intermediachannel.it

URL :http://www.intermediachannel.it/

PAESE : Italia

TYPE : Web Grand Public

► **10 maggio 2021 - 08:31**

> Versione online

Privacy, il Covid mette a rischio i dati sensibili sulla salute

In EvidenzaNews

10/05/2021

Il settore della tutela dei dati personali è sempre più spesso influenzato dalla pandemia. Dopo l'esplosione del Covid, e l'introduzione di tutte le misure volte a contenere il virus, sono infatti emersi numerosi aspetti legali alla tutela e alla gestione dei dati personali, soprattutto in ambito sanitario. Temi sui quali gli studi legali che si occupano del settore sono da tempo con le antenne alzate.

«*Appare evidente che attualmente i dati più preziosi e più delicati da trattare, oltre che di ormai costante trattamento sono quelli relativi alla nostra salute*», spiega **Giovanni Ricci dello Studio Edoardo Ricci**. *«Noi tutti siamo portati a ritenere che i dati sensibili sulla salute possano essere trattati subordinatamente al nostro consenso espresso ed informato. Questa convinzione, oltre ad essere corretta in linea di principio, è altresì stimolata dalla nostra recente esperienza diretta, che, per esempio, ci ha proposto l'utilizzo della app Immuni subordinato al nostro consenso. O come la vaccinazione contro il Covid, a sua volta subordinata alla nostra volontà in tal senso. Ma le cose stanno proprio così? Oppure, invece, noi tutti siamo in qualche modo vittima di una sorta di inganno? Il dubbio è lecito laddove si consideri che la normativa in vigore in tema di trattamento e tutela dei dati personali prevede espressamente, come copertura giuridica del medesimo trattamento, almeno un altro elemento, rappresentato dalle esigenze di tutela del pubblico interesse, e segnatamente, di tutela delle esigenze della salute pubblica, e della ricerca scientifica e statistica. Non a caso, la medesima normativa prevede come esempio di situazione che consente il trattamento obbligatorio dei nostri dati, per esigenze di tutela della salute pubblica, l'epidemia»*.

Nel corso di quest'ultimo anno le sfide poste dalle disposizioni vigenti in materia di data governance sono state numerose in quanto la pandemia ha implicato, da un lato, un'accelerazione della digitalizzazione dei processi aziendali e, dall'altro, l'individuazione del data base quale asset economico da valorizzare. *«Questo scenario si è riflesso anche sulla consulenza richiesta dai clienti che, oltre a quella tradizionale sulla conformità normativa impattata soprattutto dai trattamenti dei dati nell'ambito dei protocolli di sicurezza aziendali anti-Covid e dalle conseguenze della sentenza della Corte di giustizia dell'Unione europea c.d. «Schrems II» che ha determinato l'invalidità della decisione di adeguatezza del Privacy Shield tra Europa e Usa»*, dice I**van**

Rotunno, special counsel e practice leader cybersecurity e data protection Italy di Orrick.*«La Corte si è concentrata principalmente sia su aspetti legati alla crescita costante del cybercrime, in quanto le imprese che si sono trovate a fronteggiare attacchi ai sistemi di sicurezza informatici sono numerose, sia sullo sviluppo di nuovi progetti che si fondano sullo sfruttamento dei dati in un'ottica di cd. legal design. Allargando la prospettiva a scenari de jure condendo, è verosimile ipotizzare che nel prossimo futuro le principali aree di assistenza ai clienti saranno connesse all'implementazione del pacchetto normativo dell'Unione Europea sui servizi digitali («Digital Services Act – Dsa») e il progetto per la definizione di un sistema europeo per i servizi digitali, comprese le piattaforme e i mercati online che costituisce la prima fase dell'ambizioso piano adottato dalla Commissione Ue di rafforzare il mercato unico dei servizi digitali e favorire l'innovazione e la competitività dell'Europa rispetto ad altri Paesi già forti nel settore».*

L'emergenza sanitaria ha anche avuto l'effetto di dare una spinta alla Medicina 4.0 o eHealth, un concetto molto ampio, che copre l'interazione tra informatica medica, sanità pubblica e business. *«L'eHealth pone diversi interrogativi»*, spiega **Giangiacomo Olivi, co-head Europe del dipartimento Data privacy and security di Dentons**, *«ad esempio in relazione ai temi dei wearable devices e delle app comunque relative al monitoraggio della salute, che sono dei veri e propri collettori di dati sanitari e, sempre più spesso, il loro funzionamento si basa su algoritmi predittivi che hanno bisogno di sempre più dati. Trattandosi anche di app largamente diffuse e apparentemente «innocue«, difficilmente basiamo la nostra fiducia su una scrupolosa verifica sull'affidabilità del titolare del trattamento, sul luogo di conservazione dei dati, sull'eventuale trasferimento oltre lo Spazio Economico Europeo; ancor meno, verifichiamo né possiamo verificare le misure di sicurezza implementate a tutela dei nostri dati sanitari. Proprio con riferimento alle nuove tecnologie e all'utilizzo di algoritmi, la Commissione Europea potrebbe pubblicare già nel primo trimestre del 2021 una proposta legislativa, sperabilmente con la forma di regolamento, specificatamente dedicata ai sistemi di intelligenza artificiale, sempre più diffusi anche nella nostra quotidianità. Questa proposta legislativa dovrebbe verosimilmente normare anche il tema della responsabilità dei sistemi di intelligenza artificiale, riuscendo così a dare risposta a un interrogativo (chi risponde delle azioni e delle omissioni di un sistema di intelligenza artificiale?) che, ad oggi, può essere risolto ricorrendo unicamente a normative che, seppur tecnologicamente neutrali, spesso mal si adattano alle specificità dell'intelligenza artificiale».*

Negli ultimi mesi le questioni più delicate connesse alla privacy hanno riguardato il contemperamento degli interessi coinvolti nella gestione del rischio contagi Covid-19 sui luoghi di lavoro. *«Ci siamo infatti trovati spesso a fornire consulenza alle aziende clienti circa le corrette modalità di trattamento dei dati sanitari e di salute dei dipendenti»*, spiega **Simona Cardillo, senior associate di Lexant**, *«che il datore di lavoro può garantire, ad esempio, evitando la conservazione dei dati ed affidando al medico competente la raccolta delle informazioni sulla salute dei lavoratori. Un altro aspetto delicato in tema privacy riguarda lo smartworking, non sempre capace di garantire la sicurezza informatica aziendale e la corretta gestione dei dati personali. Anche in questo caso, il datore di lavoro è chiamato a trovare soluzioni concrete che contemperino l'esigenza di prosecuzione dell'attività aziendale, la tutela della sicurezza e della salute dei dipendenti e la riservatezza dei dati».*

Tra le misure caldeggiate per contrastare la diffusione del contagio, rientra certamente la rilevazione temperatura corporea in sede di accesso ai locali aziendali. *«Il tema ha riportato a galla l'annosa questione dei limiti che il diritto alla protezione dei dati personali può sperimentare in funzione di interessi fondamentali parimenti meritevoli di tutela, come la salute pubblica»*, dice **Enrico Napoletano dello Studio legale**

Napoletano & Partners, *«con il passaggio alla «Fase 2», abbiamo assistito al superamento dei termometri ad infrarossi – che, se non seguiti dalla registrazione del dato, non rientrano nel raggio di applicazione del Gdpr – da parte dei più sofisticati termoscanner, ove la misurazione della temperatura diventa un processo parzialmente automatizzato. Tra questi, si sono affermati i pannelli dotati di tecnologia «face detection« e «mask detection«, in grado di rilevare non solo la temperatura, ma anche il volto del soggetto e riconoscere se è munito di mascherina di protezione, emettendo in caso contrario un segnale di allarme ovvero inibendo direttamente l'apertura delle porte di accesso ai locali. Non si tratta ancora di dati biometrici: questi ultimi sono unicamente quelli che consentono l'identificazione univoca dell'interessato, come nel caso dei sistemi di «face recognition«, laddove nella «face detection» l'acquisizione dei contorni del volto serve solo per indicare il punto esatto della fronte in cui rilevare la temperatura. Tuttavia, la misurazione della temperatura corporea, qualora associata all'identità dell'interessato, costituisce un trattamento di dati personali ed è come tale soggetta alle garanzie del Gdpr, potenziate in virtù della categoria «particolare« in cui rientra il dato sanitario elettronico. Ciò comporta, oltre alla necessità di fornire l'informativa privacy, che il datore di lavoro potrà procedere alla mera rilevazione istantanea del dato, ma mai alla sua registrazione, nemmeno in caso di superamento della soglia di legge (37.5°), a meno che non sia necessario per documentare le ragioni che hanno impedito l'accesso: in altre parole, nel caso dei termoscanner, il dato termico potrà essere solo visualizzato su schermo live, ma non memorizzato.*
Ultimo, ma non per importanza: l'Edps ha chiarito che il termoscanner non deve essere collegato a nessun altro 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».*

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 neo-introdotte 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».

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».*

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. *«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.*
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».

Fonte: "Assinews.it"