

Are you experienced?

SPECIALE PRIVACY



KnowIT. Rivista scientifica trimestrale gratuita per i manager della governance digitale e della privacy.

Testata iscritta al n. 6/2016 del Registro della Stampa del Tribunale di Lecce il 23 maggio 2016 - ISSN 2532-1684

Direttore responsabile: Silvia Riezzo

Direttore editoriale: Andrea Lisi

Comitato di redazione: Adriana Augenti - Angela Busacca - Marco Camisani Calzolari - Franco Cardin - Fabrizio Cirilli - Giorgio Confente - Alessandro Di Maggio - Fernanda Faini - Massimo Farina - Laura Flora - Luigi Foglia - Lino Fornaro - Corrado Giustozzi - Nello Iacono - Michele Iaselli - Donato Limone - Massimiliano Lovati - Giovanni Manca - Marco Mancarella - Alberto Manfredi - Paolo Maresca - Daniele Minotti - Romano Oneda - Francesca Panuccio Dattola - Nazzareno Prinzivalli - Morena Ragone - Ruben Razzante - Franco Ruggieri - Giancarmine Russo - Fulvio Sarzana - Marco Scialdone - Laura Strano - Fabio Tommasi - Sarah Ungaro

Editore: Clio S.r.l. Via 95° Rgt. Fanteria n°70 - 73100 Lecce. Tel. +39 0832 344041 - Fax +39 0832 340228 - www.clio.it - info@clio.it

Indice

Prontuario per professionisti della privacy: are you experienced?	4
I nuovi artt. 2-ter e 2-sexies del Codice Privacy: interventi sul diritto nazionale presupposto	9
Controlli a distanza: quando sono leciti	12
Il trattamento di dati personali in ambito sanitario dopo l'entrata in vigore del D.Lgs. 101/2018	14
Dispositivi wearable e dati sanitari: le 8 privacy design strategies nella pratica	16
Accreditamento e certificazione nel Regolamento UE 2016/679: un'introduzione	19
Gli "zombie digitali": l'eredità dei dati personali nella società digitale	21
L'impatto del GDPR nella Chiesa cattolica	23

Prontuario per professionisti della privacy: are you experienced?

Andrea Lisi - *Avvocato, Direttore Editoriale KnowIT, Coordinatore Digital&Law Department e Presidente ANORC Professioni*

Perdonerete l'apertura di questo intervento con il titolo di un album del 1967 di *Jimi Hendrix (Are you experienced?)*, ma è in fondo in questa domanda che si racchiude la portata realmente rivoluzionaria del Regolamento 2016/679/UE (General Data Protection Regulation), che non risiede unicamente nel solo (temutissimo) apparato sanzionatorio.

Sul punto, è il caso di ribadire che il **D.Lgs. 196/2003, come modificato dal D.Lgs. 101/2018** (e adesso rubricato "Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE"), è **pienamente applicabile dal 19 settembre 2018, sanzioni comprese. Precisazione tanto ovvia, quanto necessaria, sulla scorta di interpretazioni improvvisate e fuorvianti circolate negli ultimi tempi, sulla presunta sospensione delle sanzioni (definita improvvidamente "stato di grazia") nei primi otto mesi di applicazione**[1].

Ebbene in cosa risiede la vera novità? In cosa consiste la "rivoluzione" innescata ormai a livello europeo? A mio avviso, si tratta di un cambiamento radicale di "approccio": il nuovo framework europeo impone una presa di coscienza in termini di responsabilizzazione e ha inteso rendere consapevoli (non solo gli specialisti del settore) della complessità della "quarta dimensione", quella digitale, che pervade ogni nostra azione e interazione, possibile sempre e unicamente grazie al trattamento dei dati personali.

Occorre conoscersi, avere contezza della propria entità, per applicare correttamente i principi contenuti nel GDPR.

E in che modo si traduce questa responsabilizzazione? Con riferimento a un contesto sia pubblico sia privato corrisponde alla scelta documentata di ruoli, procedure e strumenti. Responsabilizzarsi significa anche (e soprattutto) fare i conti con una realtà professionale multidisciplinare, che necessita di essere alimentata dall'acquisizione delle giuste competenze e di crescere attraverso il confronto continuo e costante. Non è solo questione di applicazione (o di applicativi) quindi, ma anche e soprattutto di metodologie documentabili, in grado di farci capire (e di dimostrare che abbiamo capito) come procedere e con chi, per applicare i principi del GDPR (e quindi del "Codice della privacy" rinnovato e allineato alle nuove necessità del

GDPR in modo che sia interpretabile in piena compatibilità con esse).

In uno scenario (quello italiano) in cui non si assiste spesso alla perfetta "quadratura del cerchio" tra norma e prassi, è quanto mai singolare per un giurista udire di strumenti (e termini) nuovi, quali: verifica delle procedure, check list, registri obbligatori, procedure di assessment e mappatura dei rischi, prevenzione e gestione del data breach, nonché monitoraggio e controllo; termini che rappresentano la traduzione reale di quanto previsto e "standardizzato" per tutto il continente europeo, e necessariamente tradotto a livello nazionale. A poco più di tre settimane dall'entrata in vigore del D. Lgs. 101/2018 di adeguamento UE, si avverte così da parte degli "addetti ai lavori" il bisogno di completare la selezione e l'adozione di quegli strumenti operativi pienamente conformi al principio di accountability, quintessenza del GDPR, e in grado di garantire lo sviluppo di processi armonizzati. Non a caso il Garante è recentemente intervenuto [2] per rendere disponibili delle **FAQ sul Registro delle attività di trattamento, corredate da modelli "semplificati" per Titolare e Responsabile.**



Procedendo con ordine, proviamo a ricostruire una sorta di "prontuario" di metodi e strumenti necessari per titolari, responsabili, DPO (Data Protection Officer) e non ultimo "consulenti privacy", che scelgono di "fare per bene" il loro lavoro:

Una, nessuna, centomila check list

Una "check list" con domande specifiche da fare è il primo passo per entrare in contatto con la nostra realtà professionale, aziendale e/o amministrativa. Il primo identikit da tracciare è quello del reparto già impegnato ad

occuparsi direttamente della materia (in genere quello amministrativo o informatico, o legale...sperando che questo reparto realmente esista!) allargando il tratto ad altri uffici più “delicati”, sulla base dei trattamenti di dati posti in essere al loro interno (ad esempio il reparto risorse umane, o l’ufficio marketing e comunicazione, quello IT e così via).

Durante questo primo audit (che può richiedere anche più check list, in rapporto all’organizzazione di riferimento) è possibile riuscire a ottenere quanto meno una mappatura completa (pur se generica) del modus operandi adottato, individuando e analizzando l’appropriatezza di:

- lettere di nomina degli incaricati e degli amministratori di sistema;
- clausole contrattuali con gli eventuali responsabili del trattamento;
- informative (dipendenti, clienti, utenti/pazienti ecc.);
- modelli di consenso;
- DPS se adottato e mantenuto aggiornato;
- policy e/o regolamenti interni in materia di trattamento dei dati personali;
- registri/elenchi hardware e software;
- eventuali procedure certificate
- etc.

Le check list consentono di effettuare un primo screening delle criticità e degli eventuali gap da colmare e, quindi, di avviare la successiva pianificazione degli interventi necessari. In questa fase, si può già riconoscere se la realtà con cui si ha a che fare debba dotarsi obbligatoriamente di un DPO (Data Protection Officer) o se per natura e dimensioni è in grado di auto regolamentarsi.

Adottare ed implementare il registro obbligatorio del trattamento dati

L’introduzione di un registro obbligatorio delle attività svolte è prevista espressamente dall’art. 30 del GDPR ed è stata più volte ribadita e caldeggiata del Garante,.

Obbligatorietà che si fa duplice, poiché oltre a riguardare il possesso dello stesso, a essere obbligatoria è soprattutto la sua corretta, aggiornata e puntuale compilazione. Le disposizioni sono chiare e precise e lasciano poco ai margini di errore, infatti l’art 30 del GDPR[3] stabilisce che: *ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità.*

Tale registro contiene tutta **una serie di indicazioni che permettono da un lato di adeguarsi alla norma, dall’altro di creare delle procedure (sartoriali) rispetto ai sistemi di gestione interni.** Le disposizioni in merito, pressoché intuitive e di facile applicazione a tutti i livelli di trattamento, si riferiscono essenzialmente a:

- a. il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;
- b. le finalità del trattamento;
- c. una descrizione delle categorie di interessati e delle categorie di dati personali;
- d. le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
- e. ove applicabile, i trasferimenti di dati personali verso un paese terzo o un’organizzazione internazionale, compresa l’identificazione del paese terzo o dell’organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell’articolo 49, la documentazione delle garanzie adeguate;
- f. ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- g. ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all’articolo 32, paragrafo 1.

I registri **non vanno mai considerati come documenti finiti, ma pensati come schema di riferimento** che può per esigenze dinamiche e temporali essere plasmato senza snaturarsi della propria natura di raccolta e conservazione.

Definire i principali attori e loro responsabilità

Dopo aver compiuto questi passi, ci troviamo in una fase intermedia del nostro processo di assessment, un punto cruciale dell’intera attività. Un momento questo, in cui abbiamo a disposizione una mappatura completa dei flussi dei dati personali sia all’interno che all’esterno dell’organizzazione e quindi, da adesso fino alla fine del processo di adeguamento, **saranno le scelte del “professionista della privacy” a fare la differenza.** Scelte che vertono essenzialmente sulle dinamiche procedurali come:

- l’individuazione dei responsabili del trattamento in linea con i principi sanciti dall’art. 28 del GDPR e la definizione dei contenuti vincolanti del contratto o di altro atto giuridico;
- la profilazione di eventuali referenti interni per la gestione delle politiche aziendali in materia di protezione dei dati personali;
- la definizione di un sistema di controllo periodico (audit interno) che consenta il costante monitoraggio del livello di compliance con il GDPR;
- la definizione di un piano formativo in grado di armonizzare le competenze interne delle diverse funzioni coinvolte.

Non ci resta che avviarcì così a un indispensabile check generale del lavoro svolto fino ad ora, così da poter rilevare e correggere eventuali gap (normativi e applicativi) tra quanto svolto (compreso la redazione della documentazione obbligatoria) e lo spirito (funzionale) del GDPR.

Diritti e doveri. Due facce della stessa medaglia

La richiesta di normalizzazione alle specifiche del Decreto di adeguamento 101/2018 ha messo in difficoltà, almeno in prima istanza, gran parte degli attori coinvolti: le criticità applicative sono però meno invasive di quanto si possa credere. **Quello che la Comunità Europea ha regolamentato (e il nostro Garante ha ribadito) non è altro che la formalizzazione di un'esigenza di tutela resa urgente dalla liquidità che caratterizza il transito di ingenti quantitativi di dati personali, nell'era della "quarta rivoluzione" industriale. Il GDPR ha solo definitivamente chiarito gli obblighi incombenti sul titolare, rafforzando il complesso di garanzie e procedure da osservare minuziosamente nel rapporto con gli interessati, attraverso l'implementazione di procedure finalizzate ad agevolare l'osservanza degli obblighi stabiliti per i responsabili del trattamento dei dati e l'esercizio dei diritti da parte degli interessati [4].**

Si ha spesso una percezione distorta delle procedure, concepite generalmente come qualcosa di rigido e poco funzionale al naturale decorso di vita operativo delle organizzazioni, più o meno complesse. Il GDPR esorta invece a ridisegnare queste procedure, in maniera sartoriale rispetto alle esigenze della propria organizzazione di riferimento, sulla base delle reali necessità esistenti, in modo che esse consentano proattivamente di rispettare i principi previsti dall'art. 5 del GDPR, verificando anche se – pur in caso di assenza di obbligo – non sia utile dotarsi comunque di un DPO (Data Protection Officer o Responsabile per la protezione dei dati personali). **Il DPO, infatti, è un professionista (sia esso soggetto interno o esterno all'organizzazione di riferimento) che deve svolgere una funzione con competenze multidisciplinari e trasversali tra loro, rispetto alle materie trattate.** La sua responsabilità principale è quindi quella di osservare, valutare e organizzare la gestione del trattamento di dati personali (e dunque la loro protezione) all'interno di un'azienda (sia essa pubblica che privata), affinché questi siano trattati nel rispetto delle normative privacy europee e nazionali [5].

Mappatura dei rischi, misure di prevenzione e gestione data breach

Come in qualsiasi processo di assessment efficace ed efficiente, non si può prescindere dalla mappatura dei rischi (ex artt. 24 e 32 del GPPR) intesa come strumento di

prevenzione e cura da possibili attacchi. Sarà assolutamente necessario (ex artt. 24 e 32 del GPPR):

- individuare i possibili ambiti di rischio che dovranno essere oggetto di valutazione;
- definire la metodologia di analisi dei rischi più adatta alla realtà organizzativa aziendale con particolare riferimento ai sistemi informativi;
- analizzare (per ogni trattamento o per trattamenti simili) sia i rischi connessi ai trattamenti effettuati senza l'utilizzo di strumenti elettronici, che quelli relativi alla configurazione dei sistemi informativi e ai software utilizzati;
- censire le attuali misure di sicurezza organizzative, fisiche e logiche;
- definire le misure di sicurezza necessarie a ridurre il rischio entro un livello di accettabilità (es. pseudonimizzazione, cifratura ecc.);
- verificare tutti gli applicativi adottati e da adottare e avviare politiche di controllo in linea con i principi di privacy by design e privacy by default (art. 25 GDPR);
- etc.

In questa fase è opportuno concentrarsi anche sulle possibili violazioni nel trattamento di dati personali (artt. 33 e 34 GDPR), quindi:

- definire e integrare le procedure di incident management per la gestione dei data breach, in modo da ridurre il più possibile il termine che intercorre tra la violazione e il momento in cui ci si accorge della violazione
- implementare un sistema di file log che consenta la raccolta di tutte le necessarie informazioni a supporto delle violazioni e delle opportune indagini sottostanti;
- impostare il registro delle violazioni;
- definire la modulistica per le notificazioni all'autorità di controllo (art. 33) e le comunicazioni agli interessati (art. 34).

Monitoraggio e controllo

Il principio di *accountability* non prevede più la verifica preliminare da parte dell'autorità di controllo (richiesta in passato prevista dall'art. 17 - oggi abrogato - del nostro Codice), ma diviene indispensabile (ex art. 35 del GDPR):

- individuare, i trattamenti per i quali è necessario effettuare la valutazione d'impatto;
- individuare la metodologia più appropriata da utilizzare per la valutazione d'impatto;
- effettuare la valutazione d'impatto per singoli trattamenti (o per gruppi simili di trattamenti che

presentino rischi analoghi) nonché le necessarie misure tecniche ed organizzative per attenuarli;

- predisporre e conservare la documentazione relativa alla DPIA (Data Privacy Impact Assessment);
- definire le modalità per il monitoraggio e l'eventuale revisione della DPIA.

Ovvio anche che, nel momento in cui le nostre azioni ci sembrano non bastare per minimizzare i rischi di carattere elevato evidenziati nella DPIA, allora si potrà (eccezionalmente) avviare un processo di consultazione preventiva con l'Authority (art. 36 GDPR).

Conclusioni

Le azioni descritte in questo (breve) prontuario sono certamente da accompagnare a letture approfondite del “nuovo” Codice per la protezione dei dati, che dovremo tutti fare. A prescindere da tutto occorre però non dimenticare l'aspetto più importante per la corretta applicazione della normativa europea e cioè: conoscersi e dimostrare di aver provato a mappare con serietà la propria organizzazione, al fine di avviare un percorso sostanziale e non solo formale di adeguamento. La ricetta del perfetto adeguamento può richiedere settimane o mesi o anche anni (a seconda della complessità dell'organizzazione di riferimento) per la sua riuscita, ma l'importante è tener presente che la semplificazione della norma si può raggiungere solo attraverso un'intesa pratica di conoscenza della propria realtà.

Resta solo da chiedersi: avremo tutti il coraggio (o purtroppo anche solo la voglia) di essere “experienced” ossia, di conoscerci davvero fino in fondo?

[1] Questa *famigerata* sospensione di cui si è tanto parlato e scritto prima che il decreto di adeguamento al GDPR venisse finalmente pubblicato in Gazzetta Ufficiale, è stata, effettivamente, suggerita da Camera e Senato, nei rispettivi pareri sullo schema di Decreto di adeguamento, invitando il Governo a valutare la possibilità che il Garante, in una fase transitoria, in ogni caso non inferiore a 8 mesi, successiva all'entrata in vigore del decreto legislativo, non irroghi sanzioni alle imprese, ma disponga ammonimenti o prescrizioni di adeguamento alla nuova disciplina. Raccomandazione, questa, mai tradotta in atto nella redazione del testo definitivo del Decreto (né, peraltro, sarebbe stato diversamente ipotizzabile, data l'evidente antinomia di una eventuale sospensione delle sanzioni rispetto al GDPR, che è fonte sovraordinata al diritto nazionale). Ad alimentare l'equivoco, peraltro, ha contribuito l'ambigua formulazione dell'art. 22 del D.Lgs. 101/2018 che, al comma 13, dispone che per i primi otto mesi dalla data di entrata in vigore del presente decreto, il Garante per la protezione dei dati personali tiene conto, ai fini dell'applicazione delle sanzioni amministrative e nei limiti in cui risulti compatibile con le disposizioni del Regolamento (UE) 2016/679, della fase di prima applicazione delle disposizioni sanzionatorie. La sospensione evidentemente non c'è e le sanzioni amministrative saranno applicate senza alcuna esenzione. Ciò che si raccomanda al Garante, nei primi otto mesi dall'entrata in vigore del Decreto di adeguamento, è, piuttosto, l'impiego di un criterio di bilanciamento nella graduazione delle sanzioni amministrative, attenuandone, eventualmente, la severità, nella misura in cui il disvalore della violazione risulti attenuato dalla complessità del percorso di adeguamento della propria organizzazione al nuovo quadro

normativo in materia di protezione dei dati personali. Un percorso che dovrà essere, comunque e necessariamente, avviato, senza ulteriori indugi.

[2] [Faq del Garante sul Registro delle attività di trattamento](#)

[3] Dalle già citate Faq del Garante troviamo conferma della generale opportunità di questo adempimento. Chi è tenuto a redigerlo? Tutti i titolari e i responsabili del trattamento sono tenuti a redigere il Registro delle attività di trattamento (v. art. 30, par. 1 e 2 del RGPD). In particolare, in ambito privato, i soggetti obbligati sono così individuabili: imprese o organizzazioni con almeno 250 dipendenti; qualunque titolare o responsabile (includere imprese o organizzazioni con meno di 250 dipendenti) che effettui trattamenti che possano presentare un rischio – anche non elevato – per i diritti e le libertà dell'interessato; qualunque titolare o responsabile (includere imprese o organizzazioni con meno di 250 dipendenti) che effettui trattamenti non occasionali; qualunque titolare o responsabile (includere imprese o organizzazioni con meno di 250 dipendenti) che effettui trattamenti delle categorie particolari di dati di cui all'articolo 9, paragrafo 1 RGPD, o di dati personali relativi a condanne penali e a reati di cui all'articolo 10 RGPD.

Si precisa che le imprese e organizzazioni con meno di 250 dipendenti obbligate alla tenuta del registro potranno comunque beneficiare di alcune misure di semplificazione, potendo circoscrivere l'obbligo di redazione del registro alle sole specifiche attività di trattamento sopra individuate (es. ove il trattamento delle categorie particolari di dati si riferisca a quelli inerenti un solo lavoratore dipendente, il registro potrà essere predisposto e mantenuto esclusivamente con riferimento a tale limitata tipologia di trattamento). Al di fuori dei casi di tenuta obbligatoria del Registro, anche alla luce del considerando 82 del RGPD, il Garante ne raccomanda la redazione a tutti i titolari e responsabili del trattamento, in quanto strumento che, fornendo piena contezza del tipo di trattamenti svolti, contribuisce a meglio attuare, con modalità semplici e accessibili a tutti, il principio di accountability e, al contempo, ad agevolare in maniera dialogante e collaborativa l'attività di controllo del Garante stesso. Si invita altresì a consultare il documento interpretativo del 19 aprile 2018 del Gruppo ex art. 29 (ora Comitato europeo per la protezione dei dati) reperibile al [seguente link](#).

[4] Del resto come ribadito dalla Commissione al Parlamento il regolamento non ha modificato in modo sostanziale i concetti e i principi fondamentali della legislazione in materia di protezione dei dati introdotta nel 1995. La grande maggioranza dei titolari del trattamento e dei responsabili del trattamento che rispettano già le attuali disposizioni dell'UE non dovrà quindi introdurre importanti modifiche nelle proprie operazioni di trattamento dei dati per conformarsi al regolamento (Comunicazione della Commissione al Parlamento Europeo e al Consiglio - Bruxelles, 24.1.2018 COM(2018) - Maggiore protezione, nuove opportunità – Orientamenti della Commissione per l'applicazione diretta del regolamento generale sulla protezione dei dati a partire dal 25 maggio 2018).

[5] E proprio in merito alla figura del DPO, credo sia doveroso richiamare la recente sentenza del TAR Friuli Venezia Giulia n. 287/2018, che ha con autorevolezza affermato il principio della non obbligatorietà (e oserei dire superfluità) delle certificazioni per svolgere questa delicata funzione, sottolineandone la necessaria competenza anche in ambito giuridico. È utile ricordare che al coro di voci negative sulle certificazioni del DPO si è aggiunta anche quella altrettanto autorevole del Comitato europeo per la protezione dei dati (ex art. 68 del GDPR), che già da tempo ha tenuto a precisare in modo lapalissiano nelle Linee guida sulle certificazioni quanto segue: *To further specify what may be certified under the GDPR, the GDPR contains additional guidance. It follows from Article 42.7 that certifications under the GDPR are issued only to data controllers and data processors, which rule out for instance the certification of natural persons, such as data protection officers for example.*



Digital & Law
Department
www.studiolegalelisi.it

“ **Vi guidiamo
verso
l'innovazione
digitale
a norma** ”

Digital&Law Department
Via Vito M. Stampacchia, 21
73100 LECCE
Tel. e fax: +39 0832 25 60 65
info@digitalaw.it
www.studiolegalelisi.it

I nuovi artt. 2-ter e 2-sexies del Codice Privacy: interventi sul diritto nazionale presupposto

Enrico Pelino - *Avvocato, partner Grieco Pelino Avvocati, professionista del D&L NET e membro del consiglio direttivo Anorc Professioni*

La recente novella di adeguamento (d.lgs. 101/2018) del Codice privacy al Regolamento europeo sulla protezione dei dati personali (“GDPR”) ha fatto massiccio uso della possibilità di deroga e di precisazione permessa agli Stati membri.

Ci si potrebbe domandare se le scelte compiute, in ultima analisi rispondenti ad apprezzamenti di politica legislativa, fossero davvero in linea con i poteri delegati al Governo dall’art. 13.3 della legge 163/2017, ma il tema, non privo di stimoli giuridici, ci porterebbe troppo lontano dall’oggetto e dalle intenzioni di questo articolo.

Il diritto nazionale presupposto

Tra gli interventi nazionali di precisazione (non quindi di deroga) si collocano quelli che riguardano la nozione di diritto nazionale “presupposto”, ossia le disposizioni nazionali che costituiscono il necessario presupposto giuridico per l’applicazione della disciplina europea. In particolare, vogliamo qui soffermarci sugli articoli:

- 6.1.c) GDPR, vale a dire la necessità di adempiere a un obbligo giuridico («legal obligation» nel testo inglese);
- 6.1.e) GDPR, vale a dire la necessità di eseguire un compito di interesse pubblico o connesso con l’esercizio di pubblici poteri;
- 9.2.g) GDPR, vale a dire il trattamento di dati sensibili per motivi di interesse pubblico rilevante.

Tutte le disposizioni richiamate trovano indifferentemente applicazione a titolari soggetti pubblici o privati.

Spieghiamo meglio il senso del diritto presupposto: se, per esempio, un soggetto privato tratta dati personali sulla base di un obbligo giuridico – si pensi alla normativa in materia di antiriciclaggio per l’avvocato – l’obbligo è definito in concreto dal diritto nazionale. Nell’esempio fatto le disposizioni del d.lgs. 90/2017 risultano quindi diritto presupposto rispetto all’art. 6.1.c). Stesse considerazioni valgono per l’art. 6.1.e) e, *mutatis mutandis*, per il 9.2.g).

Restringere il diritto presupposto vuol dire restringere la base giuridica europea

È chiara dunque la rilevanza del concetto di diritto nazionale presupposto: da essa dipende la possibilità di richiamare o no, in concreto, le basi giuridiche europee appena ricordate. **Se si restringe o si allarga la nozione di**

diritto nazionale presupposto, si restringe o si allarga proporzionalmente lo spazio applicativo di quelle basi. Va a questo punto osservato che, nello schema europeo, ogni trattamento riceve una base per così dire “naturale”, ossia concettualmente più prossima di altre alle ragioni per cui viene svolto. Se, per esempio, esiste una disposizione dell’ordinamento nazionale, anche soltanto una semplice circolare ministeriale, che prescrive ai consociati di tenere una determinata condotta, il trattamento di dati personali implicito in quella condotta deve essere collocato nell’alveo della lett. c) dell’art. 6.1 GDPR, quale base “naturale”. Unica ragione del trattamento è infatti la necessità di osservare la disposizione contenuta nella fonte giuridica citata.

Ora, le fonti giuridiche sono molteplici ed includono perfino gli usi. E che cosa accade se il legislatore nazionale, dinanzi a questa molteplicità di fonti, circoscrive il diritto presupposto solo ad alcune di esse, escludendo per esempio gli usi, le circolari, i decreti ministeriali e una buona parte di altre fonti? Accade che il povero titolare del trattamento dovrà ricorrere, in maniera del tutto impropria, a una base alternativa, forzandola. Tipicamente, un privato ripiegherà in via surrogatoria su quella del consenso o dell’interesse legittimo, ma ciò risulterà inappropriato. Invero i trattamenti costruiti sulle lettere c) ed e) dell’art. 6.1 e sulla lett. g) dell’art. 9.2, nella regolarità dei casi, devono essere svolti dal titolare, che non può cioè esimersi dal farlo.

Ne segue che l’interessato subirà ugualmente il trattamento, ma su una base artificiosa rispetto a quella “naturale”. Supporre che la limitazione del diritto presupposto offra maggiori garanzie all’interessato è perciò del tutto inesatto: semmai avviene il contrario. È come avere un flusso d’acqua che scorre: se si abbassano alcune chiuse, si ottiene solo l’effetto di convogliare l’acqua sulle restanti, non certo quello di bloccare il flusso. Come il lettore avrà intuito, la criticità di cui parliamo è proprio quella introdotta a livello nazionale dal nuovo art. 2-ter e fatalmente ribadita dal 2-sexies Cod. priv.

Il 2-ter

Diciamolo subito: il 2-ter è una brutta disposizione, anche in senso estetico, se l’aggettivo può riferirsi a un testo normativo. Ha una formulazione macchinosa, ostile alla linearità. Ad esempio, per indicare che il secondo periodo del secondo comma si riferisce a soggetti pubblici e non a privati impiega una sciarada per solutori esperti: l’espressione «svolgimento di funzioni istituzionali», da cui l’interprete deduce la soggettività pubblica dei titolari del trattamento.

Ulteriore esempio: invece di parlare tout court di “dati sensibili” viene utilizzata una perifrasi di dodici parole, «dati ricompresi nelle particolari categorie di cui all’articolo 9 del Regolamento». Eppure “dati sensibili” non è un lemma tabù, lo troviamo definito al cons. 10 GDPR, dunque ha natura tecnica, e del resto era fino all’altro ieri in pieno uso nazionale, vigente il testo ante riforma del Codice privacy. Perché non mantenerlo se giova alla concisione e di conseguenza alla chiarezza espressiva? Stesso discorso per “dati giudiziari”: perché non conservare la formulazione per esigenze di sintesi?

E addirittura perché non arrischiarsi a definire una volta per tutte “comuni” i dati che non sono né sensibili né giudiziari? In definitiva sono più di venti anni che i pratici li chiamano così, una ragione c’è. Niente da fare: in luogo delle sole sei lettere dell’aggettivo “comuni”, troviamo oggi impiegata al comma secondo una frase complessa di ben trenta parole (davvero).

Sono scelte di legistica che è difficile condividere. **Nel 1840 Stendhal scriveva a Balzac che durante la stesura della Certosa ogni mattina era solito leggere due o tre pagine del codice Napoleone, «pour prendre le ton» prima di scrivere. Lo considerava un modello di stile e lo affascinava l’asciutto nitore delle parole. Tempi andati.**

Possiamo aggiungere – a dirla tutta – che il primo periodo del secondo comma dell’art. 2-ter e l’intero terzo comma appaiono completamente inutili, poiché già perfettamente assorbiti nell’orbita del primo comma (e comunque nell’interazione con il 2-sexies), dunque finiscono solo per avere un effetto depistante per il giurista meno addentro alla materia della protezione dei dati personali.

Nel verboso 2-ter, l’interprete saggio punterà perciò dritto solo a una manciata di parole: «legge e regolamenti nei casi di legge». Punterà dritto anche all’eccezione contenuta nel secondo periodo del secondo comma, ma non è materia del presente articolo e non è comunque esente da perplessità giuridiche.

Il 2-sexies

Dunque, legge e regolamenti nei casi di legge: per il legislatore italiano la base giuridica delle lett. c) ed e) dell’art. 6.1 GDPR è tutta qui.

Le cose non vanno meglio con il 2-sexies, collegato con l’art. 9.2.g) GDPR. Non tanto per la formulazione, ma perché la base “ristretta” è qui la stessa, né potrebbe essere diversamente una volta che si è data quella impostazione al 2-ter. Il problema ora però diventa particolarmente serio, perché nell’art. 9.2 ci si muove entro margini ben più angusti del 6.1: l’utilizzabilità della base offerta dalla lett. g) è davvero preziosa in un contesto nel quale la scelta di basi “surrogate” è minima.

A ciò si aggiunga che la riforma, anziché individuare o creare il meccanismo per individuare «le misure appropriate

e specifiche per tutelare i diritti fondamentali e gli interessi dell’interessato» richieste dal legislatore europeo, si limita a ripetere pedissequamente la clausola virgolettata, con l’effetto di circoscrivere ulteriormente l’utilizzabilità della base g) dell’art. 9.2: quante norme di legge o di regolamento nei casi di legge prevedono oggi specifiche misure privacy a tutela dell’interessato? **Molto poche.** Risultato: siamo ai limiti dell’inapplicabilità della lett. g), che tuttavia è strutturalmente fondamentale nel disegno del GDPR. Dalla riforma ci si sarebbe attesi un approccio di segno opposto: l’ampliamento della possibilità di fare ricorso alla base generale della lett. g), in un contesto, come quello del 9.2, già povero di basi generali.



Un caso concreto

Facciamo un esempio concreto dei problemi attuali. Ai sensi dell’art. 109.3 R.D. 18.6.1931 n. 773 e ss.mm., cd. “TULPS”, i gestori di servizi alberghieri e altre strutture ricettive hanno l’obbligo di comunicare alle questure territorialmente competenti, via informatica o a mezzo fax, le generalità delle persone alloggiate, secondo modalità stabilite con decreto del Ministero dell’Interno, sentito il Garante per la protezione dei dati personali.

Il Ministero ha provveduto con D.M. 7.1.2013, pubblicato in G.U. 17.1.2013, n. 14. Orbene, questo atto ministeriale prevede una serie puntuale di obblighi, che determinano altrettante operazioni di trattamento. È ad esempio il decreto in questione e non la norma primaria a definire le tipologie di dati da raccogliere: data di arrivo del soggiornante, giorni di permanenza, cognome, nome, sesso, data di nascita, luogo di nascita, cittadinanza, tipo del documento d’identità, numero del documento, luogo di rilascio. E inoltre, per i nuclei familiari: individuazione dell’altro coniuge e dei figli minorenni. Per i gruppi guidati: individuazione dei componenti del gruppo da parte del capogruppo, cfr. allegato tecnico al decreto.

Ugualmente, le modalità di trattamento sono previste dal decreto citato, che individua uno schema di catalogazione delle informazioni (tabella 1 allegata al decreto), le modalità di trasmissione informatica (allegato tecnico) e

quando procedere alla stessa oppure utilizzare l'invio attraverso fax (artt. 2 e 3).

Inoltre, sempre il decreto in commento stabilisce il dovere di conservazione per cinque anni delle ricevute di trasmissione alla questura, cfr. ivi art. 4.5.

In sostanza, siamo di fronte a una minuziosa disciplina anche in materia di dati personali, che ha la sua fonte in un decreto ministeriale di natura – si noti – **non regolamentare**, dunque in una fonte diversa dalla legge o dal regolamento contemplati all'art. 2-ter Cod. priv. **Bene, che cosa deve fare in questo caso il gestore dell'hotel? A ben vedere, si trova di fronte a un ventaglio di varie scelte tutte paradossali:**

- **violare il D.M. Interno 7.1.2013** al fine di non violare l'art. 2-ter Cod. priv. La scelta espone a serie conseguenze giuridiche e non può dirsi percorribile;
- **violare l'art. 2-ter Cod. priv.** al fine di osservare il D.M. citato, con le stesse conseguenze;
- **utilizzare come base il consenso** del soggiornante per raccogliere i dati predetti, comunicarli alla questura e quindi conservarli, ricorrendo con ciò a un'opzione pasticciata, di mera sussistenza, su base "surrogata" assai debole e peraltro soggetta all'alea della revoca in qualsiasi momento. Sconsigliabile. Stesso discorso qualora si precipiti il tutto nell'alveo del consenso contrattuale e si ricorra alla base di cui all'art. 6.1.b) GDPR. Perplessità anche nel ricorso alla base 6.1. f).

Tutte le ipotesi sopra indicate sembrano da scartare: non è questo un modo civile di applicare la normativa sul trattamento dei dati personali. Invero, a ben guardare, la soluzione meno assurda si palesa quella di: **svuotare parzialmente di senso i paletti del 2-ter Cod. priv. (e del 2-sexies)**, in chiave di interpretazione della norma, considerando comunque soddisfatta la condizione della fonte di legge o di regolamento per il solo fatto che tale fonte contenga un rinvio, **sia pure completamente in bianco**, ad altra fonte diversa dalla legge o dal regolamento, come avviene appunto per il citato art. 109.3 TULPS. La strada contiene indubbiamente una forzatura e di fatto disinnescia il meccanismo del 2-ter e del 2-sexies, ma – preso atto delle alternative sconcertanti – appare di gran lunga la scelta più accettabile e la meno perturbante. Certo è auspicabile che una soluzione siffatta sia confermata in via di interpretazione autentica da parte del legislatore.

Invero è auspicabile, in senso più radicale, un totale ripensamento delle fonti prescritte dal 2-ter e dal 2-sexies. Infatti, anche la strada indicata da ultimo non soddisfa che una parte della casistica, lasciando scoperte molte altre ipotesi: quelle in cui non si ravvisi un rinvio espresso a una fonte più specifica, ma siano comunque presenti norme di

dettaglio (es. circolari), diverse dalla legge e dal regolamento, che intervengano a precisare importanti profili del trattamento, facilmente tralasciati nei gradini più alti della gerarchia delle fonti.

Sul punto andrebbe valorizzato il cons. 41 GPDR, il cui dettagliato esame fuoriesce dalla sede attuale. Si può solo osservare che, diversamente da altre disposizioni, nel considerando citato l'unica deroga consentita dal legislatore europeo a quello nazionale riguarda le sole prescrizioni derivanti dall'ordinamento costituzionale. **Ciò dovrebbe far riflettere sulla liceità di interventi come quelli degli artt. 2-ter e 2-sexies che introducono deroghe nazionali cospicue al considerando menzionato.**

Controlli a distanza: quando sono leciti

Carmine Trovato - consulente esperto in data protection e presidente di DPO innovation

Giulia Tenaglia - avvocato esperto in data protection

Il GDPR (*General Data Protection Regulation*) lascia ampio margine di manovra agli stati membri per quanto concerne il trattamento dei dati nell'ambito del rapporto di lavoro: in questo senso l'art. 88 del Regolamento Ue 2016/679, consente espressamente l'adozione di "norme più specifiche" per definire diritti e libertà delle parti nel contesto nazionale. **La normativa di riferimento per la disciplina dei controlli a distanza è oggi dettata dall'art. 4 dello Statuto dei Lavoratori [1]. Per controlli a distanza devono intendersi tutte quelle attività di rilevazione effettuate sul luogo di lavoro e/o mentre viene resa la prestazione lavorativa, tali da determinare un controllo anche solo potenziale e indiretto sulla stessa prestazione resa dal lavoratore.**

Il *Jobs act* non ha mutato le definizioni, ma ha determinato un nuovo assetto della legittimità dei controlli nel tentativo di portare maggiore certezza in un ambito dominato da forti oscillazioni giurisprudenziali. Punto fermo, da tenere bene a mente quando si discute di controlli a distanza è il divieto di effettuare controlli occulti, ovvero tutte quelle attività svolte all'insaputa del lavoratore[2].

Definito ciò che è sicuramente illegittimo, possiamo delineare i tre requisiti che rendono invece lecito il controllo sul lavoratore.

1. **Rispetto delle finalità:** l'art. 4 comma 1 dello Statuto dei Lavoratori individua le finalità per cui può essere svolto il trattamento/controllo: organizzative e produttive, sicurezza sul lavoro o tutela del patrimonio aziendale;
2. **Accordo sindacale o autorizzazione dell'Ispettorato Nazionale del Lavoro**[3];
3. **Adeguata informativa:** al lavoratore deve essere fornita un'adeguata informativa recante le modalità d'uso degli strumenti e di effettuazione dei controlli.

Definiti i presupposti del controllo legittimo, lo stesso articolo prevede tuttavia delle eccezioni stabilendo al secondo comma che: la disposizione di cui al comma 1 non si applica agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze. La riforma ha sostanzialmente liberalizzato il controllo sugli "strumenti di lavoro" e sui sistemi di accesso ai luoghi di lavoro (ad es. sui badge). Per questi non è più necessario rientrare in una delle suddette finalità e nemmeno

stipulare l'accordo amministrativo o sindacale.

La definizione di strumenti di lavoro non è tuttavia un dato univoco e sicuramente sul punto la giurisprudenza avrà un ruolo determinante. Si rileva in particolare la distinzione tra *strumenti di controllo* e *strumenti di lavoro* poiché solo i secondi potranno rientrare nell'ambito di applicazione del secondo comma dell'art. 4 dello Statuto dei Lavoratori.

Sul punto si è espresso il Ministero del Lavoro con nota del 18 giugno 2015 affermando che gli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa come pc, tablet e cellulari non possono essere considerati strumenti di controllo a distanza - proprio perché sono "ontologicamente" strumenti di lavoro. Esemplicando può dirsi che la posta elettronica è da considerarsi uno strumento di lavoro, ma l'eventuale software installato in grado di raccogliere e analizzare taluni messaggi classificabili come "pericolosi" è uno strumento di controllo ed il suo utilizzo deve essere autorizzato dal sindacato o dall'Ispettorato Nazionale del Lavoro.

Ancora, con l'espressione *rendere la prestazione lavorativa*, il legislatore ha inteso che se lo strumento è un mezzo usato dal lavoratore per adempiere la prestazione, l'accordo o l'autorizzazione non servono.

La giurisprudenza sottolinea come lo strumento di lavoro, dovendo essere utilizzato ai fini della esecuzione della prestazione, può venire in rilievo ai fini dell'art. 4, comma 2, solo se il lavoratore ha un ruolo attivo nel suo utilizzo e, cioè, se quello strumento viene concretamente impiegato dal dipendente nello svolgimento delle mansioni (in questo senso Trib. Roma sez. lav. 24/03/2017).

Lo strumento deve essere nella disponibilità del dipendente e da questi effettivamente utilizzato nell'adempimento della prestazione, diversamente da quanto avviene con gli strumenti di controllo di cui all'art. 4, comma 1, rispetto ai quali il lavoratore è invece sempre soggetto passivo (si pensi alla videosorveglianza). Pertanto, partendo dalla distinzione tra strumenti di lavoro e strumenti di controllo, l'uso degli strumenti informatici deve essere assimilato alla prima fattispecie, in quanto messi a disposizione del lavoratore per rendere la prestazione; quindi i computer, i tablet ed i cellulari devono essere considerati come i moderni attrezzi di lavoro utilizzabili senza autorizzazione nel caso in cui vengano attribuiti al lavoratore per rendere la prestazione lavorativa oggetto del contratto di lavoro (Trib. Roma sez. lav. 24/03/2017).



Oltre allo strumento di lavoro, l'altro elemento da definire con chiarezza ai fini della legittimità del controllo è quello dell'adeguata informativa. Il rispetto della normativa sulla privacy determina un ampliamento della sindacabilità giudiziale dei controlli datoriali che non sarà più circoscritta al solo rispetto dei vincoli giuslavoristici ma sarà, dunque esteso.

L'informativa ha una duplice funzione: da un lato deve far conoscere al lavoratore i limiti da non superare (ad es. rendendo note le modalità di controllo sulla propria attività o indicando le modalità d'uso della strumentazione di lavoro, anche per fini privati) e dall'altro deve impedire un uso indiscriminato dei controlli da parte del datore.

Sul tema, nelle linee guida dedicate all'attività di controllo sull'attività lavorativa del Gruppo dei Garanti Europei, è possibile individuare i principi guida del trattamento dei dati in ambito lavorativo.

In particolare, molte delle comunicazioni poste sotto il controllo del datore godono di una copertura legislativa quali diritti fondamentali: questo implica che la proprietà dei mezzi elettronici sui quali circolano le informazioni non esclude il diritto dei dipendenti al segreto della corrispondenza. Il Gruppo dei Garanti Europei ha ribadito inoltre come il consenso non possa costituire la base legittimante per il trattamento dei dati in ambito lavorativo. In questo senso il legittimo interesse del datore di lavoro ad effettuare il controllo può essere invocato quale fondamento legale del trattamento solo se lo stesso è posto in essere per uno scopo legittimo e se è rispondente ai principi di proporzionalità, sussidiarietà e continenza. Il trattamento deve cioè esser ridotto al minimo necessario per il raggiungimento dello scopo.

Ciò implica che, anche nel caso in cui sia fornita

un'adeguata informativa al lavoratore, non è consentito un controllo indiscriminato. Devono essere rispettati i principi di minimizzazione e finalità del trattamento, per raccogliere solo quelle informazioni strettamente necessarie allo scopo perseguito. Così, ad esempio, l'accesso indiscriminato e continuo alla posta del lavoratore era e rimane un'attività di controllo assolutamente illegittima[4].

In ogni caso, al datore si richiede di privilegiare gli interventi di prevenzione rispetto a quelli repressivi e, solo quando i primi abbiano fallito, è ammesso il controllo (successivo) nelle forme stabilite dalla Statuto dei Lavoratori. Qualora si verificano comportamenti sospetti dunque, occorre procedere con controlli in forma anonima e su dati aggregati (solo in caso di persistenti anomalie potrà dirsi giustificato un accertamento su base individuale). Nel caso di mancato rispetto della disciplina delineata, i dati raccolti saranno inutilizzabili per fini connessi al rapporto di lavoro tra i quali l'erogazione della sanzione disciplinare. L'unica ipotesi in cui è possibile ipotizzare uno spazio di utilizzabilità del dato è quella della difesa di propri diritti in sede di giudizio (escluso ovviamente il contenzioso lavoristico).

L'art. 81 c.p.p., tuttavia, esclude la possibilità di utilizzo di prove illecite (i.e. dati personali illegittimamente raccolti) nel processo penale. Diversamente nel codice di procedura civile non vi è una simile previsione, ragion per cui, in un'ottica di bilanciamento degli interessi, è possibile che i dati raccolti in occasione di controlli illeciti siano ammessi come prova nel processo civile.

[1] Modificato dal D.lgs 151/2015, c.d. Jobs act e dal D.lgs 196/2003, a sua volta aggiornato a seguito dell'introduzione del recentissimo D.lgs 101/2018 - c.d. "Nuovo Codice Privacy".

[2] In questo senso si è sempre espressa sia la giurisprudenza di merito e di legittimità, che il Garante per la protezione dei dati personali, ad esempio nelle [linee guida per posta elettronica e internet del 2007](#)

[3] Sul punto va rilevata la diminuzione della centralità del sindacato essendo l'accordo sindacale e l'autorizzazione amministrativa perfettamente alternativi tra loro. Inoltre, al fine di garantire uniformità nelle prassi aziendali a livello nazionale, è prevista la possibilità per le imprese con unità produttive dislocate in diverse province o regioni di procedere all'accordo sindacale a livello nazionale e di ottenere l'autorizzazione dalla sede centrale dell'Ispettorato Nazionale del Lavoro.

[4] cfr. provvedimento del Garante del 22 dicembre 2016 relativo agli accessi alla posta elettronica dei dipendenti

Il trattamento di dati personali in ambito sanitario dopo l'entrata in vigore del D.Lgs. 101/2018

Franco Cardin - *consulente esperto privacy in ambito sanitario e componente del consiglio direttivo di ANORC Professioni*

Premessa

Il Regolamento (UE) 679/2016, noto anche come GDPR (General Data Protection Regulation), divenuto applicabile a partire dal 25 maggio 2018, prevede per alcuni specifici ambiti di trattamento - tra i quali vi è anche quello relativo al **trattamento dei dati genetici, biometrici e relativi alla salute** - la possibilità di ogni Stato membro di mantenere o introdurre norme nazionali al fine di specificare ulteriormente l'applicazione delle disposizioni contenute nello stesso. In attuazione della delega conferita dall'art. 13 della Legge 25 ottobre n. 163, dopo un iter particolarmente complesso - che di fatto non ha consentito di poter adeguare il D. Lgs. 196/03 al GDPR prima della data della sua effettiva applicabilità - lo scorso 4 settembre 2018 è stato pubblicato in Gazzetta Ufficiale il Decreto legislativo 10 agosto 2018, n. 101.

Tale decreto, entrato in vigore il 19 settembre scorso ha modificato il D.Lgs. 196/2003 [1], sia abrogando tutte le disposizioni ritenute incompatibili con quelle contenute nel GDPR, sia esercitando la facoltà di poter mantenere o introdurre disposizioni più specifiche oltre che per alcuni trattamenti, quali ad esempio quelli effettuati per l'adempimento di un obbligo legale o per l'esecuzione di un compito di interesse pubblico - anche con riguardo al trattamento di categorie particolari di dati personali quali ad esempio quelli genetici, biometrici e relativi alla salute. Con riferimento a questi ultimi, infatti, il paragrafo 4 dell'art. 9 del GDPR, prevede espressamente che *“Gli Stati membri possono mantenere o introdurre ulteriori condizioni, comprese limitazioni, con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute”*.

In attuazione di questa facoltà, riservata dal GDPR ai singoli Stati membri, il D. Lgs. 101/2018 ha inserito nel Codice privacy l'art. 2-septies, rubricato “Misure di garanzia per il trattamento dei dati genetici, biometrici e relativi alla salute”, nel quale è stabilito che, fermo restando il divieto di diffusione di tali dati, gli stessi possono essere oggetto di trattamento in presenza **di una delle condizioni alternative** di legittimità di cui al paragrafo 2 dell'art. 9 del GDPR ed **in conformità alle misure di garanzia** disposte dal Garante con proprio provvedimento - il cui schema deve essere sottoposto a consultazione pubblica - da adottare con cadenza almeno biennale.

Con tale provvedimento il Garante dovrà individuare e

adottare le misure di garanzia non solo tenendo in considerazione le specifiche finalità perseguite tramite il trattamento di ognuna delle predette categorie di dati, ma anche delle linee guida e delle raccomandazioni del Comitato europeo per la protezione dei dati e dell'evoluzione scientifica e tecnologica nel settore a cui tali misure sono rivolte.[2]

Al fine di evidenziare quali siano gli obblighi che i titolari del trattamento che operano in ambito sanitario - siano essi soggetti pubblici o privati - devono rispettare a partire dal 19 settembre scorso, si riportano di seguito quelle che si ritiene siano le più rilevanti novità introdotte dal medesimo decreto, con particolare riferimento ai dati relativi alla salute e a quelli genetici, trattati per finalità di tutela della salute e incolumità fisica dell'interessato o di terzi o della collettività.



Il Titolo V del D. Lgs. 196/03 come modificato dal D. Lgs.101/2018

Per adeguare l'ordinamento nazionale alle disposizioni contenute nel GDPR, riguardanti in particolare il trattamento dei dati relativi alla salute e quelli genetici per le predette finalità, l'art. 6 del D.Lgs. 101/2018 ha apportato significative modifiche al Titolo V della Parte II del Codice privacy che, come è noto, gli articoli da 75 a 94 definiscono la disciplina specifica per il trattamento dei dati personali in ambito sanitario. Nel rispetto dei criteri direttivi contenuti nella delega conferita al Governo, di cui si è fatto cenno in premessa, tali modifiche consistono sia nell'abrogazione di diversi articoli del predetto Titolo V, sia nella modifica/integrazione di quelli non espressamente abrogati.

Particolare rilevanza assume il novellato art. 75, in quanto specifica che *“Il trattamento dei dati personali effettuato per finalità di tutela della salute e incolumità fisica dell’interessato o di terzi o della collettività deve essere effettuato ai sensi dell’articolo 9, paragrafi 2, lettere h) ed i), e 3 del regolamento, dell’articolo 2-septies del presente codice, nonché nel rispetto delle specifiche disposizioni di settore”*.

Rinviano a quanto sopra evidenziato in merito all’art. 2-septies del novellato Codice privacy, si ritiene utile ricordare - anche per il positivo impatto in termini di semplificazione dei rapporti che ne derivano tra pazienti e soggetti pubblici/privati che erogano prestazioni sanitarie - che il GDPR prevede espressamente che i dati relativi alla salute possono essere legittimamente trattati:

- se ciò è necessario, tra le altre, anche per finalità di medicina preventiva, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell’Unione o degli Stati membri o conformemente al contratto con un professionista della sanità (cfr. art. 9, paragrafo 2, lett. h);
- se ciò è necessario per motivi di interesse pubblico nel settore della sanità pubblica (cfr. art. 9, paragrafo 2, lett. i);
- se tali dati sono trattati da o sotto la responsabilità di un professionista soggetto al segreto professionale (cfr. art. 9, paragrafo 3).

Coerentemente con quanto disposto dal novellato art. 75, pertanto, sono stati abrogati gli artt. 76 e 81 del D.Lgs. 196/03 con la conseguenza che a partire dall’entrata in vigore del D.Lgs. 101/2018, i soggetti pubblici e privati e gli esercenti le professioni sanitarie possono trattare legittimamente i dati personali relativi alla salute dei loro pazienti, per le finalità sopra specificate, senza il loro consenso.

Il D.Lgs. 101/2018 ha abrogato, inoltre, gli articoli 83 e 84 del Codice privacy riguardanti rispettivamente *“Altre misure per il rispetto degli interessati”* e *“Comunicazione di dati all’interessato”*. Considerato che le misure di garanzia che dovranno essere definite dal Garante in attuazione dell’art. 2-septies del novellato D.Lgs. 196/03, dovranno riguardare anche le cautele da adottare relativamente ai profili organizzativi e gestionali in ambito sanitario, nonché le modalità per la comunicazione diretta all’interessato delle diagnosi e dei dati relativi alla propria salute, si ritiene - tenuto conto anche di quanto previsto nell’art. 22, comma 11 del D.Lgs. 101/2018[3] - che nelle more dell’adozione delle predette misure di garanzia, debbano continuare ad essere applicate le *“Altre misure per il rispetto dei diritti degli interessati”* previste

nell’abrogato art. 83, come meglio dettagliate nel provvedimento del Garante del 9 novembre 2005 *“Strutture sanitarie: rispetto della dignità”* ([doc web. 1191411](#)) e le modalità di comunicazione di dati all’interessato previste dall’abrogato art. 84.

Per quanto riguarda il trattamento di dati genetici per finalità di cura si ritiene che nelle more dell’adozione delle misure di garanzia di cui all’art. 2-septies del novellato Codice privacy e tenuto conto di quanto previsto nel già citato comma 11 dell’art. 22 del D.Lgs. 101/2018, questi particolari dati personali debbano essere trattati, come prevede l’abrogato art. 90, nei soli casi e con le modalità e cautele previste nell’Autorizzazione generale del Garante n. 8 ([doc. web. 5803688](#)), senza comunque il preventivo consenso del paziente.

Ciò in considerazione che il riferimento al consenso contenuto nel comma 6 del predetto art. 2-septies deve intendersi, a parere di chi scrive, come un eventuale ulteriore misura di protezione dei diritti dell’interessato e non quale base giuridica di liceità del trattamento dei dati genetici effettuato per finalità di tutela della salute e dell’incolumità fisica dell’interessato, di terzi o della collettività che, come è noto, trova specifica legittimazione nelle condizioni di cui alle lettere h) e i) dell’art. 9 del Regolamento 679/2016 espressamente richiamate all’art. 75 del novellato D.Lgs. 196/03.

Per quanto riguarda l’obbligo di fornire l’informativa agli interessati, si evidenzia, infine, che le modifiche introdotte dal D. Lgs. 101/2018, nel prevedere che i soggetti pubblici e privati che operano in ambito sanitario, compresi i medici di medicina generale e i pediatri di libera scelta, possono avvalersi delle modalità particolari (leggasi semplificate) previste negli artt. da 77 a 80, precisano che la forma e i contenuti della stessa devono essere conformi a quanto previsto dagli artt. 13 e 14 del GDPR.

[1] Rubricato, ora *“Codice in materia di protezione dei dati personali, recante disposizioni per l’adeguamento dell’ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE”*

[2] Su quest’ultimo aspetto si veda l’interessante analisi di Giuseppe D’Acquisto [“Salute e GDPR, l’innovazione che verrà dalle nuove norme”](#)

[3] L’art. 22, comma 11, del D.Lgs. 101/2018 recita *“Le disposizioni del codice in materia di protezione dei dati personali, di cui al decreto legislativo n. 196 del 2003, relative al trattamento di dati genetici, biometrici o relativi alla salute continuano a trovare applicazione, in quanto compatibili con il Regolamento (UE) 2016/679, sino all’adozione delle corrispondenti misure di garanzia di cui all’articolo 2-septies del citato codice, introdotto dall’art. 2, comma 1, lett. e) del presente decreto”*.

Dispositivi wearable e dati sanitari: le 8 privacy design strategies nella pratica

Debora Oliosi - esperta in comunicazione digitale e marketing

Siamo nell'epoca delle app: tonnellate di funzionalità a disposizione dei nostri smartphone che con ogni probabilità non useremo mai. Davvero troppe per una vita sola. Incontro sempre più spesso Clienti che vogliono raccontarmi la loro nuova idea rivoluzionaria di cui il mio telefono non potrà più fare a meno (più spesso di quante volte riesca a fare la spesa!). Un'idea rivoluzionaria che quasi sicuramente da qualche parte è già scaricabile – magari in versione beta – e che nella stragrande maggioranza dei casi manca della riflessione più importante: la reale motivazione che convince l'utente non solo a scaricarla, ma soprattutto a usarla dopo i primi 10 secondi dal download (che è l'unica vera ragione per cui un app dovrebbe essere progettata!).

Tra le più interessanti disponibili oggi sul mercato rientrano sicuramente quelle in grado di interloquire con i dispositivi wearable: orologi, magliette, pantaloni, occhiali, solo per citare i più diffusi. Tutti quei dispositivi, cioè, che indossati inviano dati ad una piattaforma software che, in considerazione delle finalità specifiche, li mette a disposizione di una community pubblica o privata più o meno ristretta.

Si tratta per lo più, in questo caso specifico, di **dati sanitari**: dalla frequenza del battito cardiaco alle calorie consumate, dal livello di stress, all'attività fisica che svolgiamo quotidianamente. Solo per fare qualche esempio. Un dispositivo wearable è composto da diversi elementi hardware e software, non tutti sempre presenti e non tutti accessibili direttamente dai suoi utilizzatori, nello specifico:

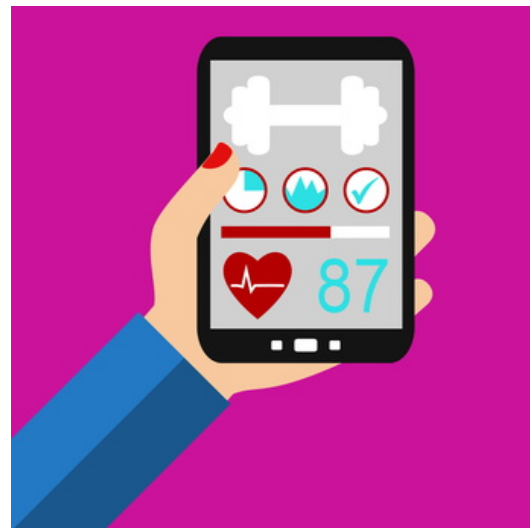
- **Il dispositivo** stesso, l'oggetto da indossare, che ha il compito di raccogliere e trasmettere i dati (tipicamente una app)
- **L'app** installata sullo smartphone
- **Un'area accessibile** via web (o più precisamente interfaccia) per l'accesso e la gestione dei dati raccolti dal dispositivo
- **Il database** che contiene i dati raccolti (che può essere diviso in più elementi separati)
- **L'applicazione lato server** che gestisce i dati e che può essere dotata di più interfacce (tipicamente un accesso via web e/o un software desktop da installarsi sul computer dell'utente)

Lato privacy sono diverse le criticità da considerare: come si sviluppa un'applicazione che gestisce in modo davvero sicuro le categorie di dati particolari elencate all'articolo 9 del GDPR? Come si proteggono informazioni tanto delicate e sensibili? Come si prevencono le violazioni e come si gestiscono nel caso in cui si verificano?

Se i concetti base della Privacy By Design sono chiari, lo sviluppo sistematico di software che li rispettano è a tutt'oggi un obiettivo di complessa realizzazione: non tanto per i costi che genera, quanto perché richiede ai programmatori un cambio della propria forma mentis e del proprio *modus operandi*.

E' per questo che **Enisa ha pubblicato le 8 privacy design strategies** descritte nel suo Privacy and Data Protection by Design – from policy to engineering: **una traccia sintetica, ma estremamente efficace, per trasformare un principio giuridico in tecniche di programmazione concrete e al tempo stesso sufficientemente generiche da lasciare al singolo piena libertà d'azione**. Aspetto indispensabile se si considera l'infinita variabilità tipica del codice sorgente. Una guida indispensabile per lo sviluppo di software che trattano categorie di dati particolari, in grado di supportare i programmatori nell'offrire reali garanzie di protezione dei dati, garantendo una maggiore tranquillità sia nella manutenzione ordinaria che in caso di data breach.

Un vademecum che nella sua semplicità offre gli strumenti per applicare appieno il principio di accountability al software. La guida che ho scelto personalmente di seguire per affiancare i programmatori nei percorsi di adeguamento e di analisi preventiva in materia di protezione dei dati. Otto regole preziosissime che applicate al singolo caso aiutano nell'individuazione delle misure di sicurezza necessarie a garantire al trattamento la compliance al Regolamento.



#1 MINIMIZZA

Dovendo fare una classifica delle parole più usate nel mondo del GDPR, minimizzazione starebbe sicuramente ai primi posti. È uno dei principi fondanti di tutto il Regolamento, una di quelle regole che non puoi ignorare, se non a caro prezzo.

Evita di trattare dati che non ti servono.

Semplice. Togli il necessario, libera spazio, impara a tenere solo quello che ti serve: non conservare all'infinito informazioni che non userai mai. Lalpalissiano, si direbbe. Tanto semplice quanto inapplicato. Tanto semplice quanto di difficile attuazione: raccogliere dati (o tenerli all'infinito) perché non si sa mai è la prassi, evitare di raccogliarli (o liberarsene terminato l'utilizzo) sembra spesso uno scoglio insormontabile. Le parole d'ordine per rispettare questo principio sono due:

1. **Analisi:** per ogni dato che si decide di raccogliere è necessario interrogarsi sulla sua effettiva utilità e sull'eventuale presenza di alternative in sua sostituzione che esulino dal concetto di dato personale
2. **Anonimizzazione:** il giusto compromesso per trasformare dati personali in "dati e basta", mantenendo valide tutte le informazioni statistiche e uscendo di fatto dal recinto del GDPR.

Se anonimizzare i dati personali presenti nel database appare piuttosto scontato, non si può dire altrettanto dei dati presenti sul singolo dispositivo, che se non adeguatamente trattati potrebbero rimanere disponibili anche in caso di smarrimento o cambio di proprietà dello stesso, persino se inutilizzati da tempo.

#2 NASCONDI

La disponibilità di un dato genera potenzialmente un abuso: è per questo che rendere indisponibile un'informazione non effettivamente necessaria ad un soggetto che acceda, mediante una qualsiasi interfaccia disponibile, a una piattaforma che esponga dati personali si rivela una strategia efficace per la protezione della stessa. Se impedire ad un utente di accedere alle proprie informazioni presenti sul proprio smartphone appare evidentemente contraddittorio, è piuttosto sul database e sull'applicazione lato server che dobbiamo concentrarci per applicare questo principio:

1. Sono stati chiaramente definiti i **ruoli degli utenti** che accederanno all'applicazione? Una delle pratiche (incredibilmente) più diffuse è quella di creare un solo ruolo utente: quello dell'amministratore che vede tutto. Si tratta di sicuro della soluzione più economica, ma non può essere considerato uno scenario realmente ipotizzabile se si tiene nella dovuta considerazione la delicatezza dei dati trattati nel caso specifico dei dispositivi wearable.
2. Definiti i ruoli utente, è stato redatto l'**elenco dei campi** a cui ogni ruolo potrà accedere? Per ogni campo c'è una reale motivazione che giustifica l'accesso a quel dato? Nel dubbio, si è scelto di non

visualizzare l'informazione rimandando a valutazioni successive la decisione?

3. È stata considerata la vulnerabilità del database? Sono state individuate adeguate soluzioni di **encryption**? Non si tratta sicuramente di soluzioni economiche, è vero: vero è anche che il GDPR considera esplicitamente i costi di attuazione nelle valutazioni di esclusiva competenza del titolare, permettendogli anche di evitare la spesa. Ma nessuna giustificazione legata ai costi dell'encryption di un database sarà sufficientemente credibile da permetterci di evitare la spesa se alla base dell'applicazione c'è un modello di business con potenzialità milionarie. E poco importa se, al momento dello sviluppo, si tratta solo di potenzialità stimate.
4. I **dati salvati nel dispositivo** sono crittografati? Ci si è chiesti che cosa succederebbe se lo smartphone finisse in mani pericolose?
5. Il collegamento tra app e server utilizzano **canali protetti**? Il sito è disponibile esclusivamente mediante protocollo https? Se si tratta di scelte che andrebbero fatte sempre, nel caso del trattamento dati sanitari l'eventuale assenza di queste precauzioni diventa una svista imperdonabile.
6. La **pseudonimizzazione** è stata applicata, laddove possibile? I collegamenti tra le tabelle sono stati criptati prima di essere salvati nel database, così da rendere complessa (o addirittura impossibile) l'associazione tra il dato personale e il relativo dato sensibile in caso di accesso diretto (in buona o mala fede poco importa)?

#3 SEPARA

Quella della separazione è, nel caso specifico dei dati particolari, una delle tecniche irrinunciabili in materia di protezione: una pratica ad elevatissimo valore aggiunto è senza dubbio quella di utilizzare database diversi, in server diversi e in reti diverse, per distribuire le informazioni. Disegnando la base dati con in mente questo principio significa elevare notevolmente le barriere di accesso alla stessa.

Qualora fosse impraticabile, si considerano indispensabili almeno la pseudonimizzazione dei collegamenti tra tabelle, e/o dei dati personali raccolti.

#4 AGGREGA

Aggregare – dal punto di vista geografico o temporale, per esempio – è **una delle regole meno praticabili quando si parla di applicazione che trattano dati sanitari:** i dati sanitari sono per definizione disaggregati e per questo risulta praticamente impossibile rispettare questa strategia nella fase in cui risulta legittimo trattare il dato.

Una strategia che diventa preziosa, invece, quando si superano i termini di conservazione: l'aggregazione di livello provinciale, per esempio, o addirittura regionale, rende l'anonimizzazione (e quindi la minimizzazione) un processo chiaro e ben definito.

#5 INFORMA

A guardare un po' da lontano, appare piuttosto curioso che la strategia legata all'informazione degli utenti sia presente a pieno titolo tra le 8 privacy design strategies: sembrerebbe scontato che la richiesta avanzata a un utente di condividere i propri dati sia supportata dalle informazioni sul loro utilizzo (modalità di gestione ed eventuale cessione a terzi, livelli di sicurezza, procedure di cancellazione o modifica). **E invece no: di scontato su questo fronte non c'è niente. Fino ad oggi lo sviluppo di applicazioni è sempre stata materia di totale competenza di un committente e del team di programmatori designato. L'utente – nonostante l'evidente indispensabilità del suo ruolo nell'intero processo – non è mai stato coinvolto se non in qualità di motore che permette alla macchina di muoversi.**

Informare significa **dichiarare (e ribadire) chiaramente, ovunque sia ritenuto utile, una sintesi comprensibile degli aspetti che riguardano i dati raccolti**: la loro posizione geografica, le misure di sicurezza cui sono sottoposti, le barriere della loro (in)violabilità, le procedure per accedervi, o eliminarli.

#6 GARANTISCI IL CONTROLLO

Occorre offrire sempre all'utente la possibilità di scegliere, dopo averlo adeguatamente informato, senza lasciare spazio a dubbi di sorta.

Garantire il controllo significa chiedere all'utente, ogni qualvolta sia necessario e senza per questo sconfinare nell'ossessività, **un consenso comprensibile ed esplicito**: completo cioè di tutte le informazioni che gli permettano di effettuare una scelta consapevole e mai forzata, includendo quindi sempre anche le conseguenze in caso di rifiuto.

Garantire il controllo significa infine **criptare i canali di comunicazione** tra i vari nodi dell'applicazione: evitando, cioè, che i dati vengano intercettati mentre sono in viaggio.

#7 APPLICA

Importante è implementare l'applicazione correttamente, con funzionalità specifiche facilmente accessibili, che permettano all'utente la **gestione completa dei propri dati** (e dei relativi diritti): sia che si tratti di informazioni personali, che dei consensi rilasciati. Qualora non prevista, occorre provvedere alla pubblicazione di un **interfaccia web che consenta di accedere/modificare i propri dati e di bloccare** immediatamente l'accesso al dispositivo e/o

all'app in caso di smarrimento o cessione a terzi. Nel caso di dati sanitari diventa fondamentale anche l'implementazione dell'autenticazione a due fattori, che garantisca la certificazione dell'identità dell'utente e un controllo immediato nel caso di eventuali accessi non autorizzati. L'utente deve essere quindi in grado di gestire in totale autonomia le informazioni, in modo da aumentare il valore commerciale e l'autorevolezza del proprio software, ottenendo specularmente il grande vantaggio di una base dati affidabile e aggiornata.

#8 DIMOSTRA

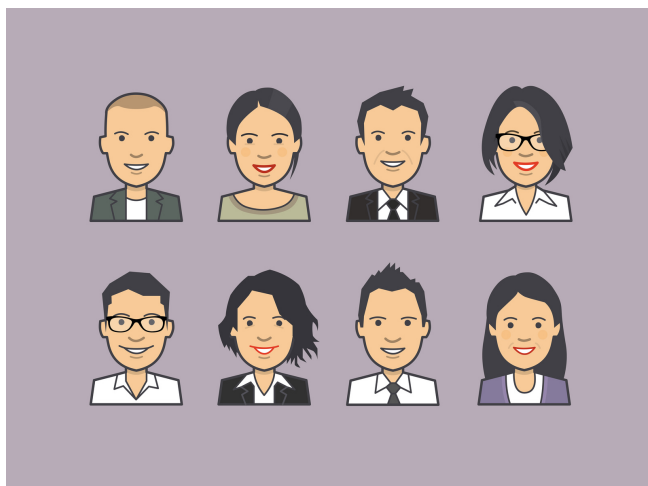
Forse la strategia di più difficile applicazione: il grande tema dei cosiddetti file di log.

Fondamentali in caso di data breach, i file di log sono lo strumento principe per riuscire a dimostrare con affidabilità chi-ha-fatto-cosa e quando. Uno strumento però strettamente legato ai framework e ai database utilizzati, oltre che dipendente dall'indispensabile sensibilità del programmatore. Un tema ancora aperto, che sarà protagonista di non poche discussioni nel futuro più prossimo.

Accreditamento e certificazione nel Regolamento UE 2016/679: un'introduzione

Dorotea Alessandra De Marco - *funzionario Garante Protezione Dati Personali*

Il Regolamento UE 2016/679 (di seguito Regolamento) agli articoli 42 e 43, **prevede e incoraggia l'istituzione di meccanismi per la certificazione della protezione dei dati personali ai fini della corretta applicazione del Regolamento e della dimostrazione della conformità allo stesso dei trattamenti effettuati dai titolari e dai responsabili del trattamento** (cfr. considerando 77, 81 e 100 e articoli 24 (3), 25(3), 28(5), 32(3), 35(8), 46(2) e 83(2)). **La certificazione rappresenta uno strumento utile per il titolare e il responsabile del trattamento per dimostrare il rispetto degli obblighi, le garanzie sufficienti, la conformità a requisiti di protezione dei dati.**



In soggetti usualmente coinvolti in un sistema di accreditamento e certificazione sono:

- l'azienda/ente che richiede la certificazione;
- l'organismo di certificazione o certificatore, accreditato, che rilascia i certificati sulla base dei risultati delle verifiche condotte da valutatori accreditati (laboratori di verifica o ispettori) e vigila sulla corretta gestione dei certificati;
- l'ente di accreditamento che accredita i certificatori e/o i valutatori (laboratori di verifica o ispettori) e controlla periodicamente il mantenimento dei requisiti previsti da parte di tali soggetti.

L'art. 43[1] del Regolamento, richiede che il certificatore debba essere accreditato dall'autorità di controllo competente o dall'organismo nazionale di accreditamento designato in virtù del regolamento (CE) n. 765/2008 o da entrambi. Il regolamento (CE) n. 765/2008 prevede che ciascun stato membro abbia uno e un

solo ente di accreditamento e definisce l'accREDITAMENTO come "l'attestazione ... che certifica che un determinato organismo di valutazione della conformità soddisfa i criteri stabiliti da norme armonizzate e, ove appropriato, ogni altro requisito supplementare, compresi quelli definiti nei rilevanti programmi settoriali, per svolgere una specifica attività di valutazione della conformità".

L'accREDITAMENTO assicura, quindi, che l'organismo di certificazione soddisfa i criteri e i requisiti stabiliti e abbia le competenze necessarie per svolgere i suoi compiti.

Il quadro legislativo vigente[2] prevede che il ruolo di ente di accREDITAMENTO sia svolto dall'organismo nazionale di accREDITAMENTO[3], fatto salvo il potere del Garante di assumere direttamente l'esercizio di tali funzioni con riferimento a una o più categorie di trattamenti.

L'accREDITAMENTO è sempre legato a uno schema di certificazione[4], ovvero, per rilasciare certificazioni, ogni organismo di certificazione deve accREDITARSI per il relativo schema secondo specifici requisiti. Tali schemi di certificazione possono essere redatti da un organismo di certificazione, da un ente pubblico (a esempio, nel caso del Regolamento, l'autorità di controllo) o un attore privato. L'accREDITAMENTO, inoltre, è rilasciato per lo schema di certificazione secondo i requisiti indicati nelle seguenti norme tecniche internazionali che differiscono per l'oggetto della certificazione:

- ISO 17065 - Conformity assessment — Requirements for bodies certifying products, processes and services: utilizzata per l'accREDITAMENTO di organismi di certificazione che si occuperanno di certificare prodotti, processi e servizi;
- ISO 17021 - Conformity assessment — Requirements for bodies providing audit and certification of management systems: utilizzata per l'accREDITAMENTO di organismi di certificazione che si occuperanno di certificare di sistemi di gestione[5];
- ISO 17024 - Conformity assessment -- General requirements for bodies operating certification of persons: utilizzata per l'accREDITAMENTO di organismi di certificazione che si occuperanno di certificare abilità, competenze e conoscenze di persone.

Nel caso del Regolamento l'articolo 43 richiama espressamente la norma EN ISO/IEC 17065/2012, ovvero certificazione di prodotti, processi e servizi, nonché i requisiti aggiuntivi stabiliti dall'autorità di

controllo competente. I requisiti della EN ISO/IEC 17065/2012 coprono numerosi aspetti e sono raggruppati in cinque macro classi: requisiti generali (es. legali e contrattuali, imparzialità, sostenibilità finanziaria, non discriminazione, confidenzialità, trasparenza) **strutturali** (es. organizzazione, procedure per assicurare imparzialità) **sulle risorse** (gestione del personale e delle relative competenze) **sui processi** (rilascio, gestione e revoca della certificazione e gestione dei reclami) e **sui sistemi di gestione dell'organismo di certificazione.**

Tali requisiti comprendono in larga parte quanto previsto dall'articolo 43(1) del regolamento in particolare circa l'indipendenza, la competenza e l'assenza di conflitto di interessi dell'organismo di certificazione, il rispetto dei criteri di certificazione (ovvero lo schema di certificazione), le procedure per il rilascio, il riesame periodico e il ritiro delle certificazioni, dei sigilli e dei marchi di protezione dei dati, le procedure e strutture atte a gestire i reclami relativi a violazioni della certificazione. **Per quanto riguarda i requisiti aggiuntivi per l'accreditamento, ai sensi dell'art. 43, paragrafo 1, lettera b) del Regolamento, il comitato europeo per la protezione dei dati (EDPB) sta perfezionando un documento di linee guida "Guidelines to identify common criteria to accredit certification bodies under Regulation 2016/679", già sottoposto a inchiesta pubblica da gennaio a marzo 2018.**

Poiché la definizione di questi requisiti è comunque strettamente legata all'individuazione dell'oggetto della certificazione che, secondo l'articolo 42(5) deve essere rilasciata in base ai criteri approvati dall'autorità di controllo competente, il comitato europeo per la protezione dei dati (EDPB) sta perfezionando un documento di linee guida "Guidelines to identify common criteria to certify processing under Regulation 2016/679", già sottoposto a inchiesta pubblica dal 30 maggio al 12 luglio 2018.

[1] D.Lgs. 10 agosto 2018, n. 101.

[2] Per l'Italia è [Accredia](#).

[3] Documento che contiene le regole, le procedure e le modalità di gestione per ottenere la certificazione per uno specifico prodotto, processo, servizio.

[4] Un Sistema di Gestione è un insieme di procedure che un'organizzazione deve seguire per raggiungere i suoi obiettivi.

Gli “zombie digitali”: l’eredità dei dati personali nella società digitale

Davide Maniscalco - avvocato, Professionista della Digitalizzazione documentale e della Privacy di ANORC Professioni e Professionista D&L NET

La progressiva evoluzione della società dell’informazione, legata alle sempre maggiori connessioni eterogenee di dispositivi, ha creato **l’esigenza di una tutela dell’identità digitale di ciascun individuo nel corso della vita e, soprattutto, nel momento della sua cessazione.**

È indispensabile affrontare il tema del “trapasso”, ossia della sorte giuridica dei dati digitali, la cui titolarità apparteneva al caro estinto, interrogandosi, tra l’altro, sulla riconducibilità ad altri soggetti della legittimazione all’esercizio dei relativi diritti, in quanto portatori di interessi parimenti meritevoli di tutela giuridica. Il tema è stato sin da subito avvertito come particolarmente sensibile da parte del legislatore nazionale, alla luce dei numerosi casi di individui che lasciano sopravvivere la loro “persona digitale”, creando nel tempo i cosiddetti “zombie digitali”.

Ed è proprio questo il punto.

La morte del soggetto esaurisce il suo ciclo di vita materiale, ma non quello digitale, che continua invece a sopravvivere nella rete. In tempi non sospetti, già il Prof. Stefano Rodotà aveva evidenziato come la diffusione di informazioni personali può avere dei risvolti nell’ambito dei diritti fondamentali e che occorre affermare una forma di “tutela del corpo elettronico” delle persone che diffondono i loro dati online.

Ci si riferisce, ad esempio, alla **sopravvivenza dell’account di posta elettronica del defunto e della sua sorte giuridica**, ovvero di quella dei dati presenti in un cloud o, ancora, alla sorte successoria delle criptovalute acquistate a suo tempo.

Al riguardo, l’art. 9, comma 3 del D.Lgs. 196/2003, nel testo previgente al D.lgs. 101/2018 prevedeva che *i diritti di cui all’art. 7, riferiti a dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell’interessato o per ragioni familiari meritevoli di protezioni.*

La norma introduce un’importante facoltà, espressamente attribuita ai soggetti portatori di un interesse proprio ovvero ad altri che agiscono o si propongono di agire nell’interesse del defunto o per la tutela del suo nucleo familiare. La facoltà giuridica appena esaminata riveste particolare importanza anche nel campo dei rapporti telematici in cui si sostanzia l’identità digitale dell’individuo.

L’accesso ai dati digitali ed alle informazioni del *de cuius* rappresentava, prima della novella introdotta dal D.lgs 101/2018, una insidia giuridica e successoria non banale, soprattutto in considerazione della eterogeneità dei “beni” del patrimonio digitale sedimentato fino al momento del trapasso (ad esempio banche dati, immagini, musica).

Il dibattito in dottrina si è concentrato, in particolare, sulla sorte dei dati esistenti su dispositivi di archiviazione di massa (*universal serial bus* e *hard disk* esterni), nonché sulla **legittimità dei diritti di rivendicazione della proprietà intellettuale o industriale ricollegabili alle opere dell’ingegno o alle invenzioni industriali eventualmente presenti** (si pensi ad un testo inedito oppure ad un modello di utilità non ancora assoggettato a brevetto, o, ancora ad un marchio non registrato).
Emergeva, inoltre, una ulteriore problematica legata alla **successione nei rapporti contrattuali dell’era digitale** (si pensi al profilo social ovvero ai contratti di hosting, salva la espressa previsione di intrasmissibilità a terzi per il caso di morte).



La sorte dell’account di posta elettronica ha dato luogo, nel tempo, ad un contratto dottrinale che ha visto avvicinarsi la tesi sulla trasmissibilità successoria dei soli diritti collegabili all’account professionale e non anche personale del defunto, a quella della successione *tout court* dei coeredi nell’account del *de cuius*, fino alla tesi -più radicale - che, addirittura, escludeva categoricamente la successione nell’account per il timore di una violazione postuma della personalità.

Le questioni sinora evidenziate trovano finalmente una propria specifica disciplina nello schema di decreto legislativo di adeguamento al quadro normativo nazionale alle disposizioni del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE.

Tra le varie novità poi introdotte dal Decreto Legislativo n.101 del 10 agosto 2018, in vigore dal 19

settembre 2018, il nostro legislatore ha introdotto la disciplina del trattamento dei dati di persone decedute per il tempo successivo alla loro morte, escluso dall'applicazione del Regolamento e demandato alla normazione da parte degli Stati membri.

Già nella relazione allo schema di decreto, al fine di non introdurre disposizioni in contrasto con il diritto nazionale in materia successoria, si prevedeva che i diritti di cui agli artt. da 15 a 22 del Regolamento, concernenti persone decedute, potessero essere esercitati da chi manifesti un interesse proprio o da chi agisca a tutela dell'interessato in qualità di suo mandatario o per ragioni familiari meritevoli di protezione[1]. Vale la pena di evidenziare a tal proposito che, come già chiarito il Garante della Privacy, il riconoscimento e l'esercizio dei suddetti diritti prescinde dalla configurazione in capo all'interessato della nozione tecnica di erede [2].

Nell'esercizio dei diritti ex art. 2-terdecies del D.lgs 101/2018 appare evidente che **il diritto alla riservatezza del *de cuius*** cede il passo ai diritti esercitati da chiunque sia portatore di un interesse meritevole di tutela giuridica. Un'altra significativa riflessione interessa anche l'ambito di applicazione materiale della norma e, in particolare, riguarda quei dati che possono essere considerati riferibili al *de cuius* e, pertanto, costituire oggetto dei diritti esercitabili ex art. 2-terdecies del D.lgs 101/2018.

A tal proposito, dal tenore letterale della norma, il diritto di accesso e, più in generale, quelli previsti dagli artt. 15-22 del Regolamento europeo, avrebbero ad oggetto i dati personali direttamente afferenti alla persona richiedente che ostenta un interesse meritevole di tutela ad accedervi. Conseguentemente l'esercizio del diritto non si estenderebbe ai dati personali non espressamente riferibili al defunto, ma che identificano soggetti terzi, estranei al rapporto successorio o, in ogni caso, all'interesse dedotto a fondamento legittimante del diritto esercitato.

La questione si rivela di particolare importanza con riguardo ai profili "social" delle persone decedute.

In tali casi, infatti, l'esercizio dei diritti da parte di chiunque palesi un interesse proprio o a tutela del defunto, potrebbe condurre ad un'interferenza con dati personali riferibili a terzi estranei al rapporto successorio "digitale", di cui magari la visibilità era stata esclusa nel corso della vita.

Di recente, alcuni social, proprio al fine di prevenire interferenze con dati di terzi, consentono al richiedente legittimato di gestire un account esclusivamente commemorativo del defunto, proponendo contestualmente l'alternativa eliminazione nel caso di

decesso ovvero di disattivazione per il caso di protratta inattività per oltre dodici mesi o di ripetuti ed infruttuosi tentativi di contatto con l'originario interessato.

Vi è poi la questione relativa all'accezione giuridica da attribuirsi alle disposizioni di cui ai co. 2 e 3 dell'art. 2-terdecies del D.lgs 101/2018.

A tal proposito, con riguardo all'offerta diretta di servizi della società dell'informazione, la norma consente all'interessato di vietare l'esercizio dei diritti previsti dagli artt. 15-22 del Regolamento europeo, con dichiarazione scritta presentata al titolare del trattamento o a quest'ultimo comunicata. Il comma 3 prosegue chiarendo che la suddetta volontà dell'interessato deve risultare in modo non equivoco e deve essere specifica, libera e informata (si precisa altresì che il divieto può riguardare anche soltanto l'esercizio di alcuni dei diritti di cui al predetto co. 1). Vale la pena di evidenziare che la norma presenta una formulazione tecnicamente infelice atteso che il divieto andrebbe piuttosto configurato come una "rinunzia" ad un diritto.

In conclusione, il nodo centrale della questione, dalla nuova prospettiva legislativa, si traduce in un'importante presa di coscienza della radicale trasformazione digitale della società e della corretta ed adeguata disciplina dei dati che sopravvivono alla morte della persona non solo "fisica", ma anche "digitale".

[1] La art. 2-terdecies del D.lgs 101/2018, recante "Diritti riguardanti le persone decedute" prevede testualmente che: I diritti di cui agli articoli da 15 a 22 del Regolamento riferiti ai dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato, in qualità di suo mandatario, o per ragioni familiari meritevoli di protezione; l'esercizio dei diritti di cui al comma 1 non è ammesso nei casi previsti dalla legge o quando, limitatamente all'offerta diretta di servizi della società dell'informazione, l'interessato lo ha espressamente vietato con dichiarazione scritta presentata al titolare del trattamento o a quest'ultimo comunicata; la volontà dell'interessato di vietare l'esercizio dei diritti di cui al comma 1 deve risultare in modo non equivoco e deve essere specifica, libera e informata; il divieto può riguardare l'esercizio soltanto di alcuni dei diritti di cui al predetto comma; l'interessato ha in ogni momento il diritto di revocare o modificare il divieto di cui ai commi 2 e 3; in ogni caso, il divieto non può produrre effetti pregiudizievoli per l'esercizio da parte dei terzi dei diritti patrimoniali che derivano dalla morte dell'interessato nonché del diritto di difendere in giudizio i propri interessi.

La norma, a seguito dell'abrogazione degli artt. 7 e 9 del Codice della Privacy, sancisce espressamente che i diritti di accesso ai propri dati spettanti a ciascun interessato e, in generale, tutti i diritti (anche nuovi) previsti dal Regolamento europeo, possono essere esercitati anche nell'interesse delle persone decedute.

Più precisamente, il decreto di adeguamento prevede espressamente che tutti i suddetti diritti possano essere esercitati, sia dagli eredi del defunto interessato, sia da chiunque abbia un interesse proprio, o agisca a tutela dell'interessato o per ragioni familiari meritevoli di protezione.

[2] cfr. Garante per la protezione dei dati personali, provv. n. 268 del 3 maggio 2018

L'impatto del GDPR nella Chiesa cattolica

Antonella D'Iorio - avvocato - esperto nella protezione dei dati personali, Professionista D&L NET

Il Regolamento europeo n. 679/2016 (GDPR) in materia di "trattamento dei dati personali" ha prodotto, inevitabilmente, i suoi effetti anche nei confronti delle chiese e associazioni religiose chiamate di recente ad adeguare le vecchie disposizioni e a modellarle secondo la nuova disciplina.

Senza voler focalizzare in questo articolo la nostra attenzione sulle chiese secondarie e/o su quelle realtà che hanno un'estensione e diffusione minore sul territorio nazionale – fenomeni che senza dubbio meriterebbero indagini accurate – è interessante dedicare alcuni spunti di riflessione alla confessione religiosa per eccellenza, portatrice di una dignità piena, sia sotto il profilo culturale e di valore, sia sotto il profilo di rappresentante della professione di fede, meglio conosciuta e riconosciuta nel mondo: la Chiesa cattolica.



In premessa, tenendo presente l'indipendenza e l'autonomia di cui gode l'ordinamento giuridico della Chiesa, anche nella sua sovranità di stato estero, che implica la non ingerenza delle autorità dello Stato nelle attività e nelle organizzazioni interne anche per le operazioni di trattamento dei dati nonché nel riconoscimento delle finalità che si attribuiscono alla sua natura istituzionale perseguita con fini pubblicistici, non appare possibile esonerare una realtà tanto complessa, dall'esigenza di essere inevitabilmente aggiornata alle leggi in vigore.

L'opportunità di predisporre una normativa che regolamentasse l'acquisizione, la conservazione e l'utilizzazione dei dati personali nel diritto particolare della Chiesa cattolica è stata in precedenza già avvertita e voluta dal Consiglio Episcopale Permanente nel 1998.

Oggi, l'art. 91 del GDPR, riguardo al trattamento sulla tutela delle persone fisiche, di fatto, fa riferimento alla applicabilità delle norme già esistenti a condizione, però, che queste stesse norme siano aggiornate e rese conformi al richiamato regolamento.

Per la Chiesa che è in Italia, il corpus normativo a cui risalire è il "Decreto Generale" (decreto n. 1285/99 promulgato dal Presidente della Conferenza Episcopale Italiana (CEI) in persona del Card. Camillo Ruini) che detta le "Disposizioni per la tutela del diritto alla buona fama e alla riservatezza" circa i dati relativi alle persone dei fedeli, degli enti ecclesiastici e delle aggregazioni laicali. Il Decreto Generale, già espressione di una regolamentazione più articolata rispetto ai principi contenuti nel Codice di diritto canonico italiano e del Codice dei canoni delle Chiese orientali, ha meritato nei mesi scorsi l'esame da parte della Santa Sede, in nome di un giusto e opportuno adeguamento alle novità legislative in materia, a cui è seguita l'approvazione ufficiale avvenuta nella 71a Assemblea Generale della CEI, tenutasi a Roma dal 21 al 24 maggio 2018, con la piena operatività per le diocesi a far data dal 25 maggio 2018.

Non è lecito ad alcuno ledere illegittimamente la buona fama di cui uno gode, o violare il diritto di ogni persona a difendere la propria intimità: secondo tali principi ispiratori, il Decreto Generale in vigore dal 1999 cuce precise disposizioni destinate all'ambiente ecclesiastico per l'acquisizione, conservazione e utilizzazione dei dati personali dedicando appositi articoli della normativa alla buona pratica delle attività che rappresentano principi tuttora validi, ma, come anticipato, rivisitati e integrati secondo le disposizioni del GDPR e ai sensi dell'art. 17 n. 1 del Trattato sul funzionamento dell'Unione europea (TFUE).

La natura stessa dei dati trattati, oltre a ricadere negli aspetti riferibili alle libertà di tipo religioso-confessionale, presenta sempre più implicazioni di tipo giuridico, politico, economico anche nelle relazioni di aspirazione laica, di pluralismo moderno della nostra società.

E non si può non tener conto degli aspetti menzionati.

Le previsioni precedenti – che già riferivano sul trattamento circa finalità, registri, archivi, elenchi e schedari, elaborazione e conservazione dei dati, segreto d'ufficio, annuari e bollettini con invito alla vigilanza da parte del Vescovo sulla corretta applicazione – si sono perciò meglio arricchite a garanzia di una adeguata protezione dei dati trattati al di là dei processi automatizzati o meno. La necessità di nominare un "titolare del trattamento", l'opportunità di ravvisare un "responsabile del trattamento"

o, in alcuni casi, come in ipotesi di attività di trattamento su larga scala, il bisogno di nominare un “responsabile della protezione dei dati” rappresentano un passaggio fondamentale e importante che testimonia nuova e crescente sensibilità da un punto di vista sostanziale e non solo formale.

Parimenti, e a maggiore conferma di quanto innanzi, si riscontra l’evidente necessità per la tenuta di appositi “registri delle attività di trattamento” e la necessità tutta nuova ad acquisire il “consenso informato” dei soggetti interessati che risulti espresso e inequivocabile e preceduto da adeguata “informativa.”

Da una prima visione, condotta per finalità di studio e ricerca, dei documenti ufficiali reperibili presso diverse sedi e strutture della Chiesa cattolica italiana per le attività di trattamento dei dati, pur dovendo ritenere perfettibili gli atti che sono oggi a disposizione, si ricava, comunque, che il tema della protezione dei dati si specchia e riflette nel presente dell’identità della Chiesa cristiana internazionale e universale. Occorre inoltre considerare l’indiscutibile valore di scrigno storico e antropologico dei popoli che le è proprio, in quanto erede del più ricco patrimonio culturale dell’umanità, sempre più consapevolmente aperta e proiettata alla società dell’informazione negli anni recenti e pronta a scambiare e creare relazioni tra singoli ed enti, siano essi appartenenti alla stessa confessione o a confessioni diverse, favorendo una circolazione di dati in crescente quantità e velocità.

Alla luce di queste considerazioni, possiamo ritenere di fatto irrinunciabili i bisogni attualmente avvertiti e recepiti sulla protezione dei dati personali, all’interno e oltre la vita sacramentale con unioni inscindibili tra organizzazioni spirituali e laiche e con la costruzione di opere sempre più radicate nel sociale. L’auspicio è che tali bisogni possano sempre meglio radicarsi e affinarsi affinché gli attori preposti al trattamento rispondano con criteri di massima adeguatezza per i casi specifici di cui andranno ad occuparsi.

Vista la particolarità del trattamento in questione, potrebbe tornare utile approfondire i futuri effetti e sviluppi scaturenti dalle disposizioni in vigore con un taglio reale e pratico dell’impatto del GDPR sulla Chiesa cattolica da riscontrare direttamente presso la Segreteria Generale della CEI.