TeLex Anie
NOVITÀ LEGISLATIVE E GIURISPRUDENZIALI

Segnalazioni giuridiche a cura del Servizio Centrale Legale

N. 9 Anno XXV
Settembre 2020

INDICE:

a) ridurre da 15 a 14 giorni il termine minimo per il suo esercizio (allineandolo con quello previsto dalla disciplina europea);

b) estendere l'ipotesi di aumento di capitale con esclusione del diritto di opzione, nei limiti del 10% del capitale sociale preesistente (o del numero di azioni preesistenti), anche alle società negoziate in un sistema multilaterale di negoziazione, prevedendo altresì l'obbligo di indicare le ragioni dell'esclusione o della limitazione in apposita relazione degli amministratori, da depositare presso la sede sociale e pubblicare sul sito internet della società entro il termine della convocazione dell'assemblea, salvo quanto previsto dalle leggi speciali.

Da notare che con riferimento alle misure di carattere strutturale, in sede di conversione del DL, l'articolo 2441, co. 3, c.c. - che aveva eliminato l'obbligo di offrire sul mercato i diritti di opzione non esercitati, dopo il decorso del relativo termine, nonché consentito alla società di imporre il contestuale esercizio del diritto di opzione e del diritto di prelazione sulle azioni non optate (c.d. **oversubscription**) - è stato sostituito e riformulato in una versione più in linea con la norma previgente, applicabile sia alle azioni quotate nei mercati regolamentati, sia alle azioni negoziate in sistemi multilaterali di negoziazione.

Viene infatti ripristinato l'obbligo in capo agli amministratori di offrire nel mercato regolamentato (o nel sistema multilaterale di negoziazione) i diritti di opzione non esercitati, entro il mese successivo alla scadenza del termine fissato per l'esercizio dei medesimi diritti, per almeno due sedute (invece di cinque, come previsto dal previgente art. 2441, co. 3, c.c.).

LEGISLAZIONE OSSERVATORIO

COSA SONO E A COSA SERVONO GLI SMART CONTRACT?

Circa un anno fa l'Italia ha inserito nel decreto Semplificazioni una prima norma di definizioni di "smart contract" e di "tecnologie basate su registri distribuiti", attribuendo ai primi (se operanti sulle seconde) il valore di forma scritta, previo rispetto di determinate caratteristiche.

Si parla molto di smart contract e blockchain, ma cosa sono e cosa servono non è sempre chiaro anche in ragione della carenza di una normativa europea di riferimento.Gli Smart Contract innanzitutto non sono una novità da associare necessariamente alla Blockchain. In effetti sono stati oggetto di sperimentazione già negli Anni '90 e sono stati ideati ben prima, e hanno una loro specifica dimensione a prescindere dalla Blockchain. Certamente il fenomeno Blockchain sta permettendo di avere garanzie di affidabilità e sicurezza necessarie per affermarsi, ma in questa sede ci concentreremo sugli Smart Contract.

Lo Smart Contract non è un contratto in senso giuridico.

Di fatto uno Smart Contract è la "traduzione" o "trasposizione" in codice di un contratto – o di una parte di esso - in modo da verificare in automatico l'avverarsi di determinate condizioni e di eseguire in automatico azioni nel momento in cui le condizioni determinate tra le parti sono raggiunte e verificate. In altre parole, lo Smart Contract è basato su un codice che "legge" sia le clausole che sono state concordate sia la condizioni operative nelle quali devono verificarsi le condizioni concordate e si auto-esegue automaticamente nel momento in cui i dati riferiti alle situazioni reali corrispondono ai dati riferiti alle condizioni e alle clausole concordate.

A livello normativo, la legge maltese nel 2018 è stata tra le prime a introdurre il concetto, mentre in Italia la L. 12/2019 di conversione del D.L. 135/2018, ha introdotto per la prima volta nel nostro ordinamento le definizioni di "smart contract" e di "tecnologie basate su registri distribuiti", attribuendo ai primi (se operanti sulle seconde) il valore di forma scritta, previo rispetto di determinate caratteristiche.

Dispone infatti all'art. 8-ter del decreto:

"2. Si definisce "smart contract" un programma per elaboratore che opera su tecnologie basate su registri distribuiti e la cui esecuzione vincola automaticamente due o più parti sulla base di effetti predefiniti dalle stesse. Gli smart contract soddisfano il requisito della forma scritta previa identificazione informatica delle parti interessate, attraverso un processo avente i requisiti fissati dall'Agenzia per l'Italia digitale con linee guida da adottare entro novanta giorni dalla data di entrata in vigore della legge di conversione del presente decreto.

3. La memorizzazione di un documento informatico attraverso l'uso di tecnologie basate su registri distribuiti produce gli effetti giuridici della validazione temporale elettronica di cui all'articolo 41 del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014. 4. Entro novanta giorni dalla data di entrata in vigore della legge di conversione del presente decreto, l'Agenzia per l'Italia digitale individua gli standard tecnici che le tecnologie basate su registri distribuiti debbono possedere ai fini della produzione degli effetti di cui al comma 3".

Pertanto sono due gli aspetti fondamentali dello smart contract:

1. **automazione**: ovvero la capacità di autoesecuzione;
2. **avvio predeterminato**: avvio o inizio di una determinata azione al momento dell'avverarsi di una condizione (o set di condizioni) predeterminate.

A livello legale, gli smart contract se correttamente impostati ed implementati possono permettere indubbi vantaggi: (ad esempio) certezza dell'esecuzione degli obblighi contrattuali, trasparenza delle obbligazioni contrattuali (sia prima che dopo l'esecuzione delle clausole preimpostate), semplificazioni di alcuni processi. Ma pongono sicuramente alcune problematiche o dubbi, quali ad esempio: il rapporto con il "mondo esterno", chi risponde in caso di errori o problemi legati, come si coordina lo smart contract con la normativa generale sui contratti e - naturalmente - il rapporto con il GDPR.
Sulle problematiche degli Smart Contract è interessante un recente documento dell'European Union Blockchain Observatory & Forum, iniziativa della Commissione europea dove troviamo un ampio capitolo dedicato ad analizzare le questioni giuridiche sollevate dall'utilizzo di smart contract. Si ricorda che a livello europeo non c'è una normativa specifica di riferimento, quindi nel documento si esaminano le problematiche alla luce di altra normativa esistente.
Nel rapporto si sottolinea che secondo la definizione del padre di Ethereum, Vitalik Buterin, smart contract sta ad indicare un software, un codice, capace di essere eseguito senza il controllo da parte di un individuo.
Quindi lo smart contract non è un contratto inteso nel senso giuridico, ma è un codice. Esso tuttavia può servire per compiere su blockchain diverse azioni: creazione e passaggio di asset digitali, creazione di valuta, governance (DAO's) tra soggetti diversi ed anche creazione ed esecuzione di accordi tra le parti. Il rapporto dunque introduce una distinzione tra:

- **smart legal contract**, che sono codici in blockchain che rappresentano un accordo tra parti diverse;
- **smart contract** che hanno implicazioni legali, che sono nuove costruzioni con effetti legali.

Nel report si affrontano due temi importanti: se lo smart contract soddisfa i requisiti formali che ogni ordinamento nazionale richiede affinché un accordo tra le parti sia contrattualmente vincolante e la firma del contratto.
Per essere legalmente validi in Europa con il Regolamento eIDAS, le firme digitali su una blockchain devono essere verificate da un TSP. Uno smart contract dovrebbe essere in grado di accertare se la firma è valida, se si riferisce alla persona corretta e indentificata e, in tal caso, se quella persona ha davvero l'autorità per firmare. In contesti commerciali, ciò potrebbe significare essere in grado di accedere ai database dell'azienda o ad altri oracoli affidabili, che se del caso dovrebbero essere autorizzati.
La seconda questione riguarda il come conciliare lo smart contract – immutabile- con le cause sopravvenute che possono inficiare l'accordo sottostante.
Insomma, conclude il report sul punto, l'uso di contratti intelligenti non risolve o elimina il problema di violazioni del contratto, della responsabilità contrattuale ed esecuzione. Il problema della mancanza di strumenti disponibili per identificare facilmente gli attori su una rete basata su blockchain si pone quindi di nuovo.

Sono ancora aperti quindi molti problemi lato tecnico, la cui soluzione consentirebbe probabilmente di risolvere alcune criticità legali. Il problema più grosso, soprattutti per noi giuristi, resta l'assenza di una regolamentazione unica europea che sostituisca leggi nazionali frammentate, senza la quale è difficile ottenere la fiducia degli utilizzatori di tali strumenti.

Avv. Alessandra Delli Ponti
Studio Legale Stefanelli

PRIVACY

IL FURTO DEI DATI RISERVATI DI UN'AZIENDA DA PARTE DEL DIPENDENTE

Trib. Milano, Sez. Imprese, n. 8246/2019

Il Tribunale di Milano, con motivata decisione, ha condannato in solido tra loro due ex dipendenti di una società e il nuovo datore di lavoro, allorché al passaggio di consegne per l'ingresso presso la nuova società avvenuta in tempi diversi, hanno trasferito al nuovo datore di lavoro dati riservati appartenenti alla loro precedente azienda.
In particolare, sono stati ritenuti responsabili dal Tribunale meneghino due dipendenti di un'azienda di selezione del personale che, in fase di uscita da una società, hanno sottratto mediante fermo immagine alcuni dati appartenenti all'ex datore di lavoro, per poi condividerli ed utilizzarli una volta passati alla società concorrente.
Significativo tuttavia che, unitamente ai dipendenti infedeli, ad essere condannato in solido sia stato anche il nuovo datore di lavoro, per aver lo stesso fornito anche solo un contributo indiretto. In particolare, i dipendenti avevano trasferito quei dati nei PC aziendali della nuova azienda, li avevano utilizzati per accaparrarsi clientela

mediante offerte più vantaggiose di quelle precedentemente riconosciute dal vecchio datore di lavoro, e avevano goduto della copertura economica e legale a protezione della pacifica violazione del patto di non concorrenza apposto al precedente contratto dalla nuova azienda.
Ebbene, tutto questo comportamento si è rivelato in contrasto con l'art.99, primo comma del Codice della Proprietà intellettuale, con particolare riferimento all'utilizzo illecito di dati illegittimamente sottratti al titolare.
Anche questa pronuncia quindi da un lato ripropone l'attenzione che sempre di più sta interessando la migliore giurisprudenza sul **dato informatico** in quanto tale, e sul valore che esso assume. Vero è infatti che, chi detiene dei dati, ha il potere di stabilire modalità e finalità del trattamento, senza che terzi (dipendenti) possano discostarsi dalle indicazioni datoriali. In futuro, di fatto, questo costituirà sempre di più un asset importante dell'impresa, evidentemente capace di assumere grande rilievo sotto il profilo economico. Ogni sottrazione, anche ai meri fini detentivi di quei dati è di fatto illecita se non espressamente autorizzata. Le ripercussioni, sotto il profilo risarcitorio però, non sono solo in capo a chi materialmente pone in essere la sottrazione, ben potendo essere coinvolto chi, anche solo agevolando (inconsapevolmente) la predetta sottrazione, se ne è poi indirettamente servito.
Massima attenzione quindi, tanto nell'ambito privacy, quanto in quello lavoristico, sul legittimo trattamento di dati riservati, gli stessi idonei a fondare richieste risarcitorie (anche) in capo al personale infedele, e alle aziende che li utilizzano senza essere stati autorizzati a farlo dal titolare del trattamento.

Avv. Andrea Marinelli
Studio Legale Stefanelli

IMPRESE E VIOLAZIONI SUL TRATTAMENTO DATI: IL DANNO RISARCIBILE

In molte realtà aziendali l'avvento del GDPR ha portato la necessità di **apportare all'organizzazione interna una serie di importanti modifiche** per potere effettuare operazioni economiche, amministrative e commerciali trattando correttamente i dati personali in esse coinvolte.
La scelta di procedere con un percorso di adeguamento secondo quanto prescritto dal Regolamento UE 679/2016, infatti, anche in relazione alle sanzioni applicabili (e direttamente proporzionali al valore del fatturato) potrebbe condizionare fortemente l'andamento dei ricavi e dei guadagni aziendali.
Un punto che spesso viene sottovalutato, però, è quello relativo alle richieste di risarcimento dei danni (materiali e non) avanzati da chi ha subito una violazione illecita dei propri dati.
Proviamo ad inquadrare in modo corretto il concetto di risarcimento del danno da trattamento illecito di dati a partire da questo caso concreto del 2019 e da quanto l'associazione dei consumatori Altroconsumo sta facendo.

Class action diretta contro Facebook (avviata da Altroconsumo)

Lo sfruttamento abusivo dei dati personali da parte di Facebook, senza aver richiesto alcun consenso agli utenti direttamente coinvolti, ha condotto l'associazione dei consumatori italiana ad agire con il lancio di una Class Action ex art. 140-bis Codice del Consumo ai fini dell'accertamento delle responsabilità del danno subito dai consumatori.
Il proposito di Altroconsumo consiste nel voler garantire ad ogni utente registrato su Facebook un giusto risarcimento rispetto al danno subito.

Un importo, a partire da almeno 200 euro, ottenuto, per ogni anno di iscrizione al Social, dal valore economico dell'uso dei dati e dai danni morali subiti dagli utenti (l'importo dovrebbe corrispondere a 285 euro).
Il **risarcimento andrebbe a quantificare il mancato guadagno che il consumatore ha subito dallo sfruttamento dei suoi dati personali** ad opera di Facebook e del relativo illegittimo utilizzo di informazioni riservate per finalità commerciali non esplicitate all'interno dell'informativa.
La tutela procedimentale (giudiziale) prevista dal GDPR, infatti, non è solo diretta esclusivamente alla protezione dei diritti fondamentali e delle libertà individuali dell'interessato, ma è anche posta a presidio della tutela di interessi collettivi di categoria e del buon funzionamento del mercato: la dimostrazione concreta è l'effettiva possibilità di procedere a mezzo di azioni legali collettive a tutela degli interessi diffusi degli interessati ex art. 80 GDPR.
Dal punto di vista soggettivo, poi, è importante partire dal fatto che, nella prospettiva di voler accrescere la tutela dell'interessato che ha subito un danno da illecito trattamento dei propri dati personali, la responsabilità che può essere ascritta in capo al danneggiante è di tipo oggettivo e di natura extracontrattuale, in continuità con la pregressa lettura prevalente data dall'art. 15 del Codice Privacy.
Questo, concretamente, nella prospettiva del danneggiato, implica una serie di facilitazioni rispetto la prova del danno subito in quanto il danneggiato dovrà limitarsi a provare:

- la mera violazione dei principi e delle regole di condotta del GDPR;
- la gravità del pregiudizio ai fini della effettiva quantificazione del danno subito;
- il nesso di casualità tra l'evento e il danno, non dovendo dimostrare l'elemento psicologico (doloso o colposo) in capo al titolare.
- Deve infine rilevarsi che i danni risarcibili sono non solo quelli prevedibili e derivanti dall'esecuzione del contratto, ma anche quelli occorsi ulteriormente e in esso non ricompresi (cd. Danni imprevedibili).

Sarà infatti onere del danneggiante provare di non essere responsabile dell'accaduto dimostrando che l'evento dannoso non gli è in alcun modo imputabile ex art. 82 punto 3.
A conferma del principio del **favor** per il danneggiato risiede il fatto che quest'ultimo non può conoscere le regole e le misure tecniche organizzative interne ed è quindi onere del danneggiante procedere con la dimostrazione di essersi attenuto al principio di adeguatezza e di avere operato in conformità a quanto prescritto dal GDPR.
Tutto ciò avviene a partire dal fatto che, a fronte del **rischio di impresa correlato all'attività massiva di trattamento dei dati personali**, appare opportuno procedere con un necessario rafforzamento del rimedio risarcitorio in ragione dell'interferenza di tale attività con i fondamentali diritti e libertà della persona e della debolezza del soggetto su cui possono ricadere le conseguenze negative di uno scorretto trattamento dei dati che lo riguardano.

Per quanto riguarda gli aspetti civilistici, è sempre l'art. 82 paragrafo 6 del GDPR che stabilisce che l'unico rimedio giudiziale esperibile sia il ricorso innanzi ai giudici degli Stati membri.
Gli interessati che mirino al risarcimento dei danni, infatti, dovranno optare per il procedimento civile a cui si applicheranno le norme regolanti il processo del lavoro.
Questo, anche dal punto di vista della diminuzione dei termini che regolano il processo ordinario, potrà fornire al danneggiato una tutela breve ed efficace, volta ad un pronto reintegro del danno patito.
Per quanto riguarda la proposizione del ricorso giudiziale, già nel 2017 la Cassazione ha riconosciuto che l'interessato che riceva una decisione favorevole dal Garante ha la possibilità di agire successivamente in sede civile per il risarcimento dei danni, e che il provvedimento del Garante ha il valore di una "prova privilegiata" per l'accertamento della violazione da parte del giudice (Cass. Civ. 13151/2017).

Titolari e responsabili, quindi, non dovrebbero sottovalutare il rischio derivante dalla possibilità di "ricorsi a tappeto", in quanto una decisione sfavorevole del Garante nei loro confronti non solo è in grado di comprometterli inesorabilmente in sede civile, ma costituisce un incentivo per tutti quegli interessati che vogliano ricorrere in giudizio per ottenere il risarcimento dei danni.

Per concludere, in ogni caso, pare opportuno sottolineare come la scarsa conoscenza del contenzioso sul punto, sebbene i meccanismi di tutela giurisdizionale siano effettivi e regolati secondo le tempistiche abbreviate del rito del lavoro, sia soprattutto dovuto alla prospettiva di gestione e prevenzione del rischio da parte del titolare del trattamento stabilito dal legislatore europeo con il GDPR (principio dell'accountability).
La forma di tutela stragiudiziale, infatti, è stata privilegiata rispetto alla tutela mediante declinazione dei diritti e delle garanzie dell'interessato in sede giudiziale, soprattutto anche per i grossi danni all'immagine che potrebbero riverberarsi in capo al titolare.

Ciò detto, l'ipotesi di potere affermare i propri diritti in sede giudiziale è un'opportunità che nessuno dovrebbe sottovalutare: né l'impresa (titolare del trattamento) affinché possa effettivamente conformarsi sempre più a quanto prescritto dal GDPR e affinché le proprie azioni in tema di accountability possano poi fungere da corretti strumenti probatori di quanto svolto (nell'ottica di un eventuale contenzioso), né l'interessato che, trovandosi in una posizione più debole, potrà ottenere una pronuncia giudiziale per vedere tutelati i propri diritti.

Avv. Vittoria Piretti
Studio Legale Stefanelli

SICUREZZA PRODOTTI ED IMPIANTI

ESPORTARE IN CINA - *CHINA COMPULSORY CERTIFICATE (CCC)* OBBLIGATORIO PER GLI APPARECCHI A GAS DAL 1 OTTOBRE 2020

A qualche giorno dall'entrata in vigore della certificazione CCC anche per gli apparecchi a gas, ricordiamo l'iter necessario per l'ottenimento del marchio.
Come stabilito dall'Autorità cinese per la regolamentazione del mercato SAMR *(State Administration for Market Regulation),* dal **1 ottobre 2020** il marchio CCC diventerà **obbligatorio** anche per gli apparecchi a gas che vengono esportati in Cina.

In particolare, secondo quanto definito con il regolamento CNCA-C24-01:2019 per l'implementazione della certificazione obbligatoria di prodotto (Apparecchi a gas domestici), il marchio CCC diventerà obbligatorio per i seguenti prodotti:

- Piani cottura a gas a uso domestico (Single burner, carico termico nominale minore di 5,23 kW)
- Scaldacqua istantanei a gas a uso domestico (Carico termico nominale non superiore a 70 kW)
- Gas boiler (Carico termico nominale non superiore a 70 kW; Pressione massima dell'acqua 0.3 MPa; Massima temperatura dell'acqua 95 °C)

L'iter per il rilascio del marchio CCC per gli apparecchi a gas è lo stesso di quello attualmente applicabile per gli apparecchi elettrici:

- Attività di prova secondo norme nazionali GB da svolgere presso un laboratorio cinese riconosciuto;
- Visita ispettiva di fabbrica (preliminare) e sorveglianza annuale;
- Esame della documentazione e rilascio della Certificazione da parte di un Ente locale riconosciuto.

Il Certificato rilasciato avrà una validità di 5 anni e potrà essere rinnovato senza bisogno di ulteriori prove in caso di assenza di nuove edizioni delle norme applicate o di modifiche al prodotto.

Per ogni informazione,
LINK UTILI
IMQ:
www.imq.it
IMQ Certification (SHANGHAI)
http://www.imq-china.com/zh/index.html

Ing. Cecilia Cantaluppi
IMQ International Services Area

DIRETTORE RESPONSABILE
Maria Antonietta Portaluri

REDAZIONE
Alessandra Toncelli – Mirella Cignoni – Mattia Ciribifera

LA REDAZIONE RINGRAZIA PER LA COLLABORAZIONE

Avv. Arianna Ruggieri, BBM Partners, Buffa, Bortolotti & Mathis (Torino) - Avv. Luigi Eduardo Bisogno, Avv. Luca Casiraghi, Avv. Riccardo Fadiga e Avv. Leonardo Stiz, Freshfields Bruckhaus Deringer (Milano) - Ing. Cecilia Cantaluppi, IMQ International Services Area (Milano) - Avv. Alessandra Delli Ponti, Avv. Andrea Marinelli, Dott. Fabio Marinello e Avv. Vittoria Piretti - Studio Legale Stefanelli (Bologna).

Proprietario ed editore:
Federazione ANIE
Viale Lancetti 43, 20158, MI
Telefono (02) 3264.1
Direttore Responsabile
Maria Antonietta Portaluri
Registrazione del Tribunale
di Milano al n° 116 del
19/2/1996

TeLex Anie

FEDERAZIONE NAZIONALE IMPRESE ELETTROTECNICHE ED ELETTRONICHE
CONFINDUSTRIA

Pubblicazione a cura di:
Servizio Centrale Legale
Viale Lancetti 43, 20158, MI
Telefono (02) 3264.246
e-mail legale@anie.it
Diffusione via web www.anie.it

PRIVACY: CHI HA PAURA DELLA DPIA?

L'APPLICAZIONE DELLA VALUTAZIONE D'IMPATTO ATTRAVERSO UN CASO CONCRETO

Sono molte le fonti in rete che ne descrivono le caratteristiche e le regole per una corretta applicazione, ma la valutazione d'impatto, o Data Protection Impact Assessment (DPIA), prevista dall'Art. 35 del GDPR, è ancora spesso vista come un'attività troppo onerosa, impegnativa, o difficile da applicare.
Insomma, nonostante l'importanza di questo processo, che consente di (e costringe ad) applicare concretamente i principi di responsabilizzazione, privacy-by-design e by-default, sicurezza del dato, approccio basato sul rischio, e coinvolgimento di tutti i soggetti attivi in un trattamento, la DPIA appare ancora come uno "spauracchio" per molti titolari del trattamento.
Così, chi è abbastanza sapiente da non nascondere la testa sotto la sabbia, spesso preferisce comunque impiegarsi in articolate spiegazioni pur di dimostrare di non essere soggetto all'obbligo, invece che investire le stesse risorse per avviare il processo di valutazione.
La tendenza a evitare l'esercizio della valutazione d'impatto potrebbe essere talvolta motivata dalla complessità a reperire tutte le informazioni necessarie (operazione che spesso richiede un equilibrato coordinamento di varie funzioni con conoscenze e competenze diverse tra loro), dalla mancanza di una ben precisa linea su come strutturare tali informazioni (e ciò nonostante gli svariati utili strumenti messi a disposizione dalle Autorità garanti europee), ma anche dal mancato accesso a "fonti di ispirazione" o esempi pratici di svolgimento.
Nella speranza di poter contribuire a sensibilizzare sul tema, riportiamo in questo articolo l'applicazione dei diversi passaggi previsti per il corretto svolgimento di una valutazione di impatto nel contesto di un ipotetico progetto digitale che sarà avviato da una struttura sanitaria (N.d.A. ai fini del presente contributo, ci focalizzeremo unicamente sui requisiti della normativa sulla protezione dei dati, evitando eventuali considerazioni aggiuntive connesse all'applicazione della disciplina medica e sanitaria).
CASO: il poliambulatorio C. ha deciso di implementare una app, ad uso dei propri pazienti, che permetterà loro di gestire un diario clinico e usufruire di un sistema di notifiche (basato sulla terapia predisposta dal medico di riferimento) volto a supportare la corretta assunzione di farmaci.

La DPIA è obbligatoria?

Prima dell'avvio di ogni nuovo progetto, la norma richiede di considerare i principi di privacy-by-design e by-default, verificando altresì la necessità di svolgere la DPIA, che se da una parte risulta obbligatoria soltanto qualora il trattamento "possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche", dall'altra diventa particolarmente importante quando viene introdotta una nuova tecnologia di trattamento dei dati.
L'avvio di una app nel contesto sanitario dovrebbe fare intuitivamente propendere per la scelta di svolgere la DPIA, ma per valutare l'effettiva obbligatorietà della DPIA al caso in oggetto, decidiamo di fare riferimento alle linee guida WP248 pubblicate dal Gruppo di lavoro Art 29 per la protezione dei dati.
Nella seguente tabella riportiamo una sintesi dei nove criteri di riferimento indicati nelle linee guida, con le rispettive considerazioni sulla loro applicazione al nostro caso:

Criterio	Applicazione al caso
1. Valutazione o assegnazione di un punteggio, profilazione e previsione, in particolare su aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato	Possibile, a seconda di come saranno utilizzate le informazioni
2. Processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente sulle persone fisiche	No
3. Trattamento utilizzato per osservare, monitorare o controllare gli interessati, inclusi i dati raccolti tramite reti o la sorveglianza sistematica su larga scala di una zona accessibile al pubblico	Possibile, a seconda di come saranno utilizzate le informazioni
4. Dati sensibili o dati aventi carattere altamente personale	Sicuramente sì
5. Trattamento di dati su larga scala (tenendo conto, in particolare: a) Del numero di soggetti interessati; b) Della mole di dati; c) Della durata e persistenza del trattamento; d) Della sua portata geografica)	Possibile, ad esempio a seconda del numero di pazienti
6. Creazione di corrispondenze o combinazione di insiemi di dati	No
7. Trattamento di dati relativi a interessati "vulnerabili" (che possono includere minori, dipendenti, infermi di mente, richiedenti asilo, anziani, pazienti, e ogni caso in cui si possa individuare uno squilibrio nella relazione tra la posizione dell'interessato e quella del titolare del trattamento)	Sì
8. Uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative	Possibile, a seconda delle caratteristiche tecniche
9. Trattamento che impedisce l'esercizio di un diritto o di avvalersi di un servizio o di un contratto	No

La regola generale è che in presenza di almeno due criteri, occorre procedere con lo svolgimento di una DPIA. Pertanto, riscontrando una piena aderenza coi criteri 4 e 7 (e la possibilità che se ne possano individuare anche ulteriori), rileviamo la necessità di avviare la valutazione d'impatto.

Per semplicità, abbiamo utilizzato una sola fonte di riferimento, escludendo dalla nostra analisi l'Elenco dei trattamenti da sottoporre a valutazione d'impatto diffuso dal Garante per la Protezione dei Dati Personali, che in ogni caso risulta sostanzialmente in linea coi criteri delle Linee Guida Wp248.

Come svolgere la DPIA?

La norma, in nome dell'accountability, lascia ai Titolari la libertà di strutturare come ritenuto più opportuno la DPIA, e ne indica unicamente i contenuti minimi, che sono la descrizione del trattamento, la sua necessità e proporzionalità in relazione alle finalità perseguite, la valutazione dei rischi per gli interessati, e le misure previste per affrontarli.

Varie e autorevoli istituzioni hanno messo a disposizione strumenti, software e checklist che supportano lo svolgimento della DPIA. La nostra preferenza è per il percorso guidato dal software gratuito PIA, promosso dall'Autorità garante francese e disponibile in lingua italiana. Pertanto, tutti gli elementi riportati sotto trovano riscontro nella struttura di questo strumento.

Nel caso che analizziamo, il contesto del trattamento sarà rappresentato dal perimetro del servizio offerto dal poliambulatorio C., Titolare del trattamento, a cui sarà probabilmente affiancato almeno lo sviluppatore informatico esterno, nel suo ruolo di Responsabile del trattamento per le attività di assistenza tecnica, manutenzione, e conservazione dei dati relativi alla app nella propria infrastruttura.
Sarà ovviamente necessario esaminare ogni singolo dato gestito tramite la app (dati anagrafici, dati informatici, diagnosi e piani terapeutici elaborati dalla app, feedback forniti dai pazienti nel momento dell'assunzione dei farmaci corredati di data e ora, ecc.), e potrebbe essere opportuno presentare, ad esempio:

- eventuali form riportati nelle schermate dell'applicazione, con un focus che distingua le informazioni inserite dal medico da quelle fornite dal paziente stesso;
- eventuali collegamenti con il gestionale utilizzato dal poliambulatorio;
- i soggetti che hanno la possibilità di accedervi (i dati rimangono ad uso del solo paziente? Sono condivisi automaticamente con il medico, o forse sono coinvolti anche i familiari del paziente?);
- le modalità di salvataggio dei dati, ad esempio con una rappresentazione della struttura del database;
- i criteri e le modalità di cancellazione dei dati previste, ad esempio al termine della terapia;
- le caratteristiche di crittografia delle trasmissioni e del salvataggio dei dati.

Il fornitore informatico dovrà essere esplicitamente citato nella DPIA, oltre che coinvolto nella sua redazione, al fine di raccogliere tutte le informazioni tecniche e ottenere assistenza nella descrizione dei sistemi in supporto al funzionamento della app.
Il trattamento potrebbe essere giustificato dalla previsione di un beneficio per i singoli pazienti (in termini di rispetto delle prescrizioni terapeutiche) e per la struttura sanitaria

stessa, ma occorrerà valutare la necessità e la proporzionalità del trattamento, presentando una serie di dettagli che permettano di garantire il rispetto della liceità del trattamento e della trasparenza nei confronti del paziente: ad esempio, l'informativa sul trattamento dei dati potrebbe essere presentata in fase di installazione dell'applicativo e lasciata a disposizione sul sito della struttura, ma anche essere esposta al paziente direttamente dal medico durante una visita. Ulteriori considerazioni sulla base giuridica dei trattamenti dovrebbero poi portarci a esporre le modalità di gestione del consenso all'attivazione del servizio offerto tramite la app.
Infine, decidiamo di presentare una serie di funzioni dell'app che supportano l'esercizio dei diritti da parte degli interessati, come la possibilità di effettuare il download di un report contenente i propri dati, una sezione per gestire autonomamente la loro condivisione con uno o più medici, e un'altra dove è consentito modificare, aggiornare o eliminare il proprio profilo.

Quali rischi identificare e come valutarli?

Aspetto fondamentale per una corretta analisi dei rischi è mantenere sempre il focus sull'interessato.
I rischi, da individuare con l'obiettivo di raggiungere il massimo livello di dettaglio possibile (il software PIA offre un primo ventaglio di possibilità), finiranno sostanzialmente col confluire all'interno delle categorie di accesso non autorizzato (violazione della riservatezza), modifica indesiderata dei dati (violazione di integrità), e perdita di dati (violazione della disponibilità), ma entrare nel vivo dell'attività, contestualizzare il trattamento e considerare ogni possibile minaccia risulterà fondamentale per individuare anche in un secondo momento le specifiche misure di mitigazione.

Nel caso dell'app, ad esempio, si potrebbero verificare accessi non autorizzati ai dati, legati a una cattiva applicazione della politica di gestione delle password da parte dei medici, così come a un'infiltrazione nelle comunicazioni (deliberata e malevola) effettuata da attaccanti esterni. Potremmo includere anche l'estrazione illegale del database da parte di un amministratore di sistema autorizzato dal nostro fornitore, e ciascuna di queste eventualità avrà impatti differenti e richiederà attenzioni diverse per mantenere controllato il rischio.

Una volta individuate tutte le fonti, la vera e propria valutazione dei rischi dovrà seguire un processo obiettivo, come nell'uso delle comuni matrici costruite su "probabilità" e "gravità" dei rischi. Si sconsiglia tuttavia la semplice attribuzione di un valore numerico arbitrario, sprovvisto di adeguata spiegazione dei criteri che hanno guidato la vera e propria stima.

Come individuare le misure di mitigazione?

Una volta individuati i rischi connessi al trattamento, occorrerà abbinarli ad un elenco di misure di sicurezza volte a mitigarli.
Ipotizziamo di aver precedentemente individuato il rischio di malfunzionamenti della app, valutando un elevato rischio di impatto sulla salute del paziente, qualora il sistema di notifiche non rispecchiasse le aspettative previste dal medico. Non potendo intervenire direttamente sulla gravità di questo scenario, potremmo decidere di ridurne la probabilità, pretendendo una rigida procedura di test e verifica del software, in occasione di ogni aggiornamento da parte dello sviluppatore.

Altre misure di sicurezza potrebbero essere efficaci nel ridurre molti dei rischi individuati (ad esempio, pianificando sessioni di formazione specifica volta a evitare errori da parte del personale medico, oppure optando per soluzioni tecniche di criptazione o

pseudonimizzazione dei dati); in altre circostanze, si potrebbero anche prediligere per misure più stringenti e decidere di eludere determinati rischi, evitando completamente di raccogliere determinati tipi di dati, o utilizzando tecnologie completamente differenti da quelle previste in un primo momento.

Come terminare la DPIA?

Individuare correttamente i rischi e le misure di mitigazione è certamente un'attività complessa, ed è probabilmente impossibile avere un elenco esaustivo e applicabile a qualsiasi contesto. Anche e soprattutto per questo motivo è importante che tutti i soggetti che possono contribuire con le proprie competenze alla gestione sicura del trattamento siano coinvolti nello svolgimento della DPIA.

In particolare, nella fase finale della valutazione di impatto, è fondamentale disporre della supervisione del DPO, che potrà suggerire ulteriori implementazioni e al quale sarà richiesto di approvare ogni valutazione svolta, prima dell'avvio dell'attività.
La DPIA, quindi, dovrà prendere la forma di un processo continuo: l'app del nostro poliambulatorio potrebbe divenire obsoleta e vulnerabile insieme al progresso tecnologico, e occorrerà pianificare un regolare aggiornamento della sua valutazione d'impatto.
D'altra parte, non è nemmeno necessario eliminare ogni rischio: il poliambulatorio C. potrebbe decidere che alcuni dei rischi rilevati siano accettabili, dati i benefici del trattamento per i pazienti e le difficoltà di mitigazione. Tuttavia, in presenza di un rischio elevato nonostante le misure di sicurezza applicate, sarà necessario consultare l'Autorità garante prima di procedere.

Conclusioni

Lo scopo ultimo del GDPR non è quello di impedire il trattamento dei dati o limitare l'applicazione delle nuove tecnologie, bensì garantire che ogni attività venga svolta nel rispetto delle libertà e dei diritti della persona. La valutazione di impatto sulla protezione dei dati rappresenta senza dubbio un percorso importante (nella sua doppia accezione di rilevante e impegnativo!), ma è perfettamente in linea con tale approccio.
Per riscattare la DPIA dall'aura terrificante che gli è stata attribuita, sarà necessario comprendere a fondo la sua utilità, spostare l'attenzione dal perimetro della sua obbligatoria applicazione, e concentrarsi sui numerosi vantaggi che derivano da un effettivo approccio basato sul rischio: così, i più "coraggiosi" e lungimiranti si accorgeranno che saper fare emergere le mancanze, individuare le criticità, e prevenire i problemi che caratterizzano ogni progetto, non potrà che essere funzionale ed efficace alla sua buona riuscita.

Dott. Fabio Marinello
Studio Legale Stefanelli