I MANUALI DELLA PRIVACY

Stefano Gorla, Michele Iaselli, Giuseppe Tacconi
Prefazione a cura di Gianluca De Vincentiis

GLI AUDIT PRIVACY

SECONDO IL NUOVO REGOLAMENTO EUROPEO GDPR 2016/679

Guida pratica per la verifica della protezione dei dati

ITER®

Indice

Prefazione (Gianluca De Vincentiis)

Cos'hanno in comune tra loro le parole Privacy ed Audit? E come mai persone di estrazione professionale diversa si sono ritrovati a scrivere un libro in comune?

Sono queste le prime domande che mi sono posto quando gli autori di questo libro mi hanno chiesto la cortesia di un'opinione ed una introduzione al loro lavoro. Tre professionisti affermati nel loro ambito con i quali ho avuto il piacere ed il vantaggio di lavorare, vederli all'opera e di sviluppare anche un'amicizia personale.

La mia formazione professionale mi porta ad associare immediatamente la parola *Privacy* al complesso delle norme che regolano la tutela e l'utilizzo dei dati personali, mentre la parola *Audit*, sempre nella mia esperienza, risulta essere l'attività (intervista) tesa alla raccolta di evidenze oggettive per una valutazione indipendente e quanto più obiettiva di conformità ad una regola nota e condivisa, tra chi conduce l'audit e chi deve fornire i riscontri richiesti.

Mentre leggevo il testo altre domande si aggiungevano alle prime, ed in particolare una è rimasta sempre latente sino alla fine della lettura, quando poi si è palesato in modo chiaro ed evidente la giustezza della loro intuizione di scrivere in comune un libro così impegnativo: *perché proprio ora?* In questa breve introduzione mi auguro di chiarire ai lettori quali sono state le mie risposte e perché mi sento di promuovere la massima diffusione di questo come di altre produzioni letterarie che trattino, purché con analoga competenza, un argomento difficile, ampio ed estremamente serio ed attuale come quello descritto sinteticamente nel titolo di questo libro.

Uno dei più noti browser internazionali sulla propria home page ha posto questo quesito ai suoi utenti: "Nel 2020 ci potrebbero essere circa 30 miliardi di dispositivi connessi a Internet. Che sensazioni ti procura questo scenario?". L'associazione di idee spontanea che mi è sorta leggendo il quesito è stato una frase celebre di uno dei fondatori della Intel, forse la più famosa società produttrice di semiconduttori al mondo che più di tutte ha tratto beneficio dallo sviluppo della tecnologia e di Internet, Andrew Stephen Grove: "Il problema più grande di quest'epoca elettronica riguarda la privacy". In effetti

sempre più il modo di comunicare, conoscere ed apprendere si sta digitalizzando ed il nostro essere parte della società spesso si configura o meglio si confonde con l'esser connessi, presenti e visibili sui social-network, o comunque sul web. La "visibilità" digitale presenta un confine molto labile tra ciò che vogliamo sia pubblico e ciò che non riusciamo a mantenere "privato". Per fortuna, questo non vale per tutte le persone e non vale in tutte le parti del nostro mondo sempre più globalizzato, ma il trend delle nostre società occidentali appare segnato da un avanzare della tecnologia estremamente più veloce della capacità degli uomini di adeguarsi ai nuovi strumenti ed alle nuove idee e possibilità che queste offrono, soprattutto per quanto riguarda la capacità di cogliere i rischi che queste novità portano con loro.

L'ignoranza verso il tecnologicamente nuovo, intesa come non-conoscenza e cioè ignorare cosa significa o cosa comporta l'uso di una nuova App o di un nuovo Social, espone tutti noi a pericoli o rischi assolutamente inattesi e tantomeno comprensibili nelle loro conseguenze. Di fronte a tutto questo, il singolo utente da solo non può gestire e proteggersi dai rischi che si conoscono e ancor di più da quelli che si sviluppano in modo imprevedibile per l'intera comunità, basti pensare alle conseguenze sulle attività che può avere il cyber-crime o alle conseguenze sociali del cyber-bullismo. Sono le organizzazioni nazionali e sovranazionali che devono farsi carico di prevedere, proteggere ed informare le persone e le attività produttive da quello che il nuovo contesto sociale o tecnologico può determinare o sta già determinando. L'esigenza di regole e di controlli sulle attività private e professionali è dunque una necessità comune assolutamente doverosa da assolvere.

Il nuovo Regolamento Europeo "GDPR" 679/2016 ha raccolto l'esigenza dell'intera comunità europea di tutelarsi in modo omogeneo e condiviso in merito a tutto ciò che riguarda il concetto alla base della privacy, e cioè il diritto alla tutela dei dati e delle informazioni della persona fisica per la salvaguardia della vita privata di ciascun individuo. Questo regolamento definisce ulteriormente rispetto a quanto già presente i diritti degli individui e le garanzie affinché questi diritti vengano tutelati da tutti coloro che possono avere a che fare

con le loro informazioni. La tutela dei diritti nasce dal controllo che tutte le possibili entità coinvolte nella gestione delle informazioni personali rispettino le regole previste dal GDPR.

Ed ecco che questo libro, in questo momento, risulta essere uno strumento assolutamente indispensabile per coloro che avranno il compito di provvedere alle verifiche di coerenza ed adeguatezza alla nuova normativa emanata ad aprile 2016. L'obbligo di cogenza è un dovere, ma anche le realtà più volenterose potrebbero incorrere in difficoltà procedurali o tecnologiche che non sono di sicuro di facile soluzione.

La capacità di condurre un audit in ambito privacy completo ed esauriente può essere una competenza sfruttabile dal professionista che si propone sul mercato sia in ambito consulenziale che in ambito di verifica da parte di enti preposti al controllo ed alla verifica. In quest'ottica la formazione di competenze sempre più qualificate deve esser vista come un'opera non solo meritoria ma assolutamente necessaria, per acquisire una metodologia chiara e ripetibile dell'attività di verifica o meglio, di audit delle realtà che devono risultare adeguate alla normativa.

La mia personale esperienza di consulente aziendale, auditor di sistemi di gestione per la sicurezza delle informazioni, e responsabile di organismi accreditati per la certificazione di persone e di sistemi di gestione, mi porta a dire che quest'opera sarà di sicuro aiuto a due tipologie di lettori:

- il singolo professionista che intende aumentare o migliorare la sua conoscenza in un ambito professionale di sicuro interesse che offrirà sicuramente moltissime opportunità nell'immediato coinvolgendo tutte le attività produttive, che avranno bisogno di figure professionali capaci e competenti nelle verifiche;
- l'imprenditore o i responsabili della compliance aziendale perché è fondamentale per loro comprendere quanto possa essere impegnativa una sessione di audit in ambito privacy, e capire di doversi rivolgere a persone qualificate che abbiano esperienza e metodo per aiutare le loro organizzazioni ad essere conformi a tutto ciò che la normativa.

La piena applicazione del regolamento europeo sulla privacy (GDPR), è prevista per il 25 maggio 2018, ed entro tale data tutte le realtà che abbiano a che fare con la gestione di dati personali dovranno essere conformi a quanto previsto dal regolamento, pena il rischio di ricevere sanzioni estremamente pesanti, in termini economici e d'immagine. Tale situazione oggettiva non rinviabile porterà al prolificare di richiesta di consulenza da parte di tutte quelle realtà che realizzeranno di non esser pronte e conformi alla normativa entro la data sopra citata, e solo coloro i quali avranno provveduto per tempo ad acquisire le giuste competenze potranno proporsi professionalmente sul mercato avendo una visione quanto più ampia e completa di quello che il GDPR richiede.

La privacy ed il rispetto dei requisiti che la nuova normativa prevede spazia in un ambito che investe contemporaneamente aspetti di giurisprudenza, conoscenze tecnologiche approfondite e modalità di verifica che solo degli esperti possono padroneggiare ed è per rispondere a questa esigenza che gli autori hanno deciso di dire la loro sugli argomenti che gli appartengono. Di sicuro un DPO (Data Protection Officer) dovrà avvalersi di esperti nel caso di grandi o specifiche realtà aziendali, ma la sua formazione non potrà prescindere dalla conoscenza di quali devono essere gli argomenti che dovrà supervisionare.

È questo insieme di considerazioni su cosa dice il nuovo regolamento europeo e su quanto di sicuro accadrà nel mercato delle aziende e dei professionisti che offriranno la loro consulenza in ambito privacy, che mi ha portato a rispondere alle domande con le quali ho esordito nella mia prefazione, ed alle quali credo, e spero, di aver risposto con le mie considerazioni.

Questo libro offre tutti gli spunti per confrontarsi con gli autori su quanto il lettore già conosce e quanto, soprattutto, non conosce ed è questo aspetto che mi ha portato a considerare opportuno il mix di competenze degli autori ed il momento particolare della loro pubblicazione.