IusTrend
il verso del diritto

PRIVACY

-> LINEE DI TENDENZA <-

MAGGIO 2018

LaScala
SOCIETÀ TRA AVVOCATI

www.lascalaw.com - www.iusletter.com

Milano | Roma | Torino | Bologna | Firenze | Venezia | Vicenza | Padova | Ancona

COME È CAMBIATA LA PRIVACY E COME LA PRIVACY CI CAMBIERÀ

1. INTRODUZIONE

È scaduto il termine di adeguamento alle disposizioni del Regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (GDPR). Le novità introdotte sono molte e non sempre facili da applicare, non solo perché la materia in sé è ostica e pervasiva, ma anche perché ancora non abbiamo un testo normativo nazionale che provveda ad adeguare il nostro ordinamento alla legge europea[1].

Pur in attesa di tali chiarimenti "autentici", in rete si contano innumerevoli contributi che spiegano quali sono le novità introdotte dal legislatore europeo e quali sono gli adempimenti, formali e sostanziali, che devono (dovevano) essere eseguiti entro il 25 maggio.

Completamente assenti, invece, sono articoli che inquadrano la nuova disciplina nei processi aziendali e sociali, che cioè colgono l'aspetto dinamico del fenomeno. Come cambierà la gestione della *privacy*? E soprattutto, qual è il mutamento culturale a cui stiamo assistendo? Possiamo considerare il Regolamento solo come un adempimento imposto da qualche burocrate di Bruxelles o si tratta di un processo evolutivo "naturale" frutto di una spinta iniziata anni fa verso una società più libera ed eguale?

2. LA *PRIVACY* E LA PROTEZIONE DEI DATI PERSONALI

Per comprendere dove ci porterà la *privacy* è necessario sapere da dove proviene.

In proposito, occorre innanzi tutto chiarire che *privacy* e protezione dei dati personali non sono la stessa cosa, ma due facce della stessa medaglia[2]. Il taglio pratico del presente lavoro, non consente di entrare in sottili distinzioni concettuali, ma sarebbe un errore non soffermarci un momento su un aspetto fondamentale che informa tutta la materia.

La *privacy* (la riservatezza) risponde ad

un bisogno primario dell'essere umano, ovvero quello di nascondere dalla conoscenza altrui la propria sfera intima e privata, personale o familiare che sia. Si tratta probabilmente di un sottoprodotto dell'io, il riflesso di un istinto primordiale di protezione e affermazione del sé.

Qualcosa quindi che nasce con la coscienza, con il libero arbitrio, con la vergogna, con il passaggio dallo stato animale all'essere senziente.

In tempi più moderni, lo sviluppo tecnologico ha reso il dato personale uno strumento di controllo ancora più sottile. Il condizionamento delle masse ha assunto caratteri orwelliani.

Il diritto alla protezione dei dati, ha invece un carattere più culturale che naturale. Nasce in primo luogo dal riconoscimento che il controllo sui dati personali può essere un temibile strumento di oppressione e condizionamento della popolazione.

Non a caso il dibattito sulla necessità di proteggere i dati personali inizia nel secondo dopoguerra. In Europa la riduzione degli individui a classi omogenee (oppositori politici, ebrei, omosessuali, zingari, portatori di *handicap*, ecc.) aveva scatenato un'irrazionale corsa alla segregazione sociale e alla progressiva negazione di diritti fondamentali. La forza banalizzante e persuasiva delle teorie razziali si basava su un'estrema semplificazione della realtà che, sebbene sacrificasse la verità a beneficio dell'opportunismo politico, aveva il pregio di essere compresa da tutti e poteva facilmente essere utilizzata per amplificare la rabbia e il disagio sociale cresciuti dopo la crisi economica della Grande Depressione iniziata nel 1929.

In tempi più moderni, lo sviluppo tecnologico ha reso il dato personale uno strumento di controllo ancora più sottile. Il condizionamento delle masse ha assunto caratteri orwelliani. Colossi del *web*, per lo più nord americani, hanno il potere di orientare le scelte politiche e di consumo di milioni di cittadini[3]. L'altro aspetto di questo enorme potere, è il valore economico dei dati personali. WhatsApp, la famosa piattaforma di messaggistica istantanea, ha 55 dipendenti ed è stata venduta a Facebook nel 2014, cioè dopo appena cinque anni dalla sua nascita, per oltre 19 miliardi di dollari. Tutto il valore dell'azienda è il numero di utenti e quindi la mole di dati di cui ha il controllo. Dati personali da cui con sistemi di analisi di BigData possono essere in futuro estratte un'infinità di informazioni molto più preziose dell'oro[4].

Privacy e protezione dei dati, sono quindi imbricate l'una nell'altra (e per questo si parla indifferentemente di "*privacy*" per indicare entrambe). Due prospettive del medesimo fenomeno: la prima è il diritto di non far sapere agli altri informazioni che ci riguardano, la seconda è il diritto di avere il controllo su tali informazioni.

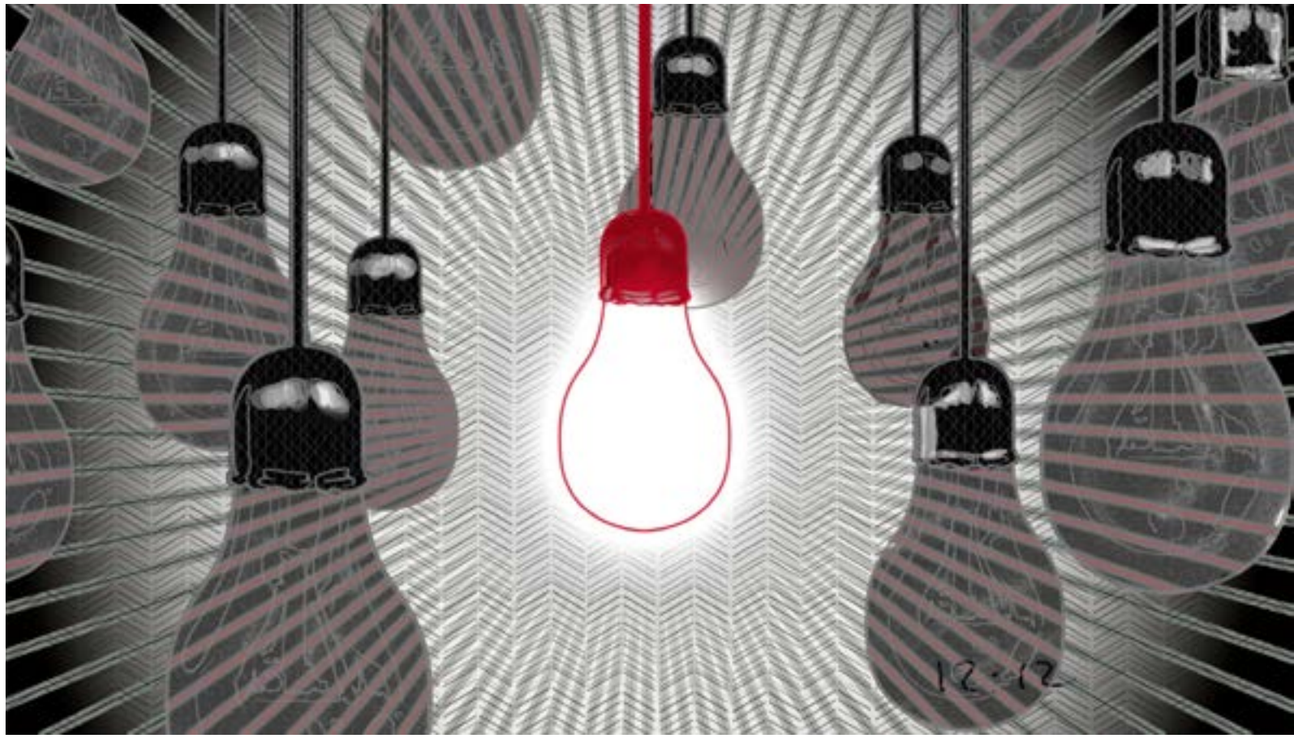
3. LA LEGGE DEL TUTTO

Un altro aspetto fondamentale da tenere in considerazione per rispettare il GDPR è la trasversalità che la sua disciplina sta assumendo. La matrice fondamentale del diritto alla *privacy*, finisce per incidere in maniera orizzontale su pressoché tutte le situazioni della vita. Ogni istituto di diritto è in qualche misura interessato dall'applicazione del Regolamento e ogni funzione aziendale ha in qualche modo a che fare con le sue prescrizioni. Ciò spiega anche la previsione del Responsabile Protezione Dati – RPD (su cui torneremo più in là) quale nuova risorsa dedicata alla verifica e controllo delle disposizioni del GDPR.

L'acquisto di un biglietto del treno, la creazione di un profilo *social*, la pubblicazione di una foto, la prenotazione di un ristorante sono solo alcune delle normali interazioni sociali che sollevano problemi di *privacy*. Anche nei rapporti professionali e commerciali la *privacy* sta diventando un *passepartout* per la tutela di una serie indefinita di situazioni soggettive[5]. Molte cause di lavoro portano con sé pretese in ordine al corretto trattamento dei dati del lavoratore e quelle civili si arricchiscono appena possono di una autonoma domanda sulla *privacy*, connessa alla principale. In tutti i casi l'azione mira, spesso con successo, a far lievitare le richieste risarcitorie.

Sul piano extragiudiziario, il discorso non è diverso. Una transazione commerciale o una *partnership* che non prendano in considerazione i dati scaturenti dallo svolgimento del rapporto contrattuale rischiano di portare alla conclusione di accordi zoppicanti. Non solo il difetto di tutela del dato in sé potrebbe esporre le parti a rischi non calcolati, ma i loro rispettivi interessi potrebbero essere falsati se il valore di una banca dati non fosse correttamente espresso e i diritti su di essa non fossero finemente regolati.

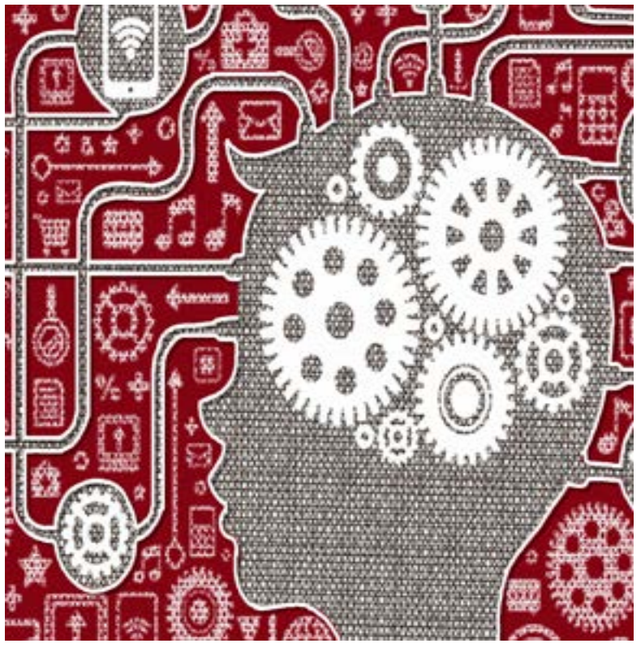
A tutto questo si aggiunga il fatto che la nozione di dato personale – e quindi l'applicazione del GDPR – è così estesa da comprendere pressoché qualsiasi informazione. Dati non sono infatti solo quelli che direttamente identificano una persona (nome e cognome, per



esempio), ma anche quelli che in associazione con altri, possono consentire in astratto l'identificazione di una persona o, pur senza l'identificazione, consentono la conoscenza di informazioni che la riguardano[6].
Non è quindi esagerato definire la privacy – come fa qualcuno – la legge del tutto.

4. I DUE LIVELLI DELLA *PRIVACY*

Alla luce della pervasività della *privacy* e la varietà delle situazioni su cui incide, l'adeguamento al GDPR non può essere limitato ad un intervento *una tantum* o all'adozione di misure correttive di trattamenti illegittimi già intervenuti, ma deve essere svolto in modo continuativo, individuando funzioni e procedure che permettano l'allocazione ottimale di risorse e responsabilità in modo da garantire la massima protezione dei dati personali senza ostacolare il titolare nel perseguimento dell'obiettivo d'impresa.
In tale prospettiva, nel prossimo futuro i titolari del trattamento dovranno affrontare i rischi connessi al trattamento dei dati operando sia sul piano giuridico che su quello dei processi di gestione.
Quest'ultimo aspetto è fondamentale per evitare che l'impianto *privacy* di una azienda diventi obsoleto, inefficace o inefficiente esponendo il titolare alle salatissime sanzioni previste dal Regolamento.
Se da un lato l'analisi legale è un momento imprescindibile per identificare il tipo di trattamento e la sua legittimità, l'implementazione di un processo continuativo di verifica e controllo è altrettanto importante per presidiare i flussi di dati e allocare in modo ottimale risorse e responsabilità.
Ad esempio, l'utilizzo dei dati personali dei dipendenti per fornire loro servizi di *welfare* aziendale solleva senz'altro dubbi di legittimità che devono essere risolti prima del trattamento. Ma risolti questi, l'intervento non può finire qui. È necessario altresì apprestare fin da subito un processo che coinvolga diverse funzioni (HR, IT, Amministrazione) per evitare che il rilascio di un nuovo servizio di assistenza o sostegno, ovvero la scelta di una soluzione *cloud*, diventino circostanze che delegittimano in modo grave l'adozione di una misura lodevole e senz'altro gradita ai dipendenti.
Dal diritto al processo quindi. Ma anche in senso inverso, dal processo di nuovo al diritto, per verificare che il requisito dell'*accountability* sia rispettato.



5. *ACCOUNTABILITY*: *LEGAL* O *COMPLIANCE*?

Una delle novità introdotte dal GDPR è il principio dell'*accountability*, tradotto nella versione italiana del Regolamento con il termine responsabilizzazione, anche se il significato è più simile a rendicontazione. Si tratta in sintesi di una manifestazione documentale (produzione, conservazione, aggiornamento ed esibizione) che attesta l'adozione di un comportamento "responsabile" da parte del titolare volto alla massima protezione dei dati personali da esso trattati.
Tradotto in termini pratici, *accountability* vuol dire progettare i trattamenti di dati personali in modo competente e trasparente, mitigando i rischi per i soggetti interessati e limitando il trattamento allo stretto necessario per il perseguimento di scopi legittimi.
Non più quindi caselle precostituite entro cui collocare i trattamenti per decidere se siano consentiti o meno. Non più intervento preventivo dell'autorità che decide se si può o meno procedere con la raccolta dati. Piena libertà invece del titolare di verificare se il trattamento che si propone di fare sia legittimo e se necessiti di particolari misure di sicurezza.
Ogni flusso dati, quindi, dovrà essere analizzato con la lente del giurista alla luce di principi di diritto con l'aiuto della vastissima casistica esistente. Il risultato dell'analisi dovrà poi essere oggetto di rendicontazione e inserito in modo stabile in definiti processi aziendali che consentano il monitoraggio e l'eventuale aggiornamento delle misure adottate.
Vien quindi da chiedersi quale sia la funzione a maggiore vocazione di essere investita di attività così eterogenee. A regime vedremo probabilmente diverse configurazioni a seconda della struttura e dimensione dei titolari.
Oggi va per la maggiore l'affidamento della questione *privacy* alla funzione legale. Questa scelta dipende in gran parte dalla diffusa percezione che la *privacy* abbia una dimensione meramente giuridica, fatta di meccanica adesione a norme prescrittive di stampo formalista del vecchio D.Lgs. 196/2003 (il c.d. Codice *Privacy*). Il principio di *accountability*, tuttavia, ribalta tale prospettiva e sarebbe il caso di considerare l'affidamento della *privacy* alla funzione *compliance* più avvezza a gestire processi e coordinare uffici e ruoli in modo efficiente.
La *privacy* ha oggi molto a che fare con analisi di rischio e svolgimento di attività di *audit* interno. Peraltro, la trasversalità e l'aspetto dinamico della *privacy,* accennati al precedente paragrafo, rende essenziale il coordinamento di molte funzioni, ciascuna coinvolta per una parte nella definizione dei processi e dei controlli. I processi stessi già in essere in azienda potrebbero essere fattorizzati, cioè imbricati l'un l'altro; e ciò potrebbe farlo solo chi ha una visione d'insieme di vari aspetti regolamentari.
Si pensi alla misura di sicurezza in ambito *privacy* che prevede il periodico controllo degli estintori nelle sale CED per prevenire il pericolo di distruzione o perdita di controllo di dati personali. Tale misura, si sovrappone anche alla corrispondente procedura per la sicurezza sul luogo di lavoro e alle generali misure antincendio a tutela del patrimonio. Tutti questi protocolli di verifica e controllo potrebbero essere assorbiti in un'unica procedura *compliant* con tutte le normative e regolamenti di settore.

In tale scenario, la funzione legale fornisce solo una tessera del *puzzle* – sia forse anche la più importante –, ma le altre tessere saranno fornite da altri reparti: dalle Risorse Umane, dall'IT e dal Responsabile del Servizio Prevenzione e Protezione. È quindi a nostro avviso più naturale che il ruolo di direttore di orchestra di queste diverse competenze sia assunto dalla *compliance*, ovvero da chi conosce le dinamiche di *audit* ed è già abituato a disegnare e monitorare procedure e a relazionarsi con le varie funzioni aziendali.

6. RDP INTERNO OD ESTERNO?

Come noto, il Regolamento impone che per taluni tipi di trattamenti il titolare designi un Responsabile della Protezione dei Dati (RPD), ovvero un soggetto che provveda a fornire consulenza in merito agli obblighi derivanti dal Regolamento e a sorvegliare l'osservanza delle sue disposizioni. Il RDP deve altresì fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento dati del titolare.

L'RDP, anche per le prerogative che gli sono riconosciute di indipendenza e autonomia[7], si appresta a diventare una figura speciale nell'organigramma aziendale chiamato ad intervenire in tutte le scelte strategiche di business presenziando anche in CdA e ad essere il primo interlocutore dell'autorità in attività di controllo e vigilanza, qualunque essa sia.

È importante quindi non solo scegliere il RDP in base alle sue qualità professionali di conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, ma anche in base alla sua attitudine a gestire e ad assumere responsabilità tipiche di una funzione apicale.

Non sempre queste due caratteristiche (competenza specialistica ed elevato livello aziendale) si cumulano in una medesima persona. Peraltro, ragioni di opportunità che tengano conto degli equilibri gerarchici esistenti in azienda (e magari anche dei rapporti personali tra colleghi), sono spesso di ostacolo all'attribuzione della qualifica di RPD alla persona più adatta, la quale però non avrebbe la forza in concreto di assumere decisioni senza subire un forte condizionamento esterno finendo per avallare le scelte di trattamento già assunte dagli organi direttivi per via della sua subordinazione gerarchica e funzionale ad essi.

Per tali ragioni, viene sempre più spesso presa in considerazione la scelta di un RDP esterno[8]. Per tale opzione depone anche il fatto che, potendo il RPD essere anche una persona giuridica, esternalizzare in *outsourcing* tale funzione consente più facilmente di avere una consulenza estesa a diversi domini, dal diritto alla *security*, dalla *compliance* all'*information tecnology*, dall'*audit* ai regolamenti di settore.

L'RPD esterno, inoltre, potrà senz'altro esercitare la propria autonomia in modo più incisivo rispetto ad una funzione interna. La sua prospettiva terza, infatti, nonché il fatto che fornisce il medesimo servizio ad altre realtà imprenditoriali, rappresenta senza dubbio un canale di ingresso per nuove idee, processi e visioni che possono essere un prezioso stimolo al cambiamento per il titolare.

L'RPD esterno, insomma, può rappresentare una opportunità di confronto con altre realtà aziendali e quindi di innovazione tanto importante quanto può esserlo un reparto di R&D in una azienda ad alto contenuto tecnologico.

7. APPROCCIO FORMALE E APPROCCIO SOSTANZIALE

Il Regolamento, rispetto alla precedente impostazione della Direttiva 95/46/CE, ribalta completamente la prospettiva dalla quale gestire il trattamento dati.

Da un'impostazione prettamente formalistica si è passati ad una impostazione sostanzialista, che guarda a valle e a monte, cioè agli effetti del trattamento sui diritti degli interessati e ai presupposti di ordine tecnico e giuridico che lo legittimano.

Fermo restando l'obbligo di redigere un certo numero di documenti, il titolare deve oggi essere soggetto attivo nella determinazione della correttezza del trattamento e delle relative misure di sicurezza atte a garantire la protezione dei dati. Gli obblighi formali imposti dal GDPR (informative, registro del trattamento, analisi dei rischi, ecc.) non sono più strumenti fini a sé stessi come erano percepiti dalla Direttiva, ma prove di un atteggiamento proattivo del titolare che dimostri la sua effettiva presa di coscienza dei diritti fondamentali degli interessati coinvolti e delle esternalizzazioni negative delle sue scelte in un quadro di sviluppo consapevole e rispettoso della *mission* d'impresa. Quest'ultima non è più vista come un veicolo portatore di interessi dei suoi azionisti, ma come uno strumento di espressione sociale che deve soddisfare gli interessi di tutti gli *stakeholder*.

Torniamo allora alla distinzione tra *compliance* e processo. Assorbire a tutti i livelli aziendali i principi e le logiche sottese al GDPR e riflettere questi in processi e responsabilità ben definiti è l'unico modo per maturare una sensibilità adeguata al fenomeno della *privacy* e riuscire a prevenire trattamenti illegittimi ed evitare le pesanti sanzioni previste dal Regolamento[9]. L'approccio deve diventare sostanziale e non solo formale.

8. IL GDPR È UN'OPPORTUNITÀ

Assorbire la scienza del trattamento dati vuol dire dotarsi di un formidabile strumento di diagnosi e cura che consente al titolare di affrontare le sfide del prossimo futuro con un vantaggio competitivo non indifferente anche rispetto a paesi tecnologicamente più avanzati e a forte crescita economica[10].

Se negli anni passati la *privacy* è stata per lo più percepita come un carico burocratico da assolvere per evitare sanzioni, essa può e deve diventare invece il motore di un cambiamento culturale che serva ad avvicinare dipendenti, fornitori e clienti all'impresa, forzando quest'ultima a porsi interrogativi profondi ridiscutendo il suo rapporto con il tessuto commerciale e sociale in cui è innervata.

Il Regolamento, rispetto alla precedente impostazione della Direttiva 95/46/CE, ribalta completamente la prospettiva dalla quale gestire il trattamento dati

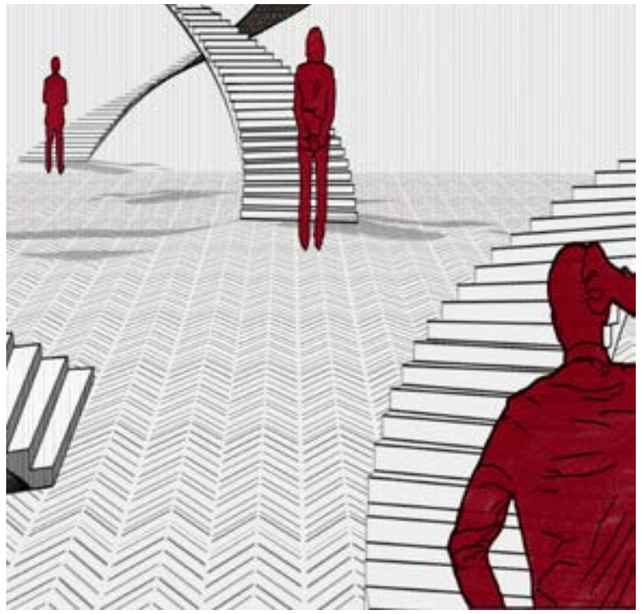
Mappare i trattamenti dati (art. 30 del GDPR), analizzare i rischi ad essi connessi (art. 35), rilevare i *data breach* (artt. 33 e 34), implementare i processi per la *privacy by design* (art. 25), sono esercizi che arricchiscono il coinvolgimento delle varie funzioni aziendali a tutti i livelli im-

PRIVACY

primendo all'impresa un forte impulso all'innovazione e al rafforzamento della c.d. *corporate identity*.
Avere la consapevolezza dei flussi dati (scopi e soggetti coinvolti), vuol dire conoscere l'azienda fin nei minimi dettagli il che si traduce quasi sempre in flessibilità, capacità di reagire rapidamente la mercato, risparmi di spesa e razionalizzazione di risorse.

9. UNO SGUARDO AL FUTURO. IL GDPR NASCE GIÀ VECCHIO?

Un'ultima considerazione a margine di questo breve contributo sulle prospettive future del GDPR è d'obbligo, e riguarda la tecnologia *blockchain*.
Il Regolamento, non diversamente dalla precedente Direttiva, ha un'impostazione prettamente centralistica, nel senso che esso contempla i trattamenti solo in una dimensione verticale, come operazioni che un soggetto (titolare) compie su dati personali altrui impiegando mezzi propri e scegliendo in autonomia lo scopo del trattamento e le misure di sicurezza adottate, avvalendosi all'occorrenza di soggetti terzi fornitori di soluzioni informatiche o servizi di *data processing* (responsabili e sub-responsabili).
Tale struttura mal si adatta alle soluzioni DLT – *Distributed Ledger Tecnology,* e in particolare alla *blockchain* di cui oggi si sente tanto parlare per l'impatto dirompente che avrà in pressoché tutti i settori di business.
La natura orizzontale e distribuita di una *blockchain* fa sì che i trattamenti di dati personali possano essere compiuti da una moltitudine indeterminata di soggetti che interagiscono tra loro in modo anonimo. Spesso si tratta di soggetti che agiscono anche in modo inconsapevole non conoscendo i dettagli del progetto globale a cui ubbidiscono semplicemente eseguendo le linee di un codice *open source* che opera secondo un protocollo *peer-to-peer.* La cieca interazione tra loro dà origine a quello che qualcuno definisce un vero e proprio organismo collettivo autonomo e semi-senziente[11].
Se nei prossimi anni le *blockchain* saranno le nuove piattaforme su cui avverranno tutte le transazioni tra utenti e su cui viaggeranno i loro dati personali, vorrà dire che l'attuale regolamento giungerà presto al suo limite elastico oltre il quale saremo costretti a pensare a questa materia (e evidentemente a molte altre) in termini completamente nuovi.



1 - Al momento di mandare alle stampe questo contributo, non è ancora diventato legge lo schema di decreto che dovrebbe abrogare il D.Lgs. 196/03 (il c.d. Codice Privacy) e introdurre una regolamentazione "interstiziale" che riempi gli spazi che il GDPR ha rimesso alla discrezionalità degli stati dell'Unione. Allo stato attuale, quindi, convivono in un connubio infelice sia il Codice Privacy che il GDPR, con disapplicazione da parte dell'interprete delle norme del primo in caso di contrasto con quelle del secondo.

2 - La distinzione è chiara nella lettera della Carta di Diritti Fondamentali dell'Unione Europea (2010) dove l'art. 7 (riprendendo i concetti già espressi all'art. 8 della Convenzione Europea dei Diritti dell'Uomo del 1950), sancisce il rispetto della vita privata e familiare (*privacy*) e l'art. 8 sancisce il diritto alla protezione dei dati di carattere personale. La prima nozione di dato personale, come «*informazione relativa ad una persona fisica identificata o identificabile*» risale invece alla Convenzione Strasburgo del 1981 (Convenzione 108), nella preistoria dell'era informatica.

3- Il recente caso di Cambridge Analytica è solo la punta di un gigantesco *iceberg*. Nei prossimi anni possiamo star certi che altri scandali sveleranno l'esistenza di consolidate prassi incompatibili con il GDPR. Frammenti di un traffico globale di dati personali in un mercato sotterraneo e miliardario.

4 - Per Future Agenda (futureagenda.com: The Increasing Value of Data) «*In Europa il valore delle nostre identità digitali, la somma di tutte le informazioni disponibili in formato digitale che ci riguardano varranno 1 triliardo di dollari entro il 2020. Ma non parliamo solo di dati personali; le "cose" stanno già generando una gran quantità di dati e nei prossimi cinque anni (2023) porteranno un incremento di valore di ulteriori 1,9 triliardi di dollari*»

5 - Per esempio, il diritto di accesso ai dati personali è stato utilizzato in sostituzione del diritto di accesso agli atti amministrativi (Caso C-434/16 Peter Nowak v Data Protection Commissioner [2017] ECLI:EU:C:2017:994) e per impedire l'utilizzo di talune prove nel processo penale (Caso C-582/14 Patrick Breyer v Bundesrepublik Deutschland [2016] ECLI:EU:C:2016:779). In altri casi è stato utilizzato per compensare l'esito di altre battaglie perse: un dipendente sospeso per motivi disciplinari ha chiesto i danni al datore di lavoro per accesso ingiustificato al proprio PC (dal quale aveva tratto elementi utili per legittimare la sospensione). Il cliente di una banca la cui domanda di mutuo era stata respinta, ha ottenuto un risarcimento per trattamento illecito dei suoi dati anche più consistente del prestito chiesto poiché il direttore della filiale al quale si era rivolto aveva lasciato incustodito il fascicolo con la pratica in corso.

6 - In tali termini, anche la targa di un taxi o il tempo atmosferico possono assurgere a dato personale (quanto alla targa è accaduto con riferimento alla combinazione dei dati di traffico dei taxi di New York raccolti dalla Taxi and Limousine Commission della città con le foto di VIP del mondo dello spettacolo; quanto al tempo atmosferico è emblematico l'esperimento di *smart city* condotto nei Paesi Bassi, in una via di Eindhoven, Stratumseind, dove l'incroci delle centraline metereologiche con le foto satellitari di aperture e chiusura di certi esercizi commerciali hanno fornito a posteriori informazioni sulla localizzazione e abitudini di taluni individui

7 - Ai sensi dell'art. 38 GDPR il RPD deve essere dotato delle risorse necessarie per assolvere i propri compiti e per mantenere la propria conoscenza specialistica. Continua l'articolo chiarendo che il titolare deve assicurarsi che il RPD «*non riceva alcuna istruzione per quanto riguarda l'esecuzione [dei suoi] compiti*» e che non sia «*rimosso*

o penalizzato [...] per l'adempimento dei propri compiti».

8 - In alternativa, il RDP più naturale è il legale interno se sufficientemente elevato di grado o il direttore generale se dotato di sufficienti competenze.

9 - Ai sensi degli artt. 83 ss. del Regolamento le sanzioni possono arrivare fino a 20 Mln di Euro o al 4% del fatturato mondiale del titolare.

10 - Come per esempio gli Stati Uniti o Paesi dell'est asiatico. Occorre tuttavia considerare che anche lì esistono numerose normative che, sebbene in modo non organico, affrontano la *privacy* in molti settori (sanitario, sicurezza lavoro, assicurazioni, ecc.).

11 - J. GARZIK, Bitcoin, the organism, TEDx Talk, Binghamton University, New York 30 marzo 2014, definisce il *bitcoin* come un organismo e il suo lavoro di sviluppo come la ricerca di un biologo. Sulla stessa linea di pensiero si pone Primavera de Filippi, Blockchain Technology and the Future of Work, Lift:Lab, Ginevra 11 febbraio 2016, che paragona le DLT ai plantoidi, delle forme di protovita artificiale ideate e realizzate per la prima volta da un *team* di ricerca dell'IIT (Center for Micro-BioRobotics) di Pontedera. Più recentemente, MATAN FIELD, The Blockchain Revolution: From Organisations to Organism, TEDx Talk, Breda 3 novembre 2016.

PRIVACY

LaScala SOCIETÀ TRA AVVOCATI

progetto grafico: www.mimmarapicano.com

Supplemento a **Iusletter** del 24/05/2018

Testata registrata il 24.09.2001, presso il Tribunale di Milano, al n. 525/01.
Proprietà di LA SCALA SOCIETA' TRA AVVOCATI PER AZIONI

Direttore Responsabile
Giuseppe La Scala

Direttore Editoriale
Luciana Cipolla

Redattori
Simona Daminelli (Capo), Francesco Concio (Vice), Tiziana Allievi, Sabrina Galmarini

Ha collaborato a questo supplemento
Francesco Rampone

Segreteria di Redazione
Ewelina Melnarowicz, Ilaria Turrini

Contatti: redazione@iusletter.com

Numero chiuso il 23 maggio 2018