La gestione dei dati personali rappresenta un tema chiave

sistema informatico, nemmeno a quello di videosorveglianza».

Anche in ambito sanitario l'approvazione del Gdpr ha contribuito a richiamare l'attenzione degli operatori sul tema della privacy e della protezione dei dati, che è strettamente connesso ai profili della sicurezza nelle cure e della dignità del paziente. «Infatti, da una parte, come ha evidenziato lo stesso Garante in una recente relazione al Parlamento, eventuali carenze nella sicurezza dei dati personali possono avere effetti deleteri nei processi di erogazione dei trattamenti medici e rappresentare, quindi, causa di disfunzioni ed errori sanitari, che sono fonte di potenziale responsabilità della struttura, e sono tanto più gravi quando incidono su aspetti qualificanti dell'esistenza individuale (come la nascita, la morte o la genitorialità)», spiega **Gabriele Chiarini**, managing partner dello ***Studio Legale Chiarini***, «dall'altra parte, è chiaro che il trattamento dei dati personali per finalità di cura può interferire, anche in modo assai incisivo, con la dignità individuale, che va sempre salvaguardata. Penso, in particolare, ai pazienti sottoposti a trattamenti medici invasivi, a quelli affetti da patologie o infezioni gravi, alle persone offese da atti di violenza sessuale. Ma penso anche alle persone comuni, che si trovano nella sala d'attesa di una qualunque clinica ed hanno il diritto a non essere chiamate per nome e cognome, magari con la specifica enunciazione della prestazione alla quale devono sottoporsi. Può sembrare superfluo rammentarlo, ma anche il Garante, non troppo tempo fa, ha dovuto stigmatizzare il comportamento di un operatore sanitario, il quale – in un ospedale del Nord – aveva chiamato per cognome la paziente presente in sala di attesa chiedendole, ad alta voce, se dovesse effettuare una interruzione di gravidanza».

Gabriele Chiarini

La protezione dei dati personali ha visto una crescente attenzione da parte dell'opinione pubblica e degli operatori del diritto, questi ultimi letteralmente travolti dalla repentina necessità di confrontarsi con i riflessi dell'uso della moderna tecnologia sulla riservatezza della persona (basti pensare alle recenti spinose questioni riguardanti l'app Immuni). «Stare al passo dell'innovazione tecnologica si è rivelata un'ardua sfida, specialmente per il legislatore, le cui scelte non sono risultate sempre soddisfacenti in ottica privacy», spiega **Giuseppe Fornari**, founding partner di ***Fornari e Associati***, «è il caso, ad esempio, del mancato aggiornamento della normativa sulla responsabilità da reato degli enti. Sebbene l'art. 24 bis del dlgs n. 231/2000 titoli «Delitti informativi e trattamento illecito di dati», tale previsione non contempla l'inserimento tra i cd. reati presupposto delle diverse fattispecie di trattamento illecito neointrodotte agli articoli 167, 167 bis e 167 ter del cd. Codice Privacy. La scelta è apparentemente inspiegabile, in controtendenza rispetto all'ampliamento dell'area di rilevanza penale voluto dalla recente riforma. La spiegazione va forse ricercata nella sfida di stare al passo con i tempi prima accennata, cui non eravamo sufficientemente pronti. Prevedere la responsabilità degli enti per i delitti in materia di privacy avrebbe infatti imposto alle aziende un significativo impegno, sia in termini organizzativi che economici; nel timore di imbrigliare le imprese con ulteriori adempimenti, si è preferito rinunciare ad una più rigorosa protezione del dato personale. Con buona pace della prevenzione di tutte quelle ipotesi di trattamento illecito che la compliance 231 avrebbe forse potuto adeguatamente scongiurare».

Giuseppe Fornari

Uno dei temi che sta divenendo di sempre maggiore interesse in ambito privacy riguarda il funzionamento degli algoritmi di App e programmi, in rapporto alla effettiva tutela dei dati personali e di taluni diritti fondamentali della persona. «Un esempio plastico dell'attualità di tale problematica viene offerto da una recentissima ordinanza emessa dal Tribunale di Bologna in data 30 dicembre 2020, nei confronti di una nota azienda multinazionale operante nel settore delle consegne a domicilio di piatti pronti mediante l'ausilio dei c.d. riders», dice **Marco Agostini**, senior associate di ***GR Legal***, «tale pronuncia, ha riconosciuto il carattere discriminatorio del sistema di profilazione dei riders attuato attraverso una apposita app che gli stessi erano obbligati contrattualmente a scaricare sul proprio smartphone per svolgere la propria attività; l'algoritmo di profilazione usato dalla app incideva infatti sulle opportunità di lavoro agli stessi riservate riducendo in sostanza le occasioni di accesso agli slot di lavoro per coloro che non rispettavano parametri di affidabilità e partecipazione. La mancata produzione in giudizio da parte della società resistente di informazioni sul funzionamento dell'algoritmo utilizzato dall'App ha precluso al tribunale una più approfondita disamina della questione. La pronuncia in rassegna conferma la crescente consapevolezza del difficile rapporto tra tutela dei diritti della personalità e nuove tecnologie».

Marco Agostini

Francesco Falco

Secondo **Francesco Falco**, partner di ***Dwf***, «l'emergenza sanitaria ha reso centrale il tema del trattamento, in ambito aziendale, dei dati inerenti la salute dei dipendenti. All'inizio dell'emergenza sanitaria, la compliance Gdpr rilevava rispetto a tale trattamento nel contesto della normativa emanata per contrastare il Covid (e.g., rilevamento della temperatura); con il persistere della pandemia, si moltiplicano le riflessioni rispetto all'adozione di strumenti innovativi per la tutela della salute dei dipendenti (e.g., obbligo vaccinale), la cui verifica di compliance rispetto al Gdpr è fondamentale per determinarne l'efficacia».

Durante la pandemia, lo smart working è divenuto una modalità di svolgimento della prestazione lavorativa sempre più comune.

Paola Pucci

«Poiché smart working vuol dire svolgere la prestazione dove si vuole e non, come avviene classicamente, all'interno dei locali aziendali», spiega **Paola Pucci**, partner e Dpo di ***Toffoletto De Luca Tamajo***, «la sua diffusione ha imposto anche una riflessione in relazione alla protezione dei dati personali trattati nell'ambito della prestazione lavorativa. Come noto, infatti, l'adozione da parte del titolare di misure organizzative e di sicurezza adeguate a proteggere la riservatezza dei dati è cruciale nell'ambito della disciplina privacy; molte di queste misure sono spesso legate all'essere fisicamente nei locali aziendali che dispongono, in genere, di tutte le necessarie strutture e strumenti di sicurezza. Quando, invece, la prestazione di lavoro si sposta al di fuori di tali locali la sfida per il titolare, dunque, è riuscire a far in modo che ogni trattamento sia svolto con i medesimi standard di sicurezza.

Molteplici sono le misure da approntare per il datore di lavoro al fine di raggiungere questo scopo: si va da quelle relative alla sicurezza dei dati in senso tecnico, come l'utilizzo di strumenti informatici con criptazione dei dati e password adeguate, all'adozione di policy ed istruzioni specifiche per il lavoratore in smart working che possono includere l'obbligo di lavoro e salvataggio solo mediante Vpn e mai in locale, particolari prescrizioni in merito alle reti internet da usare e precauzioni idonee a evitare la perdita fisica degli strumenti. A chiusura del sistema però, come sempre, resta la necessità – anche da remoto – di provvedere ad un'adeguata formazione del lavoratore nonché allo svolgimento dei necessari controlli da parte del datore di lavoro che devono essere effettuati seguendo l'art. 4 dello Statuto dei Lavoratori e la normativa sulla privacy».

Per **Maddalena Valli**, senior manager di ***Legalitax Studio Legale***, a oltre due anni dall'entrata in vigore del Gdpr «le aziende sembrano aver acquisito una maggiore consapevolezza in merito ai principi di privacy by design e by default. Tali principi impongono che in caso di un nuovo progetto/flusso, che implichi il trattamento di dati personali, venga attivata una progettazione della privacy sin dalle sue fasi embrionali. Ogni valutazione dovrà essere effettuata secondo logiche di accountability. La pandemia ha senza dubbio rappresentato un banco di prova per le imprese che si sono trovate a dover implementare velocemente nuovi flussi di trattamento dei dati. Si pensi a chi si è visto costretto ad introdurre, per la prima volta, lo smartworking e il telelavoro, dovendo porre attenzione, oltre che alle questioni giuslavoristiche, anche al trattamento dei dati di dipendenti, clienti, fornitori e prospect gestiti dagli smartworker e telelavoratori fuori dai locali aziendali. In questo contesto l'assistenza dello studio legale specializzato in privacy è stata determinante al fine di individuare correttamente i confini del principio di «minimizzazione dei dati». L'imprenditore ha potuto correttamente individuare i dati effettivamente considerabili come adeguati, pertinenti e necessari rispetto alle finalità dichiarate ed espletare, ove necessario, la Privacy Impact Assessment.

Maddalena Valli

Ma vi è di più. Le forti limitazioni alle vendite al dettaglio imposte dai vari Dpcm e provvedimenti regionali hanno indotto le aziende a ripensare alle proprie modalità di vendita. Questa è stata quindi l'occasione per costruire, rivedere ma anche rafforzare tutto l'apparato privacy connesso alle vendite eseguite attraverso le piattaforme e-commerce o i social network».