TopLegal FOCUS

PRIVACY & DATA PROTECTION

Le sfide per le imprese approfondite con gli esperti

TopLegal FOCUS
PRIVACY & DATA PROTECTION

Sommario

Gdpr: Covid-19 accende i fari sulla privacy

Il ricorso allo smart working e l'accelerazione sul fronte della digitalizzazione della sanità hanno spinto gli studi a riflettere sui processi messi in atto da aziende e Pa per la corretta applicazione delle normativa.

Il Regolamento generale sulla protezione dei dati (General data protection regulation o Gdpr) è ormai quasi al giro di boa dei suoi primi tre anni. Pubblicato nella Gazzetta Ufficiale europea il 4 maggio 2016, è entrato in vigore il 24 maggio 2016, ma la sua attuazione è avvenuta a distanza di due anni, quindi a partire dal 25 maggio 2018. L'obiettivo è l'armonizzazione della regolamentazione in materia di protezione dei dati personali all'interno dell'Unione europea favorendo così lo sviluppo digitale nei vari Paesi membri.

Tra le diverse novità, ricordiamo il concetto di accountability del titolare e quello di privacy by design, l'approccio basato su rischio e adeguatezza delle misure di sicurezza, e l'introduzione di un responsabile per la protezione dei dati (Data protection officer – Dpo). Per tracciare un primo bilancio delle innovazioni introdotte e dell'esperienza maturata, il Focus di TopLegal raccoglie gli interventi degli esperti su alcuni degli aspetti di maggior interesse a cui le aziende devono prestare attenzione.

Una riflessione che arriva in un momento di particolare sforzo del sistema che ha avuto ripercussioni anche sulla corretta applicazione della normativa sulla privacy. La pandemia di Covid-19 ha infatti alzato l'asticella sulle tematiche di privacy in relazione all'accelerazione impressa a pratiche nuove o non ancora diffuse.

Per esempio, si è assistito al ricorso esteso e repentino dello smart working, che ha comportato la comprensione delle policy e degli adempimenti, necessari in relazione alla protezione dei dati personali, da parte dell'azienda e da parte dello stesso lavoratore da remoto per quanto riguarda le informazioni aziendali. La pubblica amministrazione e gli operatori del settore sono stati posti di fronte alla prospettiva di accelerazione sul fronte della digitalizzazione della sanità, grazie alle risorse del recovery Fund che ne potranno permettere l'aggiornamento tecnologico. Un passaggio che chiama in causa la corretta gestione dei dati a fronte dell'introduzione e diffusione di applicazioni digitali e di software di intelligenza artificiale.

Centrale nella direzione impressa dal Gdpr è l'evoluzione in tema di governo del dato, ossia la strutturazione di un insieme di procedure, responsabilità e controlli per la gestione della privacy. In questo quadro, è emersa con forza la rilevanza della figura del Dpo (che può essere sia un soggetto interno sia esterno), una funzione che in poco tempo ha mostrato la sua utilità all'interno degli equilibri dell'impresa, non solo in ottica di presidio della riservatezza ma anche competitiva in relazione all'ascesa del concetto di data economy, ossia un'economia basata sulla capacità delle imprese di gestire la quantità crescente di informazioni digitali per la creazione di valore.

Per la Commissione europea l'utilizzo intelligente dei dati può avere un effetto trasformativo su tutti i settori dell'economia e può creare nuove opportunità di crescita economica, anche per le Pmi. Il valore della data economy nell'Unione Europea era nel 2019 di quasi 325 miliardi di euro nel 2019, circa il 2,6% del prodotto interno lordo. Le stime indicano che aumenterà fino a superare i 550 milioni di euro nel 2025, raggiungendo così il 4% del Pil complessivo della Ue.

A CURA DI VITTORIO DE LUCA ED ELENA CANNONE

Smart working e protezione dei dati personali

Condizioni, limiti e adempimenti che il datore di lavoro deve attuare a protezione dei dati personali dello smart worker e delle informazioni aziendali.

Con la Legge n. 81 del 22 maggio 2017 recante *"Misure per la tutela del lavoro autonomo non imprenditoriale e misure volte a favorire l'articolazione flessibile nei tempi e nei luoghi del lavoro subordinato"*, è stato regolamentato per la prima volta nel nostro ordinamento il lavoro agile (comunemente definito "*smart working*"). Si tratta di una modalità flessibile di esecuzione della prestazione lavorativa, nell'ambito del rapporto di lavoro subordinato, caratterizzata dall'assenza di vincoli di orario o luogo di lavoro e da forme di organizzazione per fasi, cicli e obiettivi.

Nell'implementare lo smart working nella propria azienda il datore di lavoro deve tener conto della normativa dettata in materia di protezione dei dati personali.

Il Regolamento (UE) 2016/679 in materia di protezione dei dati personali ("GDPR") ha introdotto il c.d. *principio di accountability* ossia l'adozione, da parte del Titolare del trattamento (nel nostro caso il datore di lavoro), di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del GDPR stesso. In sostanza, il datore di lavoro è tenuto ad individuare e gestire i rischi relativi ai trattamenti svolti, nel rispetto del principio della protezione dei dati fin dalla progettazione di ciascun trattamento ("*by design*") e della protezione dei dati medesimi di default ("*by default*").

Ciò significa che, nel lavoro agile, il datore di lavoro deve effettuare un idoneo *risk assessment* e, ove necessario, una valutazione di impatto in modo tale da analizzare tutti i rischi esistenti e potenziali nonché individuare le misure di sicurezza, tecniche e organizzative, adeguate a garantire la sicurezza e la protezione dei dati. In questa ottica il datore di lavoro deve adottare Regolamenti, Policies o Linee Guida recanti i comportamenti che gli smart workers devono tenere per garantire la riservatezza, l'integrità e la disponibilità dei dati trattati nello svolgimento delle proprie mansioni. Il datore di lavoro deve, altresì, verificare che il controllo da remoto non sia un controllo invasivo in contrasto con l'art. 4 della Legge 300/1970. Ciò comporta un esame dettagliato dei sistemi che consentono un monitoraggio continuo dell'utilizzo degli strumenti di lavoro e della rete aziendale da parte dei dipendenti. Proprio per questo lo *smart worker* deve essere dettagliatamente informato delle modalità tramite le quali il datore esercita il potere di controllo nonché di quali sono i comportamenti passibili di una eventuale sanzione disciplinare. Non solo. Il datore di lavoro deve formare gli smart workers affinché questi abbiano piena consapevolezza e conoscenza degli strumenti messi a loro disposizione, dei rischi e delle misure da adottare durante lo smart working.

De Luca & Partners

Lo Studio Legale De Luca & Partners, fondato nel 1976 e oggi composto da un team di 24 persone, è specializzato nel Diritto del Lavoro e svolge la propria attività di consulenza, assistenza e patrocinio giudiziario al fianco delle società nazionali e multinazionali appartenenti a tutti i settori merceologici, in tema di diritto del lavoro, diritto di agenzia e delle relazioni industriali, contratti di distribuzione, contratti di lavoro autonomo e parasubordinato, diritto dell'immigrazione, diritto della previdenza sociale, diritto tributario del lavoro, M&A e operazioni straordinarie, Top Management, diritto della salute e della sicurezza sul lavoro, responsabilità amministrativa degli enti (d.lgs. 231/2001), Privacy e Data Protection.

Largo Arturo Toscanini, 1 - 20122
T. +39.02.365.565.1
info@delucapartners.it

www.delucapartners.it

A CURA DI STELIO PAGNOTTA

E-Lex in prima linea per la tutela dei dati biometrici e genetici

Con lo sviluppo delle nuove tecnologie in ambito biometrico e genetico, si presentano nuove sfide e questioni critiche da affrontare

La studio romano E-Lex rappresenta da anni un'avanguardia nelle questioni attinenti alla data *protection*, affrontando, tra le tante, questioni particolarmente critiche, che coinvolgono il trattamento di dati genetici e biometrici.

Tali categorie di dati sono sempre più al centro dell'attenzione, per la loro utilizzazione all'interno del mondo scientifico e digitale e per i rischi che possono derivarne per i diritti e le libertà dei soggetti interessati coinvolti. Con l'entrata in vigore del Regolamento UE 679/2016, i dati genetici e i dati biometrici hanno ottenuto una definizione in ambito giuridico e una tutela specifica, essendo stati ricompresi all'interno dell'art. 9 sul "Trattamento di categorie particolari di dati".

Nel corso degli anni, lo studio legale E-Lex si è occupato degli aspetti giuridici, curando anche i profili relativi a cifratura, pseudonimizzazione o le altre soluzioni che permettano la riduzione del rischio di divulgazione e di re-identificazione dei soggetti: pertanto, sono necessarie misure tecnologiche, ma anche organizzative, per minimizzare i rischi connessi ai trattamenti. Prescrizioni che sono state studiate approfonditamente da E-Lex in presenza di una clientela che opera nel settore sanitario, spaziando da operatori "tradizionali" (ASL e cliniche private) a innovatori del settore, tra cui alcune delle società di maggiore sviluppo in questo settore.

Analoghe riflessioni valgono per i dati biometrici, che consentono il riconoscimento dell'individuo per mezzo dell'impronta digitale, dell'iride o di alcuni tratti del viso. Tra i primi progetti affrontati dallo studio legale E-Lex, meritano di essere ricordati quelli relativi alle firme grafometriche e biometriche, utilizzate sia nel settore privato che nelle pubbliche amministrazioni, specialmente con il socio Ernesto Belisario. Più recentemente, una *startup* molto promettente ha lanciato un servizio – di cui l'avv. Giovanni Maria Riccio ha curato gli aspetti giuridici, anche grazie ad un proficuo dialogo con il Garante per la protezione dei dati personali – che utilizza una tecnologia innovativa che, seppur basata sulle informazioni biometriche, consente di non conservare alcun dato personale, che viene processato unicamente sul device dell'utente. Una sfida importante, che ha rappresentato per E-Lex l'ennesima finestra di sfida al futuro già presente.

E-Lex Studio Legale

Via dei Barbieri, 6 - 00186 Roma
Tel.: +39 06 87750524
E-mail: posta@e-lex.it

www.e-lex.it

A CURA DI ALESSANDRO COLELLA E MICHELE LUIGI GIORDANO

La Governance e i Controlli in materia di privacy

Il Sistema di Gestione Privacy nelle aziende deve essere un modello di gestione operativo tale da garantire l'effettiva protezione dei dati personali nel rispetto dei diritti del lavoratore

A distanza di più di due anni dalla entrata in vigore del Reg. (UE) 2016/679 ("GDPR"), ed a seguito delle modifiche al Codice Privacy di cui al D.Lgs. 101/2018, le tematiche della *Governance e dei Controlli in materia di protezione dei dati personali* hanno acquisito un'importanza sempre maggiore nella definizione delle strategie e dei contenuti dei Sistemi di Gestione della Privacy (nel seguito anche SGP), imponendo una specifica valutazione sul "Governo del Dato" e sul sistema dei "Controlli Datoriali", attenzionandone le modalità operative e la trasparenza delle regole in ottica di adeguatezza e proporzionalità in relazione alle dimensioni e complessità degli specifici contesti aziendali.

Con l'espressione "Governo del Dato" riferita al trattamento dei dati personali possiamo intendere il sistema di regole che deve essere definito per determinare nella propria struttura organizzativa aziendale: ruoli, compiti, responsabilità, procedure e policy, controlli e monitoraggi, flussi informativi, e rendicontazione delle attività. In sostanza si tratta di introdurre e definire un SGP in modo che sia chiaro:

a. quali siano i contenuti del SGP in relazione allo specifico contesto aziendale;

b. quale siano la metodologia e la logica di risk-based da adottare;

c. quale sia la leadership, quali siano i ruoli e le responsabilità, ovvero:

- chi può prendere decisioni;
- chi deve conformarsi alle decisioni;
- quale sia il processo che governa le suddette decisioni dalla fase della progettazione alla fase dell'implementazione e successiva verifica;
- quali siano, infine, le responsabilità sia in capo a colui che decide sia in capo a colui che deve eseguire le decisioni;

d. quali siano i livelli di controllo;

e. come viene gestito l'esercizio del potere di controllo datoriale;

f. quali siano i flussi informativi tra gli attori del SGP;

g. come attuare la rendicontazione delle attività svolte e implementare le azioni di miglioramento.

La formalizzazione dei contenuti di tali regole deve essere declinata in specifiche misure e strumenti organizzativi, quali: il funzionigramma privacy; le nomine "interne" (es. Autorizzato, Designato, Amministratore di sistema) ed esterne (Responsabili ex art. 28 del GDPR); le deleghe di funzione; le Job description; le istruzioni e procedure operative; la procedura sui flussi informativi da e verso gli attori del SGP; la reportistica periodica sulle attività svolte; il piano di monitoraggio; le attività di controllo e di stress testing; e il piano di miglioramento sul SGP. Questa impostazione rende il SGP conforme anche ai principi di Accountability, in quanto permette ai Titolari e Responsabili: di poter progettare e implementare i trattamenti dei dati e le misure di

sicurezza pertinenti rispetto rischi connessi al trattamento e alla protezione dei dati; e di poter dimostrare, rendicontare e formalizzare sia le scelte attuate e sia l'efficace implementazione dei contenuti del SGP anche attraverso il piano di monitoraggio. In relazione al sistema dei controlli che il SGP deve prevedere, è importante focalizzare l'attenzione sui controlli datoriali. Il diritto del lavoratore a non essere sottoposto a forme di controllo invasive nello svolgimento della propria attività lavorativa rappresenta un principio consolidato nel nostro ordinamento, avendo il legislatore già con le disposizioni di cui alla L. n. 300 del 20 maggio 1970, cd. Statuto dei Lavoratori, dettato disposizioni volte alla tutela della riservatezza e dignità dei lavoratori. Il mutato contesto tecnologico con l'avvento degli "strumenti di lavoro", vale a dire dei dispositivi normalmente utilizzati al fine di rendere la prestazione lavorativa, rappresenta una nuova sfida e un terreno di contrapposizione tra libertà imprenditoriale e libertà personale nel quale gli aspetti collegati alla tutela dei dati personali hanno via via acquisito una maggiore centralità. Sotto il profilo della normativa primaria, disposizione cardine in tema di controlli datoriali è l'art. 4 dello Statuto dei Lavoratori che, a seguito della riforma del c.d. Jobs Act, statuisce, al terzo comma, che le informazioni raccolte nell'ambito dei controlli sono utilizzabili per tutti i fini connessi al rapporto di lavoro a condizione che sia stata data informativa al lavoratore sulle modalità di uso degli strumenti e di effettuazione dei controlli e siano state rispettate le disposizioni del Codice Privacy. L'articolo in questione contiene dunque, a seguito della novella del Jobs Act, un espresso richiamo al Codice Privacy, laddove subordina l'utilizzabilità dei dati acquisiti nell'ambito delle attività di controllo anche alla condizione del rispetto delle previsioni in materia di protezione dei dati. Inoltre, occorre considerare anche le implicazioni privacy puntualmente analizzate nel corso degli ultimi anni dalle autorità garanti europee. Limitandosi alla nostra Autorità Garante, in base alle Linee guida del Garante per posta elettronica e internet del 1° marzo 2007 [doc. web 1387522] centrale risulta essere il rispetto del principio di trasparenza che impone di indicare «*chiaramente e in modo particolareggiato, quali siano le modalità di utilizzo degli strumenti messi a disposizione ritenute corrette e se, in che misura e con quali modalità vengano effettuati controlli*». Dette modalità devono essere prospettate ai lavoratori «*in modo chiaro e senza formule generiche, da pubblicizzare adeguatamente (verso i singoli lavoratori, nella rete interna, mediante affissioni sui luoghi di lavoro con modalità analoghe a quelle previste dall´art. 7 dello Statuto dei lavoratori, ecc.) e da sottoporre ad aggiornamento periodico*». La consapevolezza degli effetti e delle conseguenze del controllo passa anche dalla conoscenza da parte del dipendente di «*quali informazioni sono memorizzate temporaneamente (ad es., le componenti di file di log eventualmente registrati) e chi vi può accedere legittimamente*» e dalla conoscenza della possibilità per il datore di lavoro di effettuare controlli in conformità alla legge. Alla luce di quanto sopra appare pertanto evidente come il SGP debba contenere anche una specifica policy sull'utilizzo degli strumenti di lavoro che offra una corretta e chiara informativa circa l'esercizio del potere di controllo datoriale senza la quale anche gli obiettivi perseguiti con il controllo rischiano di non essere raggiunti stante la conseguente inutilizzabilità delle informazioni raccolte ai sensi del comma terzo dell'art. 4 dello Statuto dei Lavoratori.

Studio Associato
Consulenza legale e tributaria
KPMG

Alessandro Colella

Michele Luigi Giordano

I professionisti Tax & Legal di KPMG operano in 12 uffici, Bologna, Firenze, Genova, Milano, Napoli, Padova, Perugia, Pescara, Roma, Torino e Verona, e sono parte del network globale di KPMG International. La multidisciplinarietà sviluppata dal Network internazionale consente allo Studio Associato di KPMG di offrire una gamma completa e integrata di servizi e consulenze professionali legali, fiscali e di compliance personalizzate e al passo con il mercato.

Michele Luigi Giordano
Partner - Governance, Compliance & Organisation
michelegiordano@kpmg.it

Alessandro Colella
Associate Partner - Legal
acolella@kpmg.it

Sede centrale
Via Vittor Pisani, 31
20124 Milano MI
T: +39 02 676441

www.kpmg.com/it

Martini Manna

A CURA DI LUIGI MANNA

La gestione dell'e-mail dei dipendenti

Implicazioni di tutela della privacy e giuslavoristiche

Tra i dati personali che la maggior parte delle aziende tratta, quelli relativi alla posta elettronica dei dipendenti sono senza dubbio tra i più delicati da gestire. La premessa di quanto appena scritto è che, per quanto il dominio aziendale e la casella di posta elettronica del dipendente siano giuridicamente di titolarità del datore di lavoro, nel caso di account di posta individuali sia i dati c.d. esteriori delle e-mail (data, ora, mittente, destinatario, oggetto) che, a maggior ragione, quelli inerenti al contenuto delle stesse, sono a tutti gli effetti "dati personali" dei dipendenti, e come tali vanno trattati. Non vale a sortire effetto contrario – sebbene sia doveroso – lo stabilire, nel regolamento di utilizzo delle tecnologie informatiche aziendali, che la casella e-mail lavorativa non dovrebbe essere utilizzata per comunicazioni personali.
Rispetto alla posta elettronica viene, peraltro, in rilievo, accanto alla disciplina sulla tutela dei dati personali, anche la disciplina giuslavoristica: i commi 2 e 3 dell'art. 4 Stat. lav. sui "controlli a distanza" sono unanimemente considerati applicabili all'email assegnata al dipendente. Quella che segue è una sintesi degli arresti più rilevanti emersi negli ultimi anni dalla giurisprudenza giuslavoristica e dai provvedimenti del Garante per la protezione dei dati personali.

La previa informativa è essenziale.
Il lavoratore deve essere messo in condizione di sapere in maniera trasparente dall'inizio del rapporto quali operazioni, con quali modalità e per quali finalità, sono svolte sulla sua posta elettronica; informato dei suoi diritti di accesso e opposizione; informato dei tempi di conservazione della posta sui server aziendali (o in forma di copia di back-up, ovunque conservata). Particolare rilievo dovrà essere dato ai controlli che il datore si riserva di svolgere sulla posta del dipendente al fine di prevenire e/o tutelarsi contro inadempimenti e illeciti, anche commessi contro terzi (controlli c.d. difensivi). Senza questo adempimento preliminare, qualsiasi successiva operazione sull'e-mail del dipendente diventa potenzialmente illegittima, a prescindere dalla sua legittimità nel merito. Non è, tuttavia, vero il contrario: non basta informare preventivamente il dipendente perché una determinata attività, intrinsecamente illecita, diventi lecita.

L'archiviazione indiscriminata e senza limiti temporali delle e-mail aziendali non è ammessa.
Il Garante ha ribadito in più di un'occasione che una conservazione sistematica e illimitata nel tempo dei dati esteriori e/o del contenuto di tutte le comunicazioni elettroniche scambiate dai dipendenti attraverso gli account aziendali non

può essere in alcun modo giustificata, neppure adducendo la necessità di assicurare la continuità aziendale o di poter ricostruire rapporti interni ed esterni, anche in vista di possibili contenziosi. A tali fini, secondo il Garante, l'azienda dovrebbe semmai dotarsi di sistemi di gestione documentale con i quali individuare i documenti che devono essere archiviati; inoltre il trattamento di dati personali effettuato per finalità di tutela dei propri diritti in giudizio deve riferirsi a contenziosi in atto o a situazioni precontenziose, non ad astratte e indeterminate ipotesi. Purtroppo, il Garante non ha mai fornito specifiche indicazioni positive sulla corretta conservazione delle e-mail; inoltre, a parere del sottoscritto, la posizione assunta dall'Autorità soffre di eccessiva rigidità, dove manca di considerare che, in diversi casi, la corrispondenza elettronica è il documento: ad esempio un contratto a forma libera ben può essere concluso con lo scambio di due semplici e-mail. Un possibile approccio è quello di prestabilire un tempo minimo di conservazione (es. 2-3 anni) per tutte le e-mail; e uno massimo (es. 10 anni) per alcune e-mail, individuate ad es. in base a parole chiave nell'oggetto o altri criteri di archiviazione che consentano qualche automatismo (e che richiederebbero probabilmente la collaborazione degli utenti), fatta salva la conservazione per tempi più lunghi di e-mail la cui conservazione diventi oggettivamente necessaria in relazione a contenziosi in atto o a situazioni pre-contenziose. Al tempo stesso, è necessario che l'azienda si doti di policy per l'archiviazione dei documenti allegati alle e-mail, che evitino l'eliminazione dei primi assieme alle seconde.

L'account deve essere immediatamente disattivato al termine del rapporto.

Dopo la cessazione del rapporto di lavoro, il datore di lavoro deve rimuovere gli account di posta elettronica aziendali riconducibili a persone identificate o identificabili ("in un tempo ragionevole commisurato ai tempi tecnici necessari", ma tendenzialmente nel giro di pochissimi giorni), previa disattivazione degli stessi e contestuale adozione di sistemi automatici che i) informino eventuali terzi, che scrivano all'account disattivato, della disattivazione stessa, fornendo loro indirizzi alternativi riferiti all'attività professionale dell'azienda ii) impediscano la visualizzazione da parte dell'azienda dei messaggi in arrivo durante il periodo in cui il sistema automatico è in funzione. Non è lecita, in altre parole, la diffusa prassi di tenere in vita per un certo periodo di tempo l'account dell'ex-dipendente, magari inoltrando le e-mail pervenute alla sua casella al suo ex superiore gerarchico o a un collega, giustificata con esigenze di continuità aziendale.

I controlli c.d. difensivi sull'email del dipendente sono ammessi, a condizione, anzitutto, che sin dall'assegnazione dell'account il dipendente sia stato lealmente informato della possibilità che il datore in casi eccezionali, in presenza di fondati sospetti sulla commissione di illeciti, acceda alla sua casella di posta elettronica per controllarne il contenuto, indicando anche le modalità di tali accessi e controlli. Sarebbe del tutto incompatibile con questa legittima finalità la raccolta *sistematica* delle comunicazioni elettroniche in transito sugli account aziendali dei dipendenti in servizio, la loro memorizzazione per un periodo non predeterminato e la possibilità per il datore di lavoro di accedervi per finalità indicate in astratto e in termini generali, che si tramuterebbero in controllo diretto a distanza contrario allo Statuto dei lavoratori.

Martini Manna Avvocati

Luigi Manna

Lo studio **Martini Manna Avvocati** è specializzato in proprietà intellettuale, TMT, privacy e diritto commerciale. Sua mission è offrire assistenza legale secondo i più alti standard internazionali, con un approccio pratico e un linguaggio facilmente comprensibile, in tempi rapidi e prestando attenzione alle necessità di business del cliente e al suo budget.

MILANO
Piazza Velasca 6 – 20122
T. +39 02 4507 4727; F. +39 02 4507 0327
BRESCIA
Via V. Emanuele II 1 – 25122
T. +39 030 2077 265; F. +39 02 4507 0327
VICENZA
Piazzetta Palladio 11 – 36100
T. +39 0444 1837 347; F. +39 0245070327

www.martinimanna.com

A CURA DI ROCCO PANETTA [1]

Benvenuti nel mondo della Data Economy

Come il DPO può svolgere un ruolo cruciale di equilibrio tra tutela dei diritti, valorizzazione dei dati, esigenze di business e rispetto delle regole

Nel 2020 si è celebrato il secondo anniversario dell'entrata in efficacia del Regolamento Generale sulla Protezione dei Dati (GDPR), mentre a maggio 2021 i tre anni saranno compiuti. Questa ricorrenza costituisce il primo vero giro di boa del GDPR e di tutti gli istituti che dallo stesso sono stati introdotti in forma inedita o innovativa rispetto al passato. Tra questi il *Data Protection Officer* (DPO) merita sicuramente una menzione speciale, una funzione di controllo e consulenza che in soli due anni e mezzo ha raggiunto una diffusione e un'importanza senza precedenti. Una funzione chiaramente non legal, ma ampiamente ricoperta – e a ragione – da legali; una funzione che dialoga con la *compliance*, ma che deve differenziarsi da essa, come chiarito anche da alcune importanti sentenze europee; sicuramente non una funzione di business, che tuttavia si è rivelata molto, ma molto importante proprio per il perseguimento dello scopo sociale di ogni azienda. Dopo un periodo in prima linea come DPO esterni di grandi imprese e gruppi internazionali credo che sia arrivato il momento di provare a tracciare un primo bilancio di questa esperienza, guardando ovviamente al futuro. Prima però ritengo sia importante fare qualche conto, utile a comprendere come mai sia opportuno domandarsi cosa abbiamo imparato fino ad oggi sul DPO. Secondo i dati dell'Autorità Garante per la protezione dei dati personali[2], le comunicazioni dei dati di contatto dei Responsabili della Protezione dei Dati nell'intervallo che va dal 25 maggio 2018 al 30 settembre 2020 sono state 57.998. Un numero in continua crescita ed indicativo di quanto tale figura professionale sia riuscita a penetrare nel reticolato di imprese e pubbliche amministrazioni anche oltre le ipotesi di nomina obbligatoria. Ampliando l'orizzonte di osservazione, una ricerca della *International Association of Privacy Professionals (IAPP)* ha stimato in mezzo milione le organizzazioni europee ad aver registrato un DPO presso le rispettive autorità nazionali ad un anno dall'entrata in efficacia del Regolamento[3]. In questi primi anni di applicazione sono state altrettanto consistenti le discussioni sulla disciplina del *Data Protection Officer*. L'opportunità di avvalersi di un DPO esterno rispetto a uno interno, la sua posizione nel contesto dei gruppi di imprese, la funzione e le responsabilità del DPO, le competenze, il mercato delle certificazioni e la *governance* sono solo alcuni dei vari temi dibattuti. Con il team di professionisti che coordino e al fianco dei quali lavoro ogni giorno sia come *managing partner* di Panetta & Associati Studio Legale, ma anche alla guida di PTP Privacy & Technology Professionals, società SPV specializzata nell'offerta di servizi da DPO in *outsourcing*, parte del global group Strand Advisory, abbiamo acquisito un livello di esperienza tale da permetterci di osservare questo settore da una prospettiva privilegiata. Il mercato in questi anni ci ha insegnato a riconoscere le esigenze delle aziende e le qualità e competenze richieste a un *Data Protection Officer*. Da qui abbiamo costruito il nostro "statuto" del DPO.

La (nuova) concezione della privacy

L'approfondita conoscenza della normativa sulla prote-

zione dei dati personali rappresenta senza dubbio un prerequisito fondamentale per ogni DPO. Il rapporto con questa meravigliosa ma complessa materia, tuttavia, non deve essere statico. Occorre infatti guardare anche a come le norme si sono evolute nel tempo, cercando altresì di interpretarle alla luce della specifica realtà che si sta osservando in un preciso momento storico. Da questo punto di vista, personalmente devo molto agli anni trascorsi come dirigente dello Stato presso l'Autorità Garante, così come agli insegnamenti ricevuti dai grandi Maestri della protezione dei dati personali con cui ho avuto la fortuna ed il privilegio di lavorare fianco a fianco: Stefano Rodotà e Giovanni Buttarelli. Guardando ai giorni nostri, questa disciplina, oltre a costituire un imprescindibile e costituzionalmente garantito presidio della nostra riservatezza, ha acquisito anche un elevatissimo valore competitivo. L'organizzazione da parte delle aziende dei trattamenti in un'ottica di privacy *by design e by default*, abbracciando costantemente il principio di *accountability*, costituisce ormai un vero valore aggiunto in ogni business. Un *quid pluris* sempre più ricercato e che si connota di incredibili esternalità positive. Un DPO, nell'esercitare i propri compiti di consulenza e controllo, dovrebbe dunque essere cosciente di tale, nuova, concezione della privacy, abbandonando dogmatismi e rigidità che non servono alle aziende e mortificano anche la libertà degli individui di cogliere appieno le molteplici opportunità della *data economy*.

La prospettiva internazionale

È ormai evidente che la nostra materia non corre più su binari nazionali. Il nuovo sistema europeo impatta su tutti gli attori del mercato, dai grandi gruppi multinazionali alle singole società che, per un motivo o per l'altro, si trovano ad intercettare altri Stati Membri nei propri trattamenti di dati personali. Un DPO dovrebbe sapersi calare comodamente in questo rinnovato quadro sovranazionale, mantenendo al contempo un contatto costante con le peculiarità che ancora caratterizzano il singolo Paese di riferimento. La competenza richiesta al DPO supera oggi anche i confini dell'UE. I trasferimenti di dati personali al di fuori dello Spazio Economico Europeo rappresentano un tema destinato ad assumere sempre più rilevanza, anche alla luce della recente invalidazione del *Privacy Shield* da parte della Corte di Giustizia e dei successivi interventi dell'*European Data Protection Board*. A un DPO è dunque richiesto di possedere una certa confidenza con la dimensione internazionale, da conquistare con la pratica quotidiana, ma anche con il networking. In tal senso, la IAPP, come più grande associazione di professionisti della privacy al mondo è un indubbio punto di riferimento.

La dimensione etica

Il mercato sta diventando pian piano sempre più sensibile ai problemi etici. Un percorso, avviato grazie soprattutto all'impulso delle istituzioni europee, che già pare mostrare i propri risultati nei settori più tecnologicamente avanzati. Stiamo assistendo da vicino ad una nuova e profonda trasformazione della nostra società, stretta tra l'ebbrezza tecnologica e il problema della circolazione e protezione dei dati personali, come emblema del godimento della libertà e dei diritti fondamentali di ciascuno. Il mondo deve guardare da vicino a questo nuovo ordine, e non deve rinunciare ad abbracciare il progresso e lo sviluppo dell'economia dei dati, ma occorrerà comprendere che solo un approccio che salvaguardi l'equilibrio tra uso, circolazione e valorizzazione dei dati personali secondo un principio di *ethics by default*, potrà fare la differenza e salvare l'uomo all'alba dell'era dell'intelligenza artificiale.

La sfida è per tutti, ma sono le funzioni legali, interne ed esterne, assieme ai DPO, a dover intercettare questo cambiamento, facendosi ambasciatori etici e garanti del business.

[1]Rocco Panetta – Avvocato Cassazionista, Managing Partner di Panetta & Associati Studio Legale e Fondatore di Strand | PTP Privacy & Tehcnology Professionals . E' Country Leader per l'Italia di IAPP International Association of Privacy Professionals e Membro del Board of Directors mondiale di IAPP, nonché Ethics Expert per ERCEA.

[2]www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9466298

[3]iapp.org/news/a/study-an-estimated-500k-organizations-have-registered-dpos-across-europe/

Panetta & Associati

Rocco Panetta

Panetta & Associati
Panetta & Associati è riconosciuta a livello nazionale ed internazionale come una tra le più consolidate e dinamiche law firm nel settore delle nuove tecnologie.

Strand | PTP Privacy & Technology Professionals
PTP Privacy & Technology Professionals, founding partner di Strand Advisory, è una società di consulenza leader nella fornitura di servizi di DPO esterno in Italia ed in EU.

ROMA, BRUSSELS, DUBLIN, TEL AVIV,
SAN JOSÈ, LOS ANGELES
Via Arenula, 83 – 00186
Roma Tel. & Fax: +39.06.68210129
info@panetta.net

www.panetta.net
www.strandadvisory.eu

A CURA DI SILVIA STEFANELLI

Protezione dei dati, intelligenza artificiale e legal design

Pare proprio che l'emergenza Covid abbia aperto la strada alla consapevolezza circa la necessità di mettere a sistema l'ormai diffuso (e un po' disorganizzato) utilizzo di tecnologie in sanità: dalle App medicali per la misurazione di parametri vitali ai chip sottocutanei per il controllo della glicemia, ai chatbot per verificare l'adesione dei pazienti alle sperimentazioni o PSP, ai sistemi di intelligenza artificiale per la second opinion sui tumori ovarici, fino all'esplosione dei sistemi di televisita (che hanno permesso la continuità clinica nel corso della pandemia).

In questo senso il recente PNRR prevede infatti a favore della sanità circa 20 miliardi di euro da suddividere in due ambiti principali: assistenza di prossimità e telemedicina; innovazione, ricerca e digitalizzazione dell'assistenza.

Senza dubbio poi in questo ambito uno dei temi vissuto come più critico e di difficile applicazione è quello della corretta implementazione del GDPR.

Appare, in particolare, molto complesso in questo settore coniugare gli obblighi di trasparenza (art. 12 GDPR) ed informativa (art. 13) con le numerose informazioni obbligatorie, problema amplificato nei casi in cui (ad esempio) si utilizzi una APP e si lavori quindi con le dimensioni ridotte dello schermo di un device.

Ove poi la APP lavori su un software di Intelligenza Artificiale (c.d. AI), il Titolare ai sensi dell'art. 13 co 2 lett. f) sarà altresì tenuto a fornire all'interessato le informazioni relative alla *"esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato"*.

In sostanza, sarà tenuto a spiegare come funziona la logica dell'algoritmo, con un aumento di difficoltà di comunicazione!

La necessità poi di una spiegazione chiara e comprensibile è altresì un elemento determinante anche per l'acquisizione del consenso, quale base giuridica del trattamento stesso: pacifico infatti che il consenso rilasciato dal paziente (che è e continua a rimanere il "proprietario dei dati") rappresenta una valida base giuridica solo ove il paziente stesso sia stato messo nelle condizioni di poter comprendere con esattezza *'come e perché'* i suoi dati vengono trattati, potendo quindi anche decidere se rilasciare o meno tale consenso.

Come scrivere allora un'informativa su una APP di AI in maniera tale da poter "garantire" la comprensione del paziente ?

Sotto il profilo dei contenuti, un importante aiuto è fornito da una recente guida pubblicata dall'Information Comunication Officer – ICO (il Garante ingle-

se) in ambito di Intelligenza Artificiale (AI) *"Explaining decisions made with AI - Draft guidance for consultation"*.

Molto sinteticamente, nel documento sopra citato il Garante britannico precisa che il Titolare del trattamento deve decidere "come" articolare l'informativa tenendo in considerazione i seguenti elementi:

1) il settore nel quale viene impiegato il modello di AI,
2) l'impatto sull'individuo,
3) la tipologia di dati trattati,
4) l'urgenza della decisione,
5) i soggetti a cui è destinata l'informativa.

Circa poi le modalità per la redazione materiale dell'informativa, il nostro Studio suggerisce l'utilizzo di **strumenti di Legal Design**.

Incentrato fortemente sulla UX (User Experience), il Legal Design nasce per migliorare la comprensione dei documenti giuridici, riprogettandoli completamente; si parte infatti dalla funzione che il documento deve svolgere per ridisegnarlo attraverso l'adozione di mezzi visivi come immagini, diagrammi, icone o video.

L'obiettivo è abbattere il cd. *"wall of text"*: vale a dire quella modalità di stesura dei documenti legali in cui le informazioni sono presentate solo in forma testuale e con un linguaggio strettamente "tecnico" e dunque complesso per l'utente di riferimento: l'informativa privacy è uno degli esempi tipici.

Il legal design agevola dunque il lettore attraverso la ricerca di nozioni-chiave, senza sacrificare il valore giuridico: in questo senso rappresenta per il software di AI in sanità – che nel caso di APP lavorano su limitate dimensioni dello schermo – uno strumento formidabile **in quanto rende i contenuti legali accessibili** ad ogni tipologia di utente.

Le interfacce utente (*user interface* – UI) dei software vengono infatti ridisegnate tenendo in considerazione da un lato l'interpretazione giuridica, da un altro gli aspetti visuali e comunicativi e da un altro-ancora gli strumenti tecnologici.

E' chiaro poi che si tratta di una metodologia multidisciplinare, che vede coinvolti in un lavoro comune giuristi, comunicatori, grafici e sviluppatori: è proprio la messa a fattore comune di queste diverse competenze che genera il valore aggiunto grazie a cui il Legal Design, tramite la tecnologia, può trasformare il diritto in una disciplina *human centric*, anche sotto il profilo della sua comprensione.

E si tratta di una innovazione tanto più urgente in un campo come quello sanitario in cui la trasparenza, il coinvolgimento del paziente e la sua comprensione del trattamento dei dati (e più in generale del processo di cura) rappresenta la miglior tutela dal rischio di contenzioso. Da ultimo poi l'implementazione del GDPR nell'ambito dell'Intelligenza Artificiale in sanità dovrà tenere in considerazione anche i profili etici del trattamento dei dati (la sui rilevanza è palesata nella recentissima *Proposta di Risoluzione del Parlamento Europeo recante raccomandazioni alla Commissione concernenti il quadro relativo agli aspetti etici dell'intelligenza artificiale, della robotica e delle tecnologie correlate* dell' 8 ottobre 2020) nonché tutti gli ulteriori adempimenti che dovranno essere implementati in base ad una preliminare Valutazione d'Impatto (ex art. 35 GDPR) che analizzi a monte **l'adeguatezza delle misure di protezione rispetto al rischio** sui dati, nonché **l'impatto che tale rischio può avere sui diritti degli interessati**, tra i quali, indubbiamente, non solo la riservatezza ma anche il diritto alla salute nel caso di perdita o non disponibilità temporanea dei dati stessi.

Stefanelli & Stefanelli

Silvia Stefanelli

Lo Studio Legale Stefanelli&Stefanelli, specializzato in Appalti e Sanità, ha realizzato in oltre vent'anni di attività un team di professionisti fortemente specializzato, sviluppando competenze legate ai temi innovativi della digitalizzazione, gestione del dato e nuove tecnologie. I principali clienti sono aziende che operano in ambito sanitario, farmaceutico e biomedicale, oltre ad imprese di costruzioni ed impiantistica.

BOLOGNA
Via Azzo Gardino 8/A 40122 Bologna
Telefono: +39 051520315
MILANO
Via Nino Bixio, 31 - 20129
Telefono: +39 02 87325559
ROMA
Palazzo Marignoli - Piazza di San Silvestro, 8 - 00187
Telefono: +39 0699312761
VENEZIA
Castello 2388 – 30122 Venezia

info@studiolegalestefanelli.it

www.studiolegalestefanelli.it

A CURA DI PROF. AVV. EMILIO TOSI - TOSI & PARTNERS HIGH TECH LEGAL®

Compliance privacy, DPO e GDPR: da costo a vantaggio competitivo

La novità dirompente del principio di accountability illumina tutta l'attività di prevenzione del rischio da trattamento illecito dei dati personali.

TOSI & PARTNERS HIGH TECH LEGAL® oltre ad essere apprezzato dalla clientela Corporate nei tradizionali servizi legali di ***Litigation - bancaria, commerciale, fallimentare e arbitrale*** - è leader nei settori della consulenza in materia di ***Diritto delle Nuove Tecnologie*** e della ***Corporate Compliance Privacy***. **Il Managing Partner Prof. Avv. Emilio Tosi** – *Professore Associato Abilitato di Diritto Privato* nell'Università di Milano Bicocca ***e fondatore nel 2003 della prima Collana in Italia "Diritto delle Nuove Tecnologie"***, già candidato al rinnovo della Consiliatura del Garante per la protezione dei Dati Personali per il settennato 2020-2027 – **è Direttore Esecutivo del noto *Centro Studi Diritto Nuove Tecnologie® – Studi Giuridici per l'Innovazione®***.

Nel 2019, da ultimo, pubblica il fondamentale studio monografico sul tema della ***"Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale"*** **(Giuffrè Lefebvre).** Nel citato studio si affronta il tema attualissimo della tutela dei diritti alla riservatezza e alla protezione dei dati personali alla luce dell'art.82 General *Data Protection Regulation* (GDPR). Lettura dottrinale rigorosa che registra l'oggettivazione della speciale responsabilità da trattamento illecito dei dati personali, la natura *in re ipsa* del danno correlato alla violazione del precetto conformativo previsto dal GDPR e la riemersione del danno morale con funzione deterrente-sanzionatoria alla luce del GDPR, del Codice della Privacy e della più recente giurisprudenza, attraverso il prisma del nuovo ***principio di accountability***.

Si è autorevolmente affrontato anche il rilevante problema interpretativo relativo al regime applicabile all'illecito trattamento posto in essere dal *Responsabile per la protezione dei dati personali - Data Protection Officer* (DPO) - che non pare, invero, essere destinatario di un regime speciale di responsabilità ad effetto esterno quanto piuttosto alle regole aquiliane del Codice Civile. Il **Prof. Avv. TOSI** partecipa, inoltre, ad **organi di amministrazione (CdA) e di controllo (CS ed in particolare, ODV 231) di primarie Società** ed è interpellato per predisporre *pareri pro-veritate strategici e second opinion in* relazione ai temi controversi del nuovo GDPR e del Diritto dell'Innovazione. *Last but not least*, presta alta consulenza strategica ai **DPO** di primari Gruppi industriali e bancari, nazionali e multinazionali. *"La tutela della privacy digitale e la protezione dei dati personali" – ricorda il Prof. Avv. TOSI – "non sono più un ossimoro ma costituiscono una vera e propria sfida regolatoria globale di cui il GDPR è riconosciuto legal benchmark"*.

Tosi & Partners
High Tech Legal

Via Larga, 7 - 20122 milano
tel. 02.76012753 – fax 02.76004573
info@tosilex.it

www.hightechlegal.it

Il Focus Appalti fa parte degli speciali
giuridici di TopLegal

Consulta su **www.toplegal.it**
tutti gli approfondimenti editoriali

Gli speciali:
Focus Tax
Focus Sport
Focus Fintech
Focus COVID-19
Focus Penale
Focus Lavoro
Focus Commercialisti
Focus Appalti

TopLegal
FOCUS
PRIVACY & DATA
PROTECTION