciate in conformità dell'articolo 42, paragrafo 7;
   …
   ”
6. http://www.gdf.gov.it/chi-siamo/organizzazione/compiti-istituzionali/privacy, ultima consultazione 02/01/2018.
7. http://www.gdf.gov.it/chi-siamo/organizzazione/reparti/reparti-operativi/reparti-speciali, ultima consultazione 02/01/2018.
8. GDPR - CAPO VI - Autorità di controllo indipendenti - Sezione 2 - Competenza, compiti e poteri - Art. 58 – "Poteri" - “ … **2.** Ogni autorità di controllo ha tutti i poteri correttivi seguenti:
   h) revocare la certificazione o ingiungere all'organismo di certificazione di ritirare la certificazione rilasciata a norma degli articoli 42 e 43, oppure ingiungere all'organismo di certificazione di non rilasciare la certificazione se i requisiti per la certificazione non sono o non sono più soddisfatti; ...”
9. ‘cartari e venditori di fumo’ - tutti coloro, aziende e consulenti, che vedono nel GDPR un mero adempimento burocratico e ritengono che sua attuazione possa avvenire attraverso la sola realizzazione di documentazione formale, anche se poi tale documentazione non trova riscontro nella realtà fattuale dell’azienda.

Bibliografia

1. G.Daquisto – M. Naldi, Big data e privacy by design. Anomizzazione Pseudoanomizzazione Sicurezza, Giappichelli, Torino, 2017
2. Regolamento (UE) 2016/679, http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ITA&toc=OJ:L:2016:119:TOC , ultima consultazione 02/01/2018.

A cura di: **Stefano Luca Tresoldi**