Italia Oggi Sette Affari Legali
08-FEB-2021
da pag. 1-2
Dir. Resp.: Pierluigi Magnaschi
foglio 1 / 4
Tiratura: 0 - Diffusione: 0 - Lettori: 82000: da enti certificatori o autocertificati
Superficie: 203 %

Affari Legali

Privacy, il Gdpr la fa ancora da padrone tra gli studi

Gli adempimenti legati all'introduzione del Gdpr nell'ordinamento vedono gli studi in prima linea

Privacy, la protezione dei dati settore trainante dell'avvocatura

Sicurezza e circolazione transnazionale dei dati i fronti caldi

Pagine a cura
DI ANTONIO RANALLI

Il Gdpr continua a farla da padrona tra i settori di cui si occupano gli studi legali. La consulenza alle imprese per venire a capo degli adempimenti legati all'area privacy, imposti in Europa dal General data protection regulation (Gdpr), rappresenta infatti ormai uno dei settori di punta per molte law firm. Lo impone anche la crescita del contenzioso in materia: nell'ultimo anno, secondo quanto emerge da una recente ricerca condotta da ***Dla Piper***, sono aumentate le multe inflitte alle aziende delle autorità europee preposte alla protezione dei dati personali, per un totale di 272 milioni di euro. E la metà di queste sanzioni è stata inflitta in Italia e in Germania. Secondo la ricerca, 159 milioni di euro di queste sanzioni sono state inflitte negli ultimi 12 mesi, con un aumento di quasi il 40% rispetto ai primi 20 mesi successivi all'entrata in vigore del Gdpr. Tra i settori colpiti dalle sanzioni quelli della vendita al dettaglio, turismo, telecomunicazioni e carburanti.

Questo dimostra come sia aumentato il lavoro degli studi legali. «Seguo questa materia dal 1996. Ho visto la privacy nascere, svilupparsi e arrivare fino a oggi. Gli avvocati sono arrivati di recente a occuparsi di questa materia, che è ostica dal punto di vista del linguaggio e interdisciplinare dal punto di vista della formazione», dice **Antonio Ciccia Messina**, fondatore dello ***studio legale Antonio Ciccia Messina***. «Le categorie professionali che si sono occupate di più in passato di questa materia sono state altre, come i commercialisti e i consulenti del lavoro. Ora però il lavoro dell'avvocato è orientato a sviluppare sempre più la consulenza e non più il contenzioso. E il tema della privacy necessita di un'attività organizzativa, che è più vicina a un lavoro di assistenza. Quello che ha determinato un interesse forte da parte degli avvocati è stato sicuramente il Regolamento europeo per la protezione dei dati personali. È stato uno spartiacque. Dal 2016 in avanti gli avvocati, soprattutto i più giovani, hanno capito che questo è un settore da battere con gli strumenti della conoscenza e della professionalità tipica che l'avvocato può vantare rispetto ad altre categorie. Non per nulla la materia della protezione dei dati è citata anche nel decreto delle specializzazioni forensi. Anche se la posizione poteva essere più enfatizzata, in considerazione del carattere centrale che la privacy e il trattamento delle informazioni hanno nella vita sociale ed economica».

Per **Francesco Inturri**, partner di ***Andersen***, «nell'implementazione del Gdpr presso i clienti, la mia principale preoccupazione era quella di non riuscire a trasmettere il messaggio che la nuova normativa rappresenta, a mio avviso, un'occasione per ripensare in modo complessivo il sistema di gestione dei dati personali, non tanto per timore delle sanzioni previste dalla norma, ma bensì quale risultato di una più acuta maturità del sentimento collettivo di arginare la sempre maggiore invasione della sfera privata di ogni individuo. Con grande onestà, posso affermare di aver trovato tra i clienti una sensibilità molto alta nel raccogliere questa opportunità, oltre una propensione a immedesimarsi nell'«interessato» del trattamento, che mi hanno positivamente colpito. Credo personalmente che la maturità che ho riscontrato sia, almeno in parte, figlia del fatto che ognuno di noi, prima ancora che imprenditore, manager, lavoratore, si consideri a tutti gli effetti come un «interessato», e dunque come soggetto il cui diritto alla riservatezza possa essere potenzialmente leso in qualsiasi momento».

Il Gdpr continua a essere un elemento di novità e di studio per i legali, nonché una nuova nicchia di mercato e di opportunità soprattutto per i giovani avvocati. «La normativa comunitaria sulla privacy, infatti, ben si distacca dal vecchio impianto recepito nel dlgs 196/2003, realizzando una vera e propria «rivoluzione copernicana» relativamente all'approccio concettuale

che il titolare deve avere nel tutelare i dati personali in proprio possesso», spiega **Antonio Barberisi**, coordinatore del dipartimento «Strategia, organizzazione e marketing per studi legali» dell'***Aiga***, l'Associazione italiana dei giovani avvocati. «La maggiore novità introdotta può essere rinvenuta nel principio di accountability, che si sostanzia nell'obbligo, posto in capo ai titolari del trattamento, di valutare le informazioni in loro possesso e il loro conseguente valore, al fine di approntare le misure tecniche e organizzative che ritengono adeguate per mettere al sicuro tali dati. In altre parole, il Gdpr non indica quali soluzioni occorra adottare per proteggere i dati personali in proprio possesso, a differenza di quanto previsto nell'ormai famoso allegato B al Codice della Privacy nel quale comparivano, fra gli strumenti più significativi, l'avvio di un sistema back up organizzato, l'aggiornamento delle patch dei vari software utilizzati, l'installazione di un antivirus, l'utilizzo di password e altro».

Gli indizi che la Data Protection sarà uno dei main topic del 2021 sono sparsi un po' ovunque. «Basta una occhiata alla pagina del «Garante Privacy» che nella sola giornata del 10 dicembre scorso si è pronunciato cinque volte tra pareri e provvedimenti», dice **Lorenzo Colzi**, associate di ***Spheriens***. «Google, il 25 gennaio scorso, ha effettuato modifiche alle policy di condivisione dei dati personali degli utenti al fine di migliorare alcuni suoi servizi. Le sfide che questo anno, anche a in considerazione dello scenario pandemico attuale, ci mette di fronte dal punto di vista della data protection sono molteplici, basta pensare alla tematica del trasferimento dei dati personali extra Ue a seguito della sentenza «Schrems II» che ha invalidato la decisione di adeguatezza del Privacy Shield. A due anni dalla sua piena efficacia il Gdpr rimane un territorio di frontiera dal punto di vista giuridico e tecnico. Nonostante i vari interrogativi ancora aperti la sfida per gli studi legali rimane sempre costante: aiutare aziende ed imprenditori a trasformare il rischio di compliance Gdpr in un asset gestionale in grado di coniugare diritto, etica e business, traducendosi in un vantaggio competitivo».

Diverse le problematiche che gli studi stanno affrontando. «L'interazione della tutela dei dati con altre esigenze prioritarie proprie dell'impresa», spiega **Mario Di Giulio**, partner dello studio legale ***Pavia e Ansaldo***, «come ad esempio le tematiche relative ai sistemi dei controlli interni e alle investigazioni interne, che richiedono sempre più una vigilanza attiva da parte delle imprese, per non incorrere in responsabilità di legge (si pensi alla responsabilità amministrativa degli enti prevista dal dlgs 231/2001) e danni anche reputazionali: esigenze che devono essere comunque contemperate con la tutela dei diritti dei lavoratori e la tutela della loro privacy, nonché dei terzi. Altra problematica che sempre più siamo chiamati a risolvere è la ripartizione delle responsabilità nei casi, molto frequenti, di contitolarità dei trattamenti dati legati alla fornitura di servizi cogestiti. Altra problematica che ci impegna attivamente è quella relativa alla caduta del privacy shield con gli Usa non solo e non tanto con riferimento alla gestione dei dati diretta da parte di entità basate in tali stati, quanto per la continua interconnessione che esiste nella gestione dei dati attraverso l'intervento di soggetti fornitori di servizi accessori che spesso in un secondo o terzo livello possono poi andare a interagire con soggetti non più «scudati».

Secondo **Giuseppe Di Masi,** partner e coordinatore del dipartimento compliance di ***Sza Studio Legale***, l'esperienza professionale dell'ultimo anno «ha evidenziato la necessità di una sempre maggiore attenzione al tema della cybersecurity a tutela del patrimonio informativo aziendale. Si assiste ad un aumento esponenziale di attacchi da parte di hacker ai sistemi informatici delle imprese attraverso sempre più sofisticate e ingegnose tecniche di infiltrazione, che mettono in evidenza l'inadeguatezza dei sistemi di sicurezza. Questi attacchi sono in larga parte finalizzati ad attuare vere e proprie estorsioni ai danni delle aziende, come la cronaca documenta quotidianamente. Tale realtà denota un insufficiente adeguamento alla penetrante normativa in materia di data protection, con concreti rischi di subire l'irrogazione delle pesanti sanzioni previste dal Gdpr nonché l'avvio di azioni risarcitorie da parte delle persone i cui dati sono stati violati. Oggi la sfida rivolta all'impresa è quella di colmare un gap tecnologico ed insieme un deficit culturale nell'affronto di tali tematiche».

Da diversi anni le imprese che operano attraverso numerose entità giuridiche e in una dimensione internazionale stanno adottando processi di compliance di gruppo, che costituiscono il modo migliore per rispettare le normative di contrasto al riciclaggio e alla corruzione, così come quelle che proibiscono rapporti commerciali con determinati paesi. «A mio avviso non c'è dubbio che, nei gruppi, il rispetto della normativa sulla data protection non possa che avvenire attraverso processi di compliance centralizzati», dice **Francesco De Biasi** di ***Clearv Gottlieb***. «Ebbene, quando la compliance centralizzata comporta la condivisione di dati personali fra le diverse società di un gruppo con presenza anche al di fuori dello Spazio Economico Europeo, nuove problematiche si pongono in seguito alla sentenza c.d. Schrems II, pubblicata nel luglio 2020, con cui la Corte di Giustizia Ue ha dichiarato invalido il regime E.u-U.s Privacy Shield. Questa pronuncia non si è limitata a espungere dall'ordinamento uno degli strumenti che consentivano di trasferire dati personali dal territorio dell'Unione negli Usa, ma ha reso più problematica anche l'applicazione degli altri principali strumenti utilizzabili allo stesso fine (clausole contrattuali standard e *binding corporate rules*), imponendo al soggetto che trasferisce dati personali al di fuori dello Spazio economico europeo l'onere di verificare, ogni volta, se il diritto del paese di destinazione dei dati garantisca o meno una protezione adeguata di tali dati e, se risulti necessario in esito a tale verifica, di porre in essere misure di tutela ulteriori».

Uno dei temi più caldi della Gdpr per le prossime settimane saranno anche gli aspetti legati alla Brexit. «Perché», come spiega **Carlo Majer**, comanaging partner di ***Littler***, «i trasferimenti di dati dallo Spazio economico europeo («See») verso l'esterno, ossia il Regno Unito, sono consentiti, dopo la Brexit, solo se vengono messe in atto le opportune misure di salvaguardia. La sintesi dell'accordo Brexit, pubblicata dal governo britannico, spiega che il Regno Unito e l'Ue hanno concordato un periodo di grazia fino a sei mesi durante il quale i dati personali possono circolare liberamente dall'Ue al Regno Unito (essenzialmente mantenendo la posizione esistente prima di Brexit per altri sei mesi). Durante questo periodo, la Commissione Ue si adopererà per completare la sua determinazione di adeguatezza con il Regno Unito, che, se ottenuta, consentirebbe la libera circolazione ininterrotta dei dati personali tra Ue e Uk».Un

aspetto problematico della normativa in materia di privacy è l'applicazione del Gdpr anche a soggetti non comunitari, anche se privi di qualsiasi presenza fisica in Italia o in altri paesi Ue. «Il Gdpr può trovare applicazione anche nei confronti di entità senza alcuna presenza nell'Ue», spiega **Flavio Acerbi**, salary partner di ***Fivelex Studio legale e tributario***, «nel caso in cui queste entità trattano dati personali di soggetti residenti nell'Ue e svolgano un'«offerta di beni o la prestazione di servizi ai suddetti interessati nell'Ue». Il Gdpr ha, poi, adottato una nozione di «offerta di beni/servizi» molto ampia, che comporta sostanzialmente l'estensione della normativa comunitaria a moltissimi soggetti extra-comunitari, che rivolgano parte della propria attività nei confronti di soggetti residenti nell'Ue. Questo aspetto del Gdpr ha richiesto a molti clienti extra-comunitari, in primo luogo, di esaminare e far comprendere al proprio interno la nuova normativa e, in secondo luogo, di adattare la propria normativa interna e i propri presidi esistenti in materia di privacy - basati sulla rispettiva normativa nazionale di riferimento - ai dettami del Gdpr, nonché di aggiornare la propria contrattualistica rivolta alla clientela comunitaria».

Nell'ambito delle organizzazioni aziendali, la corretta gestione degli adempimenti in materia privacy risulta ormai indispensabile, non solo per evitare l'irrogazione di sanzioni da parte del Garante, ma anche e soprattutto, per tracciare - in un'ottica di gestione di prevenzione del rischio - i concreti pericoli derivanti da un cattivo uso degli strumenti aziendali. «In tale contesto, oltre all'adozione di un sistema tecnico-informatico compliant rispetto agli standard previsti dalla normativa di settore», spiega **Andrea Puccio**, managing partner di ***Puccio Penalisti Associati***, «gioca un ruolo essenziale anche la formazione continua dei dipendenti e collaboratori. Come noto, all'atto di assunzione al dipendente viene consegnata la policy vigente in materia di utilizzo dei device aziendali, che, dopo una rapida lettura, nel migliore dei casi viene abbandonata in fondo a un cassetto della scrivania. Gli anni passano e può accadere che il dipendente – che non ricorda più il contenuto della policy – utilizzi il computer aziendale per effettuare acquisti personali su siti internet poco sicuri e, a causa di ciò, subisca un attacco hacker, con pregiudizio di tutta la struttura informatica dell'ente».

Soprattutto nel panorama italiano, formato in gran parte da piccole e medie imprese, il Gdpr viene spesso ancora percepito come uno dei tanti obblighi burocratici che rallentano e rendono ancor più macchinoso il raggiungimento degli obiettivi imprenditoriali. «Nella nostra esperienza», dice **Giovanni Aquaro**, socio dello ***studio Lambertini&Associati***, «riscontriamo infatti che le aziende che hanno investito per adeguarsi al Regolamento lo hanno fatto principalmente al fine di evitare sanzioni che sono, come noto, anche molto importanti. Da parte nostra osserviamo invece come un serio investimento sulla protezione dei dati, qualora si accompagni ad un adeguamento, non solo formale ma, sostanziale alla normativa, porti con sé una serie di rilevanti vantaggi, anche indiretti, che vanno ben oltre agli aspetti di mera compliance e che, al contrario, migliorano l'efficienza e, in definitiva, la redditività dell'impresa. Il nostro obbiettivo è dunque quello di sensibilizzare gli imprenditori rappresentando il Regolamento come un'importante occasione per avviare progetti di riorganizzazione aziendale di più ampio respiro che portino ad una puntuale mappatura dei processi produttivi».

Per **Mascia Cassella**, partner dello ***Studio Legale Masotti Cassella***, «la problematica maggiore che uno studio legale affronta nel tentativo di tutelare una società in materia di privacy risiede, in prima battuta, nella necessità di districarsi tra le normative applicabili in materia di privacy e tra i conseguenti differenti adempimenti. Il nuovo regolamento di fatto non ha mai abrogato il vecchio testo normativo, complicando il lavoro degli studi legali che devono necessariamente trasformare gli adempimenti richiesti in documenti pratici e di facile lettura per il cliente. A ciò si aggiunge la nuova figura del Dpo, introdotta dal Regolamento: questo «mostro a due teste» che deve incarnare in una sola figura molteplici competenze, sia tecniche che legali. Il suo «doppio» ruolo, infatti, crea non pochi grattacapi alle società obbligate alla nomina di tale figura perché pochi sono i consulenti in grado di calarsi nel contesto aziendale e guardare alla situazione Privacy da entrambi i punti di vista». Secondo **Massimiliano Lissi**, partner di ***Talea Tax Legal Advisory*** «se finora la gestione della privacy è stata vissuta come burocrazia, in alcuni casi necessaria per adeguarsi ai requisiti di compliance, sarà sempre più necessario assumere una diversa forma mentale. Rispettare la privacy significherà avere fatto tutto il possibile per trattare i dati in modo sicuro e l'adeguamento dovrà essere disegnato su misura, caso per caso, per ogni singola realtà, ed in continuo aggiornamento. Il tema della sicurezza potrà, poi, in un'azienda preparata all'innovazione, costituire spunto per impostare un sistema sicuro anche sotto il profilo della conservazione del proprio know how e di tutto ciò che per l'azienda rappresenta un valore».

Per **Giampaolo Furlan**, partner di ***Galbiati Sacchi e Associati***, «da giuslavoristi, capita spesso di dover affrontare problematiche legate alla privacy nel rapporto di lavoro. Recentemente abbiamo affrontato, tra gli altri, il tema delle c.d. black box installate sulle auto aziendali assegnate ai dipendenti che svolgono la propria attività sul territorio. Tale tema si interseca con il più generale tema dei controlli e della tutela del patrimonio aziendale. Le black box infatti sono in grado di rilevare numerose informazioni potenzialmente associabili a soggetti identificati o identificabili. In considerazione di ciò il Garante Privacy ha affrontato il tema in oggetto e valutato legittima (dandone specifici indirizzi) l'installazione dei suddetti dispositivi di «*event data recorder*», a bordo di veicoli commerciali da parte di società operanti nel settore del noleggio».

Tra le nuove prescrizioni introdotte dal Gdpr, spicca il principio di accountability. «Riguarda in particolar modo il titolare del trattamento», spiega **Monica Aparo**, partner dello ***Studio Picchi Angelini & Associati***, «che, in base a tale principio, dovrà provare di aver adottato tutte le misure tecniche ed organizzative atte a garantire un livello di sicurezza dei dati personali e dei sistemi aziendali adeguato al rischio. È necessario, dunque, dotarsi di processi strutturati e, soprattutto, di competenze professionali idonee al compito capaci di guidare le piccole realtà verso un maggiore livello di consapevolezza. Tra gli adempimenti previsti dal Gdpr vi è anche l'obbligo di nominare un Responsabile della protezione dei dati (c.d. Dpo) per tutte le pubbliche amministrazioni e per tutte le aziende che trattano su larga scala dati sensibili o a rischio specifico, oppure che svolgono attività in cui i trattamenti richiedono il controllo

Italia Oggi Sette Affari Legali
08-FEB-2021
da pag. 1-2
Dir. Resp.: Pierluigi Magnaschi
foglio 4 / 4
Tiratura: 0 - Diffusione: 0 - Lettori: 82000: da enti certificatori o autocertificati
Superficie: 203 %

regolare e sistematico su larga scala degli interessati, mentre questa figura rimane facoltativa per tutte le altre aziende che possono comunque decidere di dotarsi o meno di un Privacy officer. Al riguardo, l'incertezza sull'obbligatorietà o meno di designare un Dpo così come la difficoltà a reperire un soggetto indipendente in possesso dei necessari requisiti professionali, rappresentano ulteriori criticità riscontrate dalle pmi alle prese con la compliance al Gdpr».


Antonio Ciccia Messina


Francesco Inturri


Antonio Barberisi


Lorenzo Colzi


Mario Di Giulio

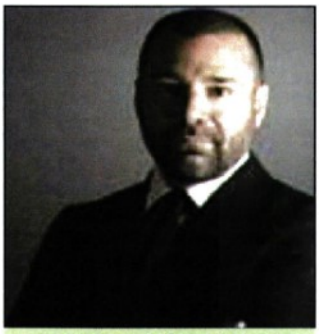

Giuseppe Di Masi


Francesco De Biasi


Carlo Majer


Flavio Acerbi


Andrea Puccio


Giovanni Aquaro


Mascia Cassella


Massimiliano Lissi


Giampiero Furlan


Monica Aparo