Il concetto di Accountability e il suo ruolo nel GDPR -

https://www.agendadigitale.eu/sicurezza/principio-di-accountability-nel-gdpr-significato-e-applicazione/

Luglio 2018

All'articolo 5 comma 2 nella versione in lingua inglese del GDPR si rinviene il concetto di Accountability come criterio guida del GDPR. In italiano è stato tradotto con il termine "responsabilizzazione" ma il concetto non è chiaramente interpretabile solo come "responsabilità". Sarebbe molto limitativo e non pienamente conforme all'approccio voluto invece dal Legislatore del Regolamento. Il termine inglese "accountability" (responsabilità) proviene dal mondo anglosassone, dove è di uso comune e viene utilizzato nel mondo della finanza, della revisione dei conti e in altri settori specifici. Non vi è dubbio che risulta complesso definire che cosa esattamente significhi "accountability" in pratica. Sono diverse le declinazioni di questo termine nei vari ambiti. Nella maggior parte delle altre lingue europee, principalmente a causa delle differenze tra i sistemi giuridici, il termine "accountability" non è facilmente traducibile. Da un punto di vista lessicale il termine in questione è una parola composta. Il verbo to account è traducibile in italiano come "dar conto". Il sostantivo "ability" significa "essere in grado di" o "avere attitudine a". Il problema è che il termine è vago (anche Responsabilizzazione lo è) per capire cosa significa bisogna intendersi bene. Lo si potrebbe tradurre con "rendicontabilità" ma anche su questo termine potrebbero sorgere ipotesi e teorie interpretative.

Di conseguenza, il rischio di un'interpretazione variabile del termine, e quindi di una mancanza di armonizzazione, è sostanziale. Altri termini che sono stati suggeriti per rendere il senso di "accountability" sono: "reinforced responsibility" (responsabilità rafforzata), "assurance" (assicurazione), "reliability" (affidabilità), "trustworthiness" (attendibilità) e, in francese, "obligation de rendre des comptes" (obbligo di rendere conto) e altri ancora. Non vi è dubbio però che nell'ambito della tutela e protezione dei dati personali il concetto di accountability assume un ruolo fondamentale, la chiave di lettura e di interpretazione sul giusto comportamento che il titolare del trattamento deve adottare da adottare davanti ad un quesito, ad un problema, al dubbio sul corretto processo organizzativo o tecnico alla base di un trattamento dei dati.

Nella letteratura in lingua inglese sulla misurazione e sulla gestione della performance i due termini Responsabilità e Accountability non sono esattamente equivalenti.

Il concetto di "responsibility" è legata al dover agire. All'obbligo di

Il concetto di "accountability" è legato al rendere conto dell'azione fatta o fatta fare, al rispondere e al rendere conto dei risultati ottenuti, delle cose fatte (fatte bene e fatte male).

In italiano entrambi vengono tradotti con un unico termine: "responsabilità" in quanto "accountability" non ha un termine diretto equivalente nella nostra lingua. Lo stesso avviene per i due aggettivi collegati: "responsible" ed "accountable" che sono tradotti entrambi con il termine "responsabile".

Personalmente mi piace tenere distinti i due concetti e quindi mantenere in italiano il termine inglese "accountability" senza tradurlo.

Deve essere sottolineato che l'accountability ha assunto un ruolo centrale anche nell'economia delle amministrazioni pubbliche. Il problema dell'accountability, e del "rendere conto" delle scelte operate, si pone ogni volta che si utilizzano risorse "non proprie" per svolgere determinate attività e pensiamo per esempio ai soldi pubblici. Nonostante la centralità dell'accountability, questo tema non è stato ancora studiato a sufficienza sotto il profilo teorico e pratico; essa è al centro degli studi e delle strategie di riforma del management pubblico a livello internazionale e oggi, nella maggior parte dei Paesi, si stanno sviluppando dei sistemi di accountability orientati ad una logica di performance. Un'analisi compiuta da soggetti qualificati ha consentito di giungere ad una conclusione che accomuna le esperienze di ben 97 paesi: le nuove forme di accountability contribuiscono a migliorare l'efficacia e l'efficienza delle amministrazioni pubbliche. Non vi è dubbio che lo scopo del GDPR con l'Accountability è lo stesso rispetto alla protezione dei dati: porre l'Accountability come "un faro nella notte" al fine di fornire la chiave di lettura rispetto a certe situazioni di criticità.

Perché non è sufficiente tradurre Accountability con Responsabilità e/o Responsabilizzazione ? Perché il termine è più vicino al concetto di Rendicontazione di cui la "responsabilizzazione" è solo uno degli aspetti. Il punto fondamentale del concetto di Accountability è in realtà posto sulla dimostrazione di come viene esercitata la responsabilità e sulla sua verificabilità. La responsabilità e l'obbligo di rendere conto sono due facce della stessa medaglia ed entrambe sono elementi essenziali di una buona governance e di un buon modo di rispondere ai problemi che derivano dal trattamento dei dati. Solo quando si dimostra (ovvero si è in grado di

rendicontare) "come" e "in che modo" si è provveduto a gestire quel problema il concetto di "responsabilizzazione" e della conseguente "Responsabilità" funziona effettivamente ed in concreto.

Si potrebbe dire che per "Accountability" ci si deve riferire piuttosto ad un atteggiamento proattivo ovvero a saper anticipare e agire in anticipo per far fronte ad un'azione futura e saperlo rendicontare.

L'approccio proattivo è forse il modo migliore di risolvere il tema del "Essere Accountable" richiesto dalla norme regolamentari. Già nel Parere del Gruppo dei 29 (3/2010 - WP 173) sul principio di responsabilità adottato il 13 luglio 2010 si parlava di accountability nell'ambito della terminologia utilizzata per declinare il principio della responsabilità nel settore della protezione dei dati. Essere proattivi è in fondo lo stesso atteggiamento che un'altra norma già presente nel DLgs n. 196/2003 richiedeva e imponeva con l'art. 15 e che oggi, nel regolamento sembra essere presente nell'art. 5: l'aver fatto e il poter dimostrare di aver fatto tutto il possibile per evitare il danno. Essere proattivi è il necessario atteggiamento da adottare per non rispondere in futuro di un danno derivante da trattamento dei dati personali attraverso la dimostrazione (inversione dell'onere della prova) di aver fatto tutto il possibile per evitarlo. Tale atteggiamento è richiesto al titolare del trattamento dei dati dalle norme regolamentari (es: data breach, misure adeguate di sicurezza) proprio nella fase privacy by design. Anche nelle successive fasi dell'analisi dei rischi, quando il danno è solo un ipotesi da prevedere, occorre anche in questa fase saper agire in anticipo per far fronte ad una situazione futura anche solo possibile, ipotetica,

probabile. Significa avere il controllo e far accadere le cose piuttosto che adattarsi a una situazione o attendere che qualcosa accada per poi porvi rimedio.

Responsabilizzarsi non è certamente l'aver adempiuto soltanto agli obblighi di legge. Vuol dire avere un atteggiamento proattivo che non si esaurisce nel semplice adempimento normativo (conformità delle attività di trattamento con il regolamento come reca il considerando 74) e nel dare prova solo di questo adempimento ma ad esempio, come richiamato dalla norma del considerando 74, anche "dimostrare l'efficacia delle misure", rendicontare come si è proceduto e con quali metodologie a definire le misure di sicurezza. Anche in caso di violazione tale atteggiamento, se correttamente rendicontato, può determinare ex art. 83 del GDPR da parte dell'Autorità di controllo nel calcolo e nella dosimetria della sanzione eventualmente da applicare, una condizione di favore in capo al titolare che ha saputo attenuare i rischi fino ad un certo limite (qui poi entra in gioco il superamento del limite stesso e l'eventuale punibilità)e l'ha saputo dimostrare.

Sull'Enciclopedia Treccani, il termine Accountability è definito come Responsabilità incondizionata, formale o non, in capo a un soggetto o a un gruppo di soggetti (accountors), del risultato conseguito da un'organizzazione (privata o pubblica), sulla base delle proprie capacità, abilità ed etica. Tale responsabilità richiede giudizio e capacità decisionale, e si realizza nei confronti di uno o più portatori di interessi (account-holders o accountees) con conseguenze positive (premi) o negative (sanzioni), a seconda che i risultati desiderati siano raggiunti o disattesi. L'accento non è posto sulla responsabilità delle attività svolte per raggiungere un determinato risultato, ma sulla definizione specifica e trasparente dei risultati attesi che formano

le aspettative, su cui la responsabilità stessa si basa e sarà valutata. La definizione degli obiettivi costituisce, dunque, un mezzo per assicurare l'accountability. Con il concetto di responsabilità, l'accountability presuppone quelli di trasparenza e di compliance. La prima è intesa come accesso alle informazioni concernenti ogni aspetto dell'organizzazione e dei processi metodologici del Modello privacy. La seconda si riferisce al rispetto delle norme ed è intesa sia come garanzia della legittimità dell'azione sia come adeguamento dell'azione agli standard stabiliti da leggi, regolamenti, linee guida etiche o codici di condotta. Sotto questi aspetti, l'Accountability può anche essere definita come l'obbligo di spiegare e giustificare il proprio comportamento per adempiere al meglio agli obblighi previsti dalla normativa Regolamentare privacy (GDPR) e dalla normativa nazionale in materia (decreti legislativi e norme di settore).

Nel campo della governance ci si potrebbe riferire all'obbligo per un soggetto di rendere conto delle proprie decisioni e di essere responsabile per eventuali danni cagionati a causa della mancata (o scarsa) capacità di anticipare e prevenire (o attenuare) un evento prevedibile. Ma ci si potrebbe riferire anche, in assenza di danni e in caso di controlli dell'Autorità di controllo, all'aver applicato misure di sicurezza non adeguate al rischio calcolato o non aver saputo rendicontare la propria attività e di conseguenza dimostrare di aver fatto tutto il possibile per (provare a) evitare quel danno.

Nell'ambito della sicurezza informatica, l'accountability è anche la capacità di un titolare attraverso il proprio Modello privacy di dimostrare attraverso l'audit delle tracce e dal sistema di autenticazione (login) di aver adempiuto agli obblighi previsti

dalla normativa in modo sufficientemente anticipatorio di possibili eventi dannosi o critici. Di aver previsto misure organizzative e tecniche rapportate al caso concreto del trattamento ma in grado di essere adatte e adeguate ad una serie sufficientemente ampia di rischi calcolati. Il criterio interpretativo del nesso è sempre ex ante in concreto e mai ex post. Nessuna norma e non certo il criterio di cui parliamo può spingersi fino a dover dimostrare l'impossibile, il caso fortuito o la forza maggiore o l'evento raramente verificabile. Come in ogni cosa occorre approcciarsi al concetto anche con un po' di buon senso per evitare che la soglia di anticipazione, di previsione e di rendicontazione retroceda all'infinito e diventi impossibile o quasi.

Saper anticipare il verificarsi di situazioni critiche, l'accadimento di eventi rischiosi possibili o molto probabili e trovare soluzioni che, ex ante in concreto, forniscano un certo margine di sicurezza, significa forse essere accountable. Vedremo cosa accadrà nel prossimo futuro quando arriveranno i primi pronunciamenti dell' Autorità di controllo europea e degli stati membri. Il concetto di responsabilizzazione e di accountability e' senza alcun dubbio, piaccia o no, una delle sfide più importanti e decisive che ci pone davanti l'attuale normativa sulla protezione dei dati personali.

Roma agosto /settembre 2018