Rivista Semestrale

Luglio – Dicembre 2018

N. 1/2018

Data Protection Law

Diritto delle nuove tecnologie, privacy e protezione dati personali

PRIVACY E PROTEZIONE DATI PERSONALI

DATA PROTECTION LAW

www.dataprotectionlaw.it

Diretta da Elio Errichiello

www.dataprotectionlaw.it

DATA PROTECTION LAW – RIVISTA GIURIDICA

Rivista online non soggetta ad obbligo di registrazione ai sensi dell'art. 3-bis del Decreto Legge 103/2012

DIRETTORE:
Elio Errichiello

COMITATO SCIENTIFICO:
Elio Errichiello, Livia Aulino, Lucrezia D'Avenia, Rosanna Celella, Giulio Riccio.

Sito web: www.dataprotectionlaw.it

Contatti: info@dataprotectionlaw.it

"Data Protection Law" è una rivista elettronica di diritto Open access pubblicata dall'associazione Data Protection Law. La rivista pubblica con cadenza semestrale numeri costituiti da articoli scientifici inediti, saggi, traduzioni di estratti da opere scientifiche significative e di recente pubblicazione o articoli rilevanti per la comunità scientifica, recensioni di libri ed eventi culturali.
I numeri della rivista ospitano contributi scientifici prodotti e sottoposti su invito diretto della redazione.
Tutti i contributi sono sottoposti a doppia blind peer review.

Indice.

ELIO ERRICHIELLO, Privacy by design e privacy by default: origini, prospettive e criticità.

Pag. 3

ROSANNA CELELLA, La circolazione dei dati personali. Trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali.

Pag. 16

LUCREZIA D'AVENIA, Il principio di accountability e la sicurezza del trattamento dei dati: un focus sull'anonimizzazione e sulle potenzialità della pseudonimizzazione dei dati.

Pag. 28

GIULIO RICCIO, La tutela della proprietà intellettuale e gli internet service provider.

Pag. 38

RITA DI MARCO, Blockchain e diritto italiano: uno sguardo d'insieme.

Pag. 51

PRIVACY BY DESIGN E PRIVACY BY DEFAULT: ORIGINI, PROSPETTIVE E CRITICITÀ

di Elio Errichiello

SOMMARIO: 1. Premessa. 2. Antecedenti legali all'articolo 25 del GDPR. 3. Aumentare l'efficienza attraverso un approccio proattivo. 4. Incorporare la privacy nel processo di progettazione, da dove iniziare? 5. Implementazione nelle dinamiche aziendali. 6. Criticità. 7. Conclusione.

This text provides a brief overview of the principles of "Privacy by Design" and "Privacy by default", codified in Article 25 of the European Regulation for the protection of personal data. These are important innovations in the field of European privacy law, although they already had legal and juridical precedents. The principles enucleated here constitute a positive change for stakeholders, and although the burden of complying with data protection legislation for data controllers becomes significantly more burdensome, setting an active role right from the project phase, they also offer benefits in terms of business efficiency, despite some critical issues.

1. Premessa.

Oggi i dati personali sono il nuovo "petrolio", sono tra le fonti di reddito più interessanti e proficue sia per le imprese commerciali che per le attività criminali, quindi è di vitale proteggerli nel modo adeguato. In questo contesto, i concetti di "*Privacy by Design*" e "*Privacy by Default*", introdotti dall'articolo 25[1] del Regolamento

[1] Articolo 25 - Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita:
"1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.
2. Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.

europeo per la protezione dei dati personali europea (regolamento 2016/679), devono essere considerati una soluzione obbligatoria per la tutela dei dati. Si tratta di uno delle maggiori novità introdotte dalla Commissione UE nel nuovo quadro giuridico per la protezione dei dati personali che verrà applicato dal Maggio 2018.

In questo documento, viene condotto un esame critico dell'articolo 25 del regolamento generale sulla protezione dei dati dell'Unione Europea. Con un titolo traducibile come "*Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita",* l'articolo 25 richiede che i principi fondamentali della protezione dei dati siano integrati nella progettazione e nello sviluppo di sistemi per l'elaborazione dei dati personali. Questo articolo delinea il retaggio giuridico dell'articolo 25 e mostra come le sue disposizioni offrano un sostegno considerevolmente più forte alla protezione dei dati in base alla progettazione e per impostazione predefinita rispetto a quanto previsto dalla Direttiva sulla protezione dei dati del 1995 (direttiva 95/46/CE). Il documento mostra inoltre che questo rafforzamento della protezione è in linea con la giurisprudenza della Corte europea dei diritti dell'uomo e della Corte di giustizia dell'Unione europea.

Nondimeno, l'articolo 25 soffre di molteplici difetti, in particolare la mancanza di chiarezza sui parametri e le metodologie per raggiungere i suoi obiettivi, una mancanza di comunicazione chiara e diretta con coloro che sono impegnati nella progettazione di servizi e prodotti, nonché la sua portata limitata ai soli titolari del trattamento. Presi insieme, questi difetti probabilmente ostacoleranno l'applicazione dei principi dell'articolo 25 nella prassi.

Il Regolamento generale sulla protezione dei dati (GDPR) modifica in modo significativo le norme sulla privacy europea. L'introduzione dei concetti "*Privacy by Design*" e "*Privacy by Default*" è una delle novità più attese della normativa, ed infatti le disposizioni dell'articolo 25 del GDPR sono tra le più innovative e ambiziose del nuovo regime di protezione dei dati riformato dell'UE. Sono rivolte essenzialmente allo sviluppo di sistemi di informazione, con l'obiettivo di garantire che si tengano in debito conto gli interessi relativi alla privacy durante l'intero ciclo di vita di tale sviluppo. Possono essere visti come una manifestazione della maggiore enfasi nel GDPR sul rendere conto della protezione dei dati e, allo stesso tempo, sul rendere i titolari del trattamento dei dati più responsabili. La loro motivazione è radicata nella convinzione

3. Un meccanismo di certificazione approvato ai sensi dell'articolo 42 può essere utilizzato come elemento per dimostrare la conformità ai requisiti di cui ai paragrafi 1 e 2 del presente articolo".

che l'implementazione di principi di protezione dei dati nell'architettura dei sistemi informativi potrà sostanzialmente migliorare l'applicazione degli stessi principi. Parte integrante di questa logica è un riconoscimento implicito del potenziale dell'architettura dei sistemi di informazione nel modellare la condotta umana in modo più efficace che non attraverso la semplice imposizione di leggi o contratti. Con l'incorporazione di norme legali nella fase di progettazione ci si promette di migliorare, se non di automatizzare, la loro applicazione *ex ante*, riducendo così il problema dello sviluppo tecnologico che spesso ostacola gli sforzi normativi dei legislatori.

La privacy by design richiede che i titolari del trattamento debbano considerare la privacy nelle fasi iniziali di progettazione e nel processo di sviluppo completo di nuovi prodotti, processi o servizi che implicano l'elaborazione di dati personali. Essa inverte la logica tradizionale e costituisce un approccio proattivo ed orientato al risultato rispetto alla problematica della privacy[2].

La *privacy by default*, ossia per impostazione predefinita, significa che quando un sistema o un servizio include delle scelte per l'individuo su quanti dati personali intende condividere con altri, le impostazioni predefinite dovrebbero essere quelle più attente a garantire la privacy. Anche se la *privacy by Design* e la *privacy by Default* diventeranno nuovi requisiti legali solo con l'entrata in vigore del GDPR, questi concetti non sono nuovi. Considerare l'impatto sulla privacy sin dall'inizio del processo di sviluppo è essenziale per affrontare con successo la tematica della protezione dei dati personali dei consumatori/clienti.

Questo nuovo approccio alla privacy si applica non solo alla progettazione di software o hardware; si estende anche alle strategie di business e ad altre pratiche organizzative. Strettamente collegato ad esso è un discorso politico più vecchio incentrato sulla creazione di "*Privacy-Enhancing Technologies*" (PET), cioè meccanismi tecnologici che promuovono il rispetto per gli interessi legati alla privacy. Tali discorsi si inseriscono in un più ampio sforzo interdisciplinare volto a incorporare i valori umani chiave - in particolare quelli centrali dell'etica - nel processo di progettazione tecnologica.

[2] GUTWIRTH - LEENES - DE HERT, *Reforming European Data Protection Law*, Springer, 2014, p. 303.

I principi fondamentali della "*Privacy by design"* sono stati così riassunti[3]: usare misure proattive piuttosto che reattive, anticipare e prevenire eventi invasivi (*Proactive not reactive*); i dati personali devono essere protetti automaticamente in ogni sistema informatico, se un individuo non fa nulla la sua privacy deve restare intatta (*Privacy as the Default*); la privacy deve essere incorporata nell'architettura dei sistemi informatici e nelle pratiche commerciali, non aggiunta dopo come un corollario (*Privacy embedded into design*); tutti gli interessi legittimi e gli obiettivi sono sistemati in modo daassicurare un risultato positivo (*Full Funcionality - Positive Sum, not Zero Sum*); la sicurezza è applicata all'intero ciclo vitale dei dati, i dati sono conservati in sicurezza e poi distrutti in sicurezza (*End-to-End Security - Full Lifecycle Protection*); agli stakeholder è assicurato che qualsiasi processo tecnologico o prodotto è soggetto a una verifica indipendente (*Visibility and Transparency - Keep it Open*); ingegneri e tecnici devono tenere al primo posto gli interessi degli individui, offrendo le misure più forti come default, fornendo informazioni e opzioni semplici da usare (*Respect for User Privacy - Keep it User-centric*).

2. Antecedenti legali all'articolo 25 del GDPR.

2.1 Legislazione.

L'articolo 25 non ha un equivalente esatto nella Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati. Quest'ultima contiene, tuttavia, disposizioni con una spinta analoga a quella dell'articolo 25, sebbene con un accentuato orientamento alla sicurezza. Il considerando 46 del preambolo della direttiva fa riferimento alla necessità di adottare "*misure tecniche e organizzative adeguate*" per salvaguardare gli interessi di protezione dei dati "*sia al momento della progettazione che al momento dell'esecuzione del trattamento, in particolare per garantirne la sicurezza ed impedire in tal modo qualsiasi trattamento non autorizzato*". Il considerando prosegue affermando che tali misure "*devono assicurare un adeguato livello di sicurezza, tenuto conto delle conoscenze tecniche e dei costi dell'esecuzione rispetto ai rischi che i trattamenti presentano e alla natura dei dati da proteggere"*. L'articolo 17 è simile, ma con un'enfasi sulla sicurezza ancora più pronunciata. Infatti, tutte le misure di protezione elencate nell'articolo 17

[3] CAVOUKIAN, *The 7 Foundational Principles of Privacy by Design, Implementation and Mapping of Fair Information Practices*, 2009.

riguardano direttamente la sicurezza delle informazioni, che è un elemento necessario, ma insufficiente, di un regime di protezione dei dati completo.

Le disposizioni equivalenti nella Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche) sono meno legate alle preoccupazioni in materia di sicurezza.

Mentre l'articolo 4, paragrafo 1, della direttiva continua a incentrare l'attenzione sulla sicurezza disponendo che il *"fornitore di un servizio di comunicazione elettronica accessibile al pubblico deve prendere appropriate misure tecniche e organizzative per salvaguardare la sicurezza dei suoi servizi*", il considerando 30 del preambolo fornisce un incoraggiamento diretto per le misure di progettazione che vanno oltre un obbligo di sicurezza: "*I sistemi per la fornitura di reti e servizi di comunicazione elettronica dovrebbero essere progettati per limitare al minimo la quantità di dati personali necessari*". Un'altra disposizione pertinente che non è legata alla sicurezza è l'articolo 14, comma 3, che richiede l'adozione di misure "*dirette a garantire che le apparecchiature terminali siano costruite in maniera compatibile con il diritto degli utenti di tutelare e controllare l'uso dei loro dati personali* ". Questa disposizione è in linea con l'articolo 3, comma 3, lettera c) della direttiva 1999/5/CE che stabilisce che le apparecchiature radio e le apparecchiature terminali di telecomunicazione incorporano dei dispositivi di sicurezza per garantire la protezione dei dati personali e della vita privata dell'utente e dell'abbonato.

Guardando oltre la legislazione dell'UE, troviamo poche norme giuridiche che riguardano direttamente o indirettamente la protezione dei dati in base alla progettazione e per impostazione predefinita. A livello nazionale, la legge federale tedesca sulla protezione dei dati del 1990 è quella che si avvicina di più alla norma del GDPR. Sotto la nomenclatura "*Datenvermeidung und Datensparsamkeit*" (eliminazione dei dati ed economia dei dati), la sezione terza della legge richiede che i sistemi di informazione siano progettati con l'obiettivo di elaborare il minor numero possibile di dati personali. Inoltre, stabilisce che i dati personali devono essere pseudonimizzati o resi anonimi per quanto ragionevole in relazione al livello di protezione desiderato.

A livello internazionale, l'unico trattato che riguarda specificamente la protezione dei dati - la convenzione del Consiglio d'Europa del 1981 per la protezione delle

persone rispetto al trattamento automatizzato di dati personali - omette principi specifici sulla protezione dei dati in base alla progettazione e per impostazione predefinita. Tuttavia, la proposta di revisione della Convenzione del 2016 introduce una serie di disposizioni all'articolo 8bis che abbracciano alcuni di tali principi, ma utilizzando formulazioni diverse rispetto a quelle contenute nell'articolo 25 del GDPR. In particolare, il testo dell'articolo 8bis non prevede disposizioni chiare per la protezione "*di default*" - diversamente dall'articolo 25, comma 2, del GDPR.

2.2 Giurisprudenza.

La Corte europea dei diritti dell'uomo (CEDU) ha affrontato già in passato l'applicazione di principi simili a quelli manifestati nell'articolo 25. Ciò si è verificato nel 2008 nel caso I c. Finlandia[4] (sentenza del 17 luglio 2008). In questo caso, la Corte ha constatato all'unanimità che la Finlandia aveva violato i suoi obblighi di garantire il rispetto della vita privata ai sensi dell'articolo 8 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (CEDU), a causa della sua incapacità di assicurare, attraverso misure organizzative tecnologiche, la riservatezza dei dati dei pazienti in un ospedale pubblico. La ricorrente era una donna che era stata infettata dall'HIV e che sospettava che le sue cartelle cliniche, redatte mentre era ricoverata, fossero state visualizzate da terze persone non autorizzate. La sua denuncia riguardava principalmente il fatto che l'ospedale in questione aveva creato un sistema di gestione delle cartelle cliniche senza mettere in atto un meccanismo per la registrazione all'accesso che conservasse i dati del registro in modo tale da poter verificare successivamente se i registri delle cartelle erano stati aperti senza un'autorizzazione adeguata. Mentre la legge finlandese ha fornito protezione per i dati dei pazienti - compreso il risarcimento agli interessati per i danni subiti in caso di divulgazione non autorizzata dei dati - la Corte EDU ha dichiarato che la Finlandia doveva fornire più della protezione dei dati per soddisfare i suoi obblighi positivi ai sensi Articolo 8 della CEDU. La Corte osservava che il semplice fatto che la legislazione nazionale avesse fornito al richiedente l'opportunità di chiedere il risarcimento dei danni causati da una presunta divulgazione illecita di dati personali non era sufficiente a proteggere la sua vita privata. Ciò che è richiesto in questo contesto è una protezione pratica ed efficace per escludere qualsiasi possibilità di accesso non autorizzato che si verifichi. Questa protezione non è stata riscontrata nel caso esaminato. Anche se la Corte non ha fatto

[4] CEDU, I c. Finlandia, 17 luglio 2008, n. 20511/03.

alcun riferimento alla protezione dei dati mediante design e per default, o nozioni strettamente correlate, la motivazione alla base della sua sentenza richiede l'adozione di una mentalità e di metodi in linea con queste nozioni. Inoltre, si può leggere nella sentenza della Corte un principio di garanzia dei limiti di accessibilità dei dati che, come punto di partenza, garantisce la riservatezza dei dati. Di conseguenza, il risultato complessivo della sentenza I c. Finlandia è effettivamente quello di garantire la protezione dei dati in base alla progettazione e per impostazione predefinita, un requisito integrale degli obblighi positivi di uno Stato per garantire il rispetto dei diritti stabiliti nell'articolo 8 della CEDU, almeno in relazione alla garanzia della riservatezza dei dati relativi alla salute di una persona.

Se questo risultato può essere esteso al trattamento di altri tipi di dati personali rispetto ai dati sanitari, o per coprire altre funzionalità piuttosto che garantire la riservatezza dei dati, è meno certo. La Corte ha fondato la sua motivazione sulla natura speciale dei dati sanitari, rilevando che la loro protezione è di fondamentale importanza per il godimento da parte di una persona del suo diritto al rispetto della vita privata e familiare come garantito dall'articolo 8 della Convenzione, un principio vitale nei sistemi giuridici di tutte le parti contraenti della convenzione e cruciale non solo per la privacy della persona interessata ma anche per preservare la sua fiducia nella professione medica e nei servizi sanitari in generale. La Corte ha poi affermato che queste considerazioni sono particolarmente valide per quanto riguarda la protezione della riservatezza delle informazioni sull'infezione da HIV di una persona, date le questioni delicate che circondano questa malattia. Pertanto, secondo la Corte EDU, il diritto nazionale deve offrire garanzie adeguate per impedire qualsiasi comunicazione o divulgazione di tali dati personali che possa essere in contrasto con le garanzie di cui all'articolo 8 della Convenzione.

Fermo restando lo status speciale di tali dati, tuttavia, non vi sono ragioni per ritenere che altri tipi di dati personali non si qualifichino di fatto per una protezione analoga. Ciò è particolarmente vero per le categorie di dati personali comunemente considerate sensibili, come quelle elencate nell'articolo 6 della Convenzione 108 (origine razziale, opinioni politiche, credenze religiose o di altro tipo, oltre ai dati relativi alla loro "*salute*" o alla loro vita sessuale).

Ancora, il trattamento di tipi di dati personali più ordinari può richiedere l'attuazione di una "*protezione pratica ed efficace*" (utilizzando le parole della Corte) in particolari circostanze - ad esempio quando il trattamento può facilmente dar luogo ad

una discriminazione ingiusta. In tali casi si può ritenere che tale protezione possa estendersi a funzionalità diverse dall'assicurare la riservatezza dei dati - ad esempio garantire che la quantità di dati personali raccolti sia limitata a quanto necessario per conseguire lo scopo o ai fini per i quali i dati sono raccolti e ulteriormente elaborati.

La Corte di giustizia dell'Unione europea (CGUE) non si è ancora pronunciata direttamente sull'articolo 25 del GDPR, né ha emesso una sentenza che impone la protezione di fatto dei dati personali in modo così diretto come nel citato caso della Corte EDU.

Tuttavia, ha pronunciato alcune sentenze significative lungo il percorso di diffusione della tecnologia legata a Internet. Le prime due pronunce[5] hanno riguardato le proposte fatte in Belgio per impiegare mezzi invasivi di ispezione volti a contrastare la pirateria digitale, tramite *Deep Packet Inspection* (DPI), una modalità di analisi del contenuto dei pacchetti di dati che transitano all'interno di una rete al fine di individuare contenuti non aderenti a precisi criteri definiti in precedenza. Sebbene la CGUE si sia astenuta dal promuovere attivamente la protezione dei dati by design e by default, in questi casi, ha fermato efficacemente la diffusione di una tecnologia intrusiva della privacy.

Successivamente, la Corte di giustizia dell'Unione europea si è pronunciata nel famoso caso *Google Spain*[6]. La sentenza della Corte non ha messo in crisi il motore di ricerca di Google; nondimeno, respingendo l'argomento di Google secondo cui le sue operazioni sui motori di ricerca sono neutrali dal punto di vista del valore, in quanto semplici applicazioni robotiche di algoritmi al di fuori dell'ambito della legge sulla protezione dei dati, la CGUE ha richiesto a Google (e ad altri operatori dei motori di ricerca) di riconfigurare aspetti sistemici di tali operazioni in modo da garantire maggiormente la privacy degli utenti. Ha quindi indirettamente alimentato gli obiettivi dell'articolo 25 del GDPR.

Inoltre, la CGUE ha indirettamente trattato questi principi anche nel caso *Digital Rights Ireland*[7]. In tale giudizio, con sentenza dell'8 aprile 2014, la Corte ha dichiarato

[5] C-70/10, *Scarlet Extended* contro *Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM*), 24 novembre 2011, ECLI: EU: C: 2011: 771; C-360/10, SABAM / Netlog, 16 febbraio 2012, ECLI: EU: C: 2012: 85.
[6] C-131/12, *Google Spain* c. *Agencia Española de Protección de Datos* (AEPD) e Mario Costeja González, 13 maggio 2014, ECLI: EU: C: 2014: 317.
[7] C-293/12 e C-594/12, *Digital Rights Ireland Ltd* e Seitlinger e altri, 8 aprile 2014, ECLI: EU: C: 2014: 238.

invalida la Direttiva 2006/24/EC sulla conservazione dei dati, a seguito di rinvio pregiudiziale presentato sia dalla *High Court* irlandese che dalla *Verfassungsgerichtshof* (Corte costituzionale) austriaca per violazione dei diritti fondamentali del rispetto della vita privata e della protezione dei dati personali, sanciti entrambi dalla Carta dei diritti fondamentali dell'Unione Europea. La direttiva prevedeva, ai fini della prevenzione, individuazione e perseguimento di reati gravi, quali, in particolare, la criminalità organizzata e il terrorismo, che i fornitori di servizi di comunicazione elettronica debbano conservare i dati di traffico e localizzazione e comunque i dati necessari per identificare l'utente, mentre non consente la conservazione dei contenuti della comunicazione o dell'informazione consultata. La Corte ha ritenuto che ciò non fosse compatibile con gli articoli 7, 9, e 11 della Carta dei diritti fondamentali dell'Unione europea.

3. Aumentare l'efficienza attraverso un approccio proattivo.

Come anticipato, secondo la Direttiva 95/46/CE, i responsabili del trattamento devono già adottare misure tecniche e organizzative adeguate per proteggere i dati contro l'elaborazione illecita. Ciò, tuttavia, lascia spazio alle considerazioni sulla privacy soltanto come un mero discorso a margine nel processo di sviluppo. Il GDPR, invece, richiede che le organizzazioni considerino la privacy e la protezione dei dati come il primo passaggio da cui partire. Potrebbe sembrare un cambiamento complesso, ma è in realtà più facile adottare soluzioni adeguate alla tutela sin dall'inizio piuttosto che applicare le considerazioni sulla privacy dopo che un progetto è completamente sviluppato[8].

Quando si è pensato in anticipo a quali dati personali si desideri utilizzare, per quale scopo e come farlo in modo legittimo, si ridurrà la possibilità di scoprire in una fase successiva che l'incorporazione di un meccanismo di tutela della privacy sia tecnologicamente impegnativa, costosa o addirittura impossibile.

L'applicazione del concetto di privacy by design renderà quindi il processo di sviluppo più efficiente. Conoscere i dati che si desiderano utilizzare e dare ai soggetti una scelta sul modo in cui i propri dati vengono utilizzati, applicando la *privacy by default*, renderà anche più facile rendere trasparenti i dati trattati. E la trasparenza è fondamentale quando si tratta di guadagnare la fiducia dei clienti per raccogliere i dati.

[8] HOEPMAN, *Privacy Design Strategies*, in CUPPENS-BOULAHIA, CUPPENS, JAJODIA, ABOU EL KALAM, SANS T. (eds) *ICT Systems Security and Privacy Protection.* SEC 2014. *IFIP Advances in Information and Communication Technology*, vol 428, Springer, 2014, p. 446.

Inoltre, l'applicazione del principio di *privacy by design* può "[…] *consentire di raggiungere più facilmente l'obiettivo di una maggiore sicurezza delle informazioni e come, letta alla luce di questo nuovo principio, la sicurezza possa dare un impulso nuovo al raggiungimento di un obiettivo cruciale per l'affermazione dei Big Data, quale è quello legato alla qualità dei dati*"[9].

In sintesi, l'applicazione obbligatoria dei principi di *privacy by design* e *privacy by default* è un'innovazione di cui molti avvertivano già l'esigenza, e che risponde in primo luogo alle esigenze di efficienza delle aziende.

È per queste ragioni che molte società hanno già incorporato questi concetti nei loro processi di sviluppo prima ancora che il testo del GDPR diventi operativo.

4. Incorporare la privacy nel processo di progettazione, da dove iniziare?

Per incorporare la privacy nel processo di progettazione occorre tener conto di diversi aspetti.

Anzitutto, occorre operare entro i confini legali ed essere responsabile.

Una strategia sulla privacy è essenziale per fare scelte anticipate nel processo di sviluppo in merito a come si desidera affrontare la privacy all'interno del nuovo servizio o prodotto. Occorre valutare anticipatamente se l'idea può essere eseguita entro i confini legali pertinenti. Un buono strumento per farlo è la realizzazione di una valutazione dell'impatto sulla privacy (*Privacy Impact Assessment* o *P.I.A.*). Un *P.I.A.* aiuterà le aziende a individuare i rischi per la privacy all'interno del nuovo design in fase di sviluppo. Non bisogna dimenticare di conservare i risultati della valutazione dell'impatto sulla privacy. Questo strumento permetterà di dimostrare la ragion d'essere dietro determinate decisioni in una fase successiva.

Inoltre, la comunicazione è fondamentale.

La comunicazione verso i soggetti interessati è molto importante per affrontare le fasi iniziali di progettazione e per tutto il processo di sviluppo nella sua interezza. Per i soggetti interessati deve essere chiaro a chi possono rivolgersi se vogliono sapere di più sul trattamento dei propri dati personali e su come esercitare i propri diritti.

Infine, va posta l'attenzione alla sicurezza dei dati, alla qualità e alla cessazione.

In ogni fase di sviluppo, è importante pensare a misure di sicurezza adeguate, a come garantire la qualità dei dati e a cosa fare con i dati quando il prodotto o il servizio verranno ritirati.

[9] D'ACQUISTO - NALDI, *Big Data e Privacy by design*, Torino, 2017, p.3.

5. Implementazione nelle dinamiche aziendali.

La riuscita implementazione della *privacy by design* e della *privacy by default* richiede che i dipendenti - in particolare quelli coinvolti nello sviluppo di nuovi prodotti e servizi - abbiano abbastanza conoscenze di base sulla tutela della privacy. È necessario sviluppare politiche, linee guida ed istruzioni di lavoro relative alla protezione dei dati, ed uno specialista della privacy dovrebbe essere disponibile per contribuire all'applicazione di tali requisiti. Deve essere preso in considerazione il metodo di sviluppo (agile, cascata ecc.) utilizzato all'interno dell'azienda, per applicare i concetti in esame durante tutto il processo di sviluppo. Ciò permetterà ai team di sviluppo di adottare misure appropriate nelle fasi corrispondenti. E quando un progetto è stato completato, deve essere testato dall'azienda e monitorato per tutta la durata della sua vita.

Infine, la *PbD* non dovrebbe limitarsi allo sviluppo di soluzioni tecniche intelligenti e alla loro integrazione nei sistemi. È altrettanto importante esaminare molto presto nel processo di pianificazione se e come limitare la quantità di dati personali al minimo indispensabile, e trattarli solo se necessario, come richiesto dal considerando 78 e dall'art. 25 del GDPR. La tendenza a riprodurre sistemi burocratici sempre più complicati nella tecnologia dell'informazione può essere riconosciuta in altri processi IT e può portare a gravi problemi per la protezione dei dati. Questo rischio esiste anche quando si fanno grandi sforzi per garantire la protezione dei dati e prevenire l'uso improprio dei dati[10].

6. Criticità.

L'articolo 25 del GDPR soffre di molteplici carenze. Una ovvia debolezza è la vaghezza e la complessità del suo linguaggio. Ciò è accresciuto da una scarsità di indicazioni autorevoli e chiare sui parametri e le metodologie per il raggiungimento della protezione dei dati sin dalla progettazione e per impostazione predefinita. Questo potrebbe creare difficoltà per l'applicazione della norma, nondimeno applicare rigide sanzioni per la violazione dell'articolo 25, comma 1, non sarà facile, dato il modo molto generale (e orientato ai processi) in cui vengono formulati i suoi obblighi.

Inoltre, la vaghezza e la complessità del linguaggio legale nell'articolo 25 ostacola la "*conversazione normativa*" non solo tra i legislatori dell'UE e gli altri membri

[10] SCHAAR, *Identity in the Information Society*, Springer, 2010.

della comunità legale, ma, soprattutto, tra i legislatori dell'UE e le autorità di protezione dei dati da una parte e dall'altra parte, la comunità di persone che lavorano effettivamente nel campo dello sviluppo di servizi e prodotti.

Il linguaggio utilizzato nell'articolo 25 può apparire in effetti, come una sorta di crittografia nei confronti di persone che sono prive di qualifiche e competenze legali in questo settore. Questo ostacola la capacità dell'Articolo 25 di stimolare la comunità ingegneristica affinché lavori nella direzione desiderata.

La portata dell'articolo 25 sullo sviluppo dei sistemi di informazione è probabilmente anche ostacolata dalla sua portata limitata. Come indicato, le misure dell'articolo 25 sono principalmente imposte ai titolari del trattamento dei dati. Tuttavia, non possiamo presumere che le decisioni di progettazione di base nello sviluppo dei servizi o prodotti siano prese esclusivamente o prevalentemente da soggetti che agiscono in qualità di titolari. L'aggravante di questa lacuna è che l'articolo 25, comma 1, formula la fase di progettazione come "il momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso", una fase che potrebbe non coincidere con il momento in cui un particolare prodotto è effettivamente progettato e prodotto.

Il Gruppo di lavoro Articolo 29 ha adottato una visione espansiva della categoria "controller" (titolare del trattamento in italiano) in relazione alle entità coinvolte nello sviluppo o nella fornitura di dispositivi e piattaforme per l'emergente Internet delle cose. La CGEU ha anche preso in considerazione un'ampia visione della categoria "*controller*" nel caso *Google Spain*. Ciò nonostante, è molto dubbio che l'articolo 25 comprenda tutti i soggetti della comunità di ingegneri e progettisti coinvolti nella fase di sviluppo.

I redattori del Regolamento sembrano essere consapevoli di queste carenze in quanto il regolamento stabilisce che i "*produttori*" di prodotti, servizi e applicazioni che implicano l'elaborazione dei dati personali dovrebbero essere incoraggiati a tener conto degli ideali dell'articolo 25 nell'esercizio delle loro attività (considerando 78). Questa clausola, tuttavia, è confinata alla fine di un considerando lungo e densamente formulato nel preambolo del regolamento; ed è anche formulata in modo meno rigoroso rispetto ad altri obblighi dei *data controller*.

7. Conclusione.

L'introduzione dei principi di *privacy by design* e *default* è la formalizzazione di un modello sano di gestione dei dati personali coordinato all'efficienza aziendale.

Il GDPR intende dare ai soggetti interessati più potere sui loro dati personali. L'implementazione di *privacy by design* e *default* rispecchia chiaramente tale obiettivo. Offrire l'opzione più restrittiva sulla privacy come impostazione predefinita darà alle persone un messaggio chiaro su quali dei loro dati personali possono essere usati dal servizio o prodotto. L'incorporazione della *privacy by design* nel processo di sviluppo è l'unico modo per applicare la privacy con successo in un'ottica aziendale. Per le imprese, questi concetti forniscono un'opportunità per aumentare l'efficienza e ottenere la fiducia dei soggetti interessati.

In conclusione, si tratta di due concetti che riescono a far combaciare i diritti e gli interessi dei consumatori con quelli delle aziende, e sono a tal punto una delle migliori innovazioni del nuovo Regolamento che iniziano a trovare spazio nella prassi aziendale già da prima che la normativa in oggetto divenga operativa.

Il principale ostacolo da affrontare per la corretta applicazione della norma è, invece, nella lettera dell'art. 25 del GDPR, in quanto da una parte la norma rischia di essere di difficile interpretazione per i tecnici preposti alla fase di sviluppo, d'altra parte gli obblighi sembrano ricadere espressamente sul solo titolare del trattamento, che resta normalmente estraneo alla progettazione.

LA CIRCOLAZIONE DEI DATI PERSONALI. TRASFERIMENTI DI DATI PERSONALI VERSO PAESI TERZI O ORGANIZZAZIONI INTERNAZIONALI

di Rosanna Celella

SOMMARIO: 1. Nozioni introduttive. 2. I flussi di dati transfrontalieri in base alla Direttiva 95/46/CE. 3. Cosa cambia con il nuovo Regolamento. 4. Dal caso *Schrems* al caso *Microsoft Ireland*.

This paper focused on the international data transfers and flows of personal data and on the principal differences between Directive 95/46/CE and General Data Protection Regulation (GDPR).

Under EU law, the General Data Protection Regulation provides for the free flow of data within the European Union. However, it contains specific requirements relating to the personal data transfers to third countries outside the EU and to international organisations. These transfers are not possible unless they meet the conditions set out in the GDPR; infact the GDPR aims to offer the same level of protection to personal data being transferred to third countries as they enjoy within the EU.

After the analyse of the law, we will continue with the analys of Schrems case and the very recent Microsoft Ireland case, both focused on the international data transfers.

1. Nozioni introduttive

La Direttiva 95/46/CE in materia di protezione dei dati personali, che tra pochi mesi sarà abrogata Regolamento UE 2016/679, trova la sua base giuridica nell'art. 100 A TUE. L'instaurazione ed il funzionamento del mercato interno, volto ad assicurare la libera circolazione di merci, persone, servizi e capitale, non possono prescindere dalla libera circolazione dei dati personali da uno Stato membro all'altro e dalla salvaguardia dei diritti fondamentali della persona. Si era già previsto che l'integrazione economica e sociale, conseguente all'instaurazione del mercato unico, avrebbe comportato un sensibile aumento dei flussi transfrontalieri di dati e tale concetto è ribadito

dal considerando n. 5 del nuovo Regolamento[11]. L'esigenza di armonizzazione del diritto alla protezione dei dati personali nasce proprio dalla necessità di consentire la circolazione dei dati, in quanto la scelta di abbattere i dazi nel mercato europeo non avrebbe avuto senso ed effettività se non fosse stata accompagnata dalla libera circolazione dei dati; peraltro, accelerare le 4 libertà fondamentali dell'Ue[12] richiedeva inevitabilmente l'implementazione della ulteriore libertà di circolazione dei dati. Dunque non deve stupire l'effervescenza normativa che sta recentemente caratterizzando la materia e che deriva dall'evoluzione economica e dagli obiettivi dello stesso processo di integrazione europea[13]. Attualmente la situazione in materia di trasferimento dei dati è decisamente *sui generis* e crea non poche difficoltà in termini di interpretazione ed applicazione pratica. Si applica, infatti, una Direttiva che attualmente è in vigore, ma che vi rimarrà solo fino al maggio 2018, ossia dal momento in cui il Regolamento, esistente ma non ancora efficace, comincerà ad essere applicato. Difficile, dunque, muoversi in questo scenario che richiede un acrobatico e rilevante esercizio ermeneutico che si presenta più semplice quando il Regolamento si pone in termini di continuità con la Direttiva e quindi ne costituisce solo uno sviluppo, una specificazione, ma che diventa più complesso quando tra Regolamento e Direttiva è evidente qualche contraddizione.

La preoccupazione maggiore si denota all'interno degli uffici legali delle aziende che vorrebbero investire in *compliance*, tenendo conto anche del fatto che, quantomeno con riferimento ai flussi transfrontalieri di dati, ci si ritrova ad avere a che fare con assetti normativi e statuali differenti da quelli dell'Ue. Tutto ciò dimostra come il lavoro di interpretazione ed attuazione dell'attuale quadro normativo europeo in materia di protezione dei dati personali ponga innumerevoli nuove sfide per gli Stati e le aziende che non vanno assolutamente sottovalutate.

2. I flussi di dati transfrontalieri in base alla Direttiva 95/46/CE

[11] "*L'integrazione economica e sociale conseguente al funzionamento del mercato interno ha condotto a un considerevole aumento dei flussi transfrontalieri di dati personali e quindi anche dei dati personali scambiati, in tutta l'Unione, tra attori pubblici e privati, comprese persone fisiche, associazioni e imprese. Il diritto dell'Unione impone alle autorità nazionali degli Stati membri di cooperare e scambiarsi dati personali per essere in grado di svolgere le rispettive funzioni o eseguire compiti per conto di un'autorità di un altro Stato membro*".

[12] Libertà di circolazione dei capitali, delle merci, dei servizi e delle persone.

[13] Il diritto alla protezione dei dati personali è previsto dall'art. 16 TFUE e, dunque, figurando tra i primi articoli, se ne può ben comprendere il valore fondante nel processo di integrazione europea.

La Direttiva sulla protezione dei dati non si limita a prevedere la libera circolazione di dati fra gli Stati membri, ma contiene anche disposizioni sui requisiti da soddisfare per il trasferimento dei dati personali verso Paesi terzi al di fuori dell'Ue[14].

La nozione di trasferimento la troviamo all'art. 25 par. 1: <<*trasferimento verso un Paese terzo di dati personali oggetto di un trattamento o destinati ad essere oggetto del trattamento dopo il trasferimento*>>. Il flusso transfrontaliero dei dati consiste nel trasferimento di dati personali verso un destinatario soggetto a giurisdizione straniera.

In materia di trasferimento dei dati personali va ricordata la nota sentenza *Bodil Lindqvist*[15], in cui per la prima volte la Corte di Lussemburgo affronta l'argomento dei dati personali connesso con il mondo del *web*, stabilendo che il caricamento di dati personali su una pagina *web* non configura un trasferimento di dati personali, bensì un semplice trattamento[16].

Il trasferimento di dati personali verso Paesi terzi è libero da restrizioni nell'ambito del diritto nazionale sulla protezione dei dati se è stata accertata l'adeguatezza della protezione dei dati presso il destinatario o qualora risulti necessario per interessi specifici dell'interessato o per prevalenti interessi legittimi altrui, in particolare per interessi pubblici rilevanti.

La libera circolazione dei dati verso Paesi terzi con un adeguato livello di protezione di detti dati è prevista dall'art. 25 par. 1 della Direttiva. A norma dell'art. 25 par. 6 della Direttiva, la Commissione europea è competente a valutare il livello di protezione dei dati in paesi stranieri attraverso decisioni di adeguatezza. Una decisione di adeguatezza da parte della Commissione europea è vincolante, dunque, in tal caso, i dati possono circolare verso il Paese terzo in questione senza procedure di verifica o di autorizzazione presso le autorità nazionali[17].

L'art. 26 par. 1 della Direttiva prevede casi che devono essere intesi come deroghe alla regola secondo cui il libero trasferimento di dati verso altri Paesi richiede un

[14] La Direttiva disciplina i flussi transfrontalieri di dati personali alla Sezione IX, Capo IV, artt. 25 e 26.
[15] CGUE, *Bodil Lindqvist*, 6 novembre 2003.
[16] La Corte, infatti, ha sottolineato che, tenuto conto dello sviluppo di Internet all'epoca della redazione della Direttiva, "*non si può presumere che il legislatore comunitario avesse l'intenzione di includere prospettivamente nella nozione di "trasferimenti verso un paese terzo di dati personali" l'inserimento (...) di dati in una pagina Internet, anche se questi sono così resi accessibili alle persone di paesi terzi in possesso dei mezzi tecnici per consultarli*".
[17] Una delle più importanti decisioni di adeguatezza riguarda norme molto simili ad un codice di condotta note come principi di approdo sicuro in materia di riservatezza. Tali principi sono stati messi a punto tra l'UE e gli USA per le imprese commerciali statunitensi. Si tratta del cosiddetto *Safe Harbour*, recentemente messo in discussione dalla CGUE e sostituito dal nuovo accordo denominato *Privacy Shield*.

adeguato livello di protezione di tali dati nel Paese destinatario e vanno interpretate in senso restrittivo; tali casi sono il consenso dell'interessato ed altre circostanze equiparate[18].

In caso di trasferimento di dati verso Paesi terzi che non garantiscono un adeguato livello di protezione dei dati, il titolare del trattamento può essere tenuto a sottoporre il flusso di dati in questione all'esame dell'autorità di controllo, dimostrando l'esistenza di una base giuridica per il trasferimento di dati verso il destinatario e la presenza di misure idonee a garantire un'adeguata tutela dei dati presso il destinatario. Tali misure possono includere: clausole contrattuali fra il titolare del trattamento che trasferisce i dati ed il destinatario straniero dei dati; norme vincolanti d'impresa, applicabili solitamente per i trasferimenti di dati nell'ambito di un gruppo multinazionale di imprese; accordi internazionali speciali che disciplinano i trasferimenti di dati verso autorità straniere.

La Commissione europea, con l'ausilio del Gruppo di lavoro articolo 29, ha elaborato clausole contrattuali tipo ufficialmente certificate da una decisione della Commissione come prova di un'adeguata protezione dei dati. Poiché le decisioni della Commissione sono vincolanti negli Stati membri, le autorità nazionali di controllo dei flussi transfrontalieri di dati devono riconoscere la validità di tali clausole contrattuali tipo nei propri procedimenti, in quanto esse costituiscono una prova sufficiente dell'esistenza di garanzie adeguate[19].

Tali clausole contrattuali tipo, incorporate nel testo di un contratto avente ad oggetto l'esportazione dei dati personali, impegnano l'importatore (stabilito al di fuori dell'Ue) al rispetto di precise garanzie relative al loro trattamento e garantiscono un livello adeguato di tutela dei dati limitatamente ad una determinata finalità di trattamento. Attualmente, si dispone di tre set di clausole-tipo, sempre adeguate per decisione della Commissione e sussiste, inoltre, la possibilità di elaborare clausole *ad hoc*,

[18] Ai sensi della Direttiva gli interessi dell'interessato possono giustificare la libera circolazione dei dati verso un Paese terzo sé è soddisfatta almeno una delle seguenti condizioni: l'interessato ha espresso il proprio consenso inequivocabile al trasferimento dei dati; l'interessato ha stipulato o si accinge a stipulare un contratto che richieda chiaramente il trasferimento dei dati verso un destinatario all'estero; è stato concluso un contratto tra il titolare del trattamento ed un terzo nell'interesse dell'interessato; il trasferimento avviene a partire da un registro pubblico, ossia si è in presenza di un caso di interessi prevalenti della popolazione in generale che consiste nel fatto di poter accedere a informazioni conservate in registri pubblici; il trasferimento è necessario per la salvaguardia dell'interesse vitale dell'interessato, di un interesse pubblico rilevante (diverso dalla sicurezza nazionale o pubblica, in quanto tali settori non rientrano nell'ambito di applicazione della Direttiva), per rivendicare, esercitare o difendere un diritto per via giudiziaria.

[19] FRA, *Manuale sul diritto europeo in materia di protezione dei dati*, Agenzia dell'Unione europea per i diritti fondamentali e Consiglio d'Europa, 2014.

ma *sub iudicium* della Commissione. Difatti, l'esistenza di clausole contrattuali tipo non vieta ai titolari del trattamento di formulare altre clausole contrattuali *ad hoc* che, tuttavia, dovrebbero garantire il medesimo livello di tutela offerto dalle clausole contrattuali tipo.

Il contenuto tipico delle clausole contrattuali consta in una prima parte destinata alle informazioni identificative dell'esportatore e dell'importatore dei dati personali ed altre disposizioni di natura definitoria, seguite da clausole sulla responsabilità dell'esportatore, clausole sugli obblighi dell'importatore e la cosiddetta "clausola di terzo beneficiario", che consente agli interessati di esercitare diritti contrattuali, pur non essendo parte del contratto.

Per i trasferimenti da titolare del trattamento ad incaricato esiste un unico set di clausole contrattuali tipo ed è quello di cui alla Decisione 2010/87/EU della Commissione[20]. Si tratta dell'ipotesi in cui *data controller* affidano a terzi attività relative al proprio *core business* che comportino il trasferimento di dati personali dal luogo di stabilimento del *data controller* verso Paesi la cui normativa non appronta garanzie adeguate e similari rispetto alle normative europee. In tali particolari ipotesi la clausola 2010/87/EU stabilisce nei confronti del *data processor* precisi e restrittivi obblighi a tutela della sicurezza del trattamento.

Le norme vincolanti di impresa (*Binding Corporate rules*), invece, si traducono in regolamenti interni, *policies* aziendali, codici di condotta, attività di audit o altre previsioni attraverso cui una società si obbliga, nell'effettuare il trasferimento verso le società infragruppo[21], al rispetto di un certo standard nel trattamento dei dati personali. Il contenuto minimo delle BCR prevede natura dei dati, scopi del trattamento, riferimenti alle società del gruppo stabilite all'interno e all'esterno dell'Ue, chiara descrizione degli standard di tutela e dell'organizzazione interna.

Infine si è fatto riferimento agli accordi internazionali specifici, tra cui il cosiddetto Codice di prenotazione (*Passenger Name Record*). I dati relativi ai codici di prenotazione sono raccolti dai vettori aerei durante il processo di prenotazione ed includono nomi, indirizzi, dati delle carte di credito e numeri di posto dei passeggeri. Ai

[20] Commissione UE, decisione 2010/87/EU, 5 febbraio 2010, relativa alle clausole contrattuali tipo per il trasferimento di dati personali ad incaricati del trattamento stabiliti in Paesi terzi.
[21] Le norme vincolanti d'impresa coinvolgono diverse autorità di controllo europee; affinché siano approvate, il progetto relativo alle BCR deve essere trasmesso all'autorità capofila che informa poi tutte le autorità di controllo dei Paesi membri in cui sono stabiliti gli affiliati del gruppo, sebbene la loro partecipazione al processo di valutazione delle BCR sia facoltativa.

sensi della Direttiva PNR, approvata nell'aprile 2016, che regola l'utilizzo dei dati PNR ai fini di gravi reati di natura transnazionale e terrorismo, le compagnie aeree sono obbligate a comunicare alle autorità i dati dei passeggeri provenienti da Paesi terzi verso l'Ue e viceversa[22]. I dati sono conservati per un periodo massimo di 5 anni e, in ogni caso, dopo sei mesi, devono essere anonimizzati e mascherati.

3. Cosa cambia con il nuovo Regolamento

Con il nuovo Regolamento (GDPR), già in vigore dal 24 maggio 2016, ma che sarà applicato a partire dal 25 maggio 2018, resta vietato il trasferimento di dati personali verso Paesi situati al di fuori dell'Ue o organizzazioni internazionali che non rispondano agli standard di adeguatezza in materia di protezione dei dati personali che, peraltro, diventano più stringenti.

L'art. 44 del GDPR, nel definire il trasferimento, introduce due novità: il riferimento a "trasferimenti successivi"[23] e l'estensione dell'ambito applicativo alle organizzazioni internazionali.

L'art. 45 riguarda il concetto di adeguatezza, ampliato e specificato alla luce della sentenza sul caso *Schrems.* Tale articolo si pone in linea di continuità con la Direttiva per quanto riguarda il trasferimento dei dati personali verso Paesi terzi o organizzazioni internazionali con un livello adeguato di protezione dei dati personali. A differenza del vecchio art. 26 della Direttiva, che prevedeva un parallelismo provvisorio di competenze tra Commissione e Stati membri in merito al sindacato sull'adeguatezza, pur lasciando alla Commissione l'ultima parola, nel nuovo art. 45 scompare ogni riferimento agli Stati membri. Per quanto concerne, invece, gli elementi da valutare nel giudizio di adeguatezza, la formulazione concisa e generica dell'art. 25 della Direttiva lascia il posto a quella più completa ed analitica dell'art. 45 del GDRP[24].

---

[22] Recentemente con il parere 1/15 del 26 luglio 2017 la CGUE ha ritenuto che l'accordo tra Canada e Ue sul trasferimento dei dati PNR è incompatibile con l'art. 16 TFUE e gli artt. 7,8 e 21 della Carta di Nizza, nonché con il criterio di proporzionalità di cui all'art. 52 par.1: l'ingerenza nel diritto fondamentale alla protezione dei dati personali non ha carattere necessario, in quanto varie disposizioni dell'accordo non sono limitate allo stretto necessario e non prevedono norme chiare e precise.

[23] Vale a dire trasferimenti ulteriori e secondari da un Paese terzo ad un altro Paese terzo, onde evitare che avvengano trasferimenti verso un Paese *compliant* e che da quest'ultimo venga eseguito un successivo trasferimento verso un Paese non *compliant*, allo scopo di eludere la normativa in materia di protezione dei dati personali

[24] Nel valutare l'adeguatezza del livello di protezione, la Commissione prende in considerazione: lo stato di diritto, il rispetto dei diritti umani e delle libertà fondamentali, la pertinente legislazione generale e settoriale, le norme in materia di protezione dei dati, la giurisprudenza, nonché i diritti effettivi e azionabili degli interessati ed un ricorso effettivo in sede amministrativa e giudiziaria per gli interessati i cui dati personali siano oggetto di trasferimento; l'esistenza ed effettivo funzionamento di una o più autorità di controllo indipendenti nel Paese terzo; gli impegni internazionali assunti dal Paese terzo o dall'organizzazione internazionale o altri obblighi derivanti da convenzioni o strumenti giuridicamente

Le decisioni di adeguatezza sinora adottate dalla Commissione (dal Privacy Shield alle clausole contrattuali tipo) e gli accordi internazionali in materia di trasferimento dati stipulati prima del 24 maggio 2016 dagli Stati membri restano in vigore fino a loro eventuale revisione o modifica.

Con il GDPR viene meno il requisito dell'autorizzazione nazionale: il trasferimento verso un Paese terzo adeguato ai sensi della decisione della Commissione, ovvero sulla base di clausole contrattuali tipo debitamente adottate, o di norma vincolanti d'impresa approvate attraverso la specifica procedura ex art. 47, potrà avere inizio senza attendere l'autorizzazione nazionale del Garante. Tuttavia, l'autorizzazione del Garante sarà ancora necessaria nel caso in cui il titolare decida di utilizzare clausole contrattuali *ad hoc* ed in caso di accordi amministrativi stipulati tra autorità pubbliche, novità questa introdotta dal GDRP.

Il nuovo art. 46, rubricato "trasferimento soggetto a garanzie adeguate" prevede ipotesi alternative ad una decisione di adeguatezza della Commissione e valide in ogni caso a condizione che gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi. Sotto la generica dicitura di "garanzie adeguate" sono ricondotte differenti fattispecie, ulteriori a quelle previste dalla Direttiva; il Regolamento, infatti, consente di ricorrere anche a codici di condotta o schemi di certificazione[25].

Dunque, come avviene già oggi, in mancanza di un riconoscimento di adeguatezza da parte della Commissione, i titolari potranno utilizzare per il trasferimento specifiche garanzie contrattuali; in assenza di garanzie contrattuali o riconoscimenti di adeguatezza, i flussi di dati al di fuori dell'Ue sono vietati, a meno che non vi sia il consenso esplicito dell'interessato o non ricorrano particolare condizioni ex art. 49, che ricalcano quelle già delineate dalla Direttiva[26].

Il GDPR vieta, inoltre, il trasferimento o la comunicazione di dati personali di un cittadino dell'Ue ad autorità giudiziarie o amministrative di Paesi terzi, a meno

vincolanti, come pure la loro partecipazione a sistemi multilaterali o regionali, in particolare il relazione alla protezione dei dati personali.

[25] L'adesione ad un codice di condotta approvato a norma dell'art. 40 oppure ad un meccanismo di certificazione approvato a norma dell'art. 42, unitamente all'impegno ad applicare le garanzie adeguate, assunto dal titolare o dal responsabile mediante uno specifico strumento contrattuale o altro strumento, che sia giuridicamente vincolante ed azionabile dagli interessati.

[26] Necessità per l'esecuzione o la conclusione di un contratto, difesa o esercizio di un diritto in sede giudiziaria, importanti motivi di interesse pubblico (ma deve trattarsi di un interesse pubblico riconosciuto dal diritto dello Stato membro del titolare che esporta i dati o dal diritto dell'Ue, dunque non può essere fatto valere l'interesse pubblico dello Stato terzo ricevente).

dell'esistenza di accordi internazionali di mutua assistenza giudiziaria o analoghi accordi fra Stati.

4. Dal caso Schrems al caso Microsoft Ireland

Con sentenza del 6 ottobre 2015[27] la CGUE ha dichiarato invalida la decisione n. 2000/520/CE[28] con cui la Commissione europea aveva accertato l'adeguatezza della protezione dei dati personali offerta dal *Safe Harbour* quale condizione per il trasferimento dei dati personali dall'Ue agli USA.

All'origine della vicenda vi è un ricorso presentato dal cittadino austriaco, Maximillian Schrems, innanzi all'autorità per la protezione dei dati personali irlandese. Il ricorrente lamentava che i dati personali forniti al *social network* Facebook, oggetto di trasferimento dalla filiale irlandese alla sede principale negli USA, fossero sottoposti ad attività di sorveglianza di massa condotte dal governo statunitense, alla luce delle dichiarazioni rese da Edward Snowden nel contesto del cd. *Datagate*.

Schrems chiedeva, pertanto, all'autorità irlandese di vietare il trasferimento dei propri dati personali verso gli Stati Uniti, ma l'autorità respingeva il ricorso ritenendo, da un lato, che non vi fosse prova che i dati personali del ricorrente fossero stati oggetto di accesso da parte delle autorità pubbliche statunitensi, dall'altro, che l'adeguatezza dei trasferimenti di dati verso gli USA era stata già determinata sulla base della Decisione n. 2000/520/CE. Schrems, allora, impugnava il provvedimento innanzi alla *High Court of Ireland*, la quale decideva di rimettere la questione alla CGUE.

La Corte di Giustizia ha chiarito che l'esistenza di una decisione della Commissione europea che dichiari il livello di adeguatezza di un Paese terzo ai fini del trasferimento di dati personali non può sopprimere o ridurre i poteri di cui dispongono le autorità di controllo in forza della Carta dei Diritti Fondamentali dell'Ue e dell'art. 28[29] della Direttiva 95/46/CE. Qui viene in rilievo anche l'art. 47 della Carta, ossia il diritto ad un ricorso effettivo innanzi ad un giudice imparziale e dunque il diritto ad un giusto processo.

[27] CGUE, *Maximillian Schrems c. Data Protection Commissioner*, C-362/14, 6 ottobre 2015.
[28] Tale decisione era stata adottata in conformità dell'art. 25 della Direttiva, il quale consente il trasferimento solo se il Paese terzo garantisce un livello di protezione adeguata, considerando la sua legislazione nazione o i suoi impegni internazionale e affidando alla Commissione la valutazione sull'adeguatezza.
[29] L'art. 28 attribuisce alle autorità per la protezione dei dati personali dei vari Stati membri ampi poteri investigativi e di intervento al fine di assicurare la corretta applicazione della Direttiva.

La Corte passa poi a verificare la validità della decisione osservando che la Commissione era tenuta a constatare che gli USA garantissero effettivamente, in considerazione della loro legislazione nazionale e degli impegni internazionali assunti, un livello di protezione dei diritti fondamentali sostanzialmente equivalente a quello garantito nell'Ue; tuttavia essa non ha proceduto ad una constatazione del genere, limitandosi ad esaminare il regime del cd. approdo sicuro.

Infine la Corte puntualizza che l'applicazione del *Safe Harbour* conosce dei limiti laddove siano prevalenti la sicurezza nazionale o l'interesse pubblico, ciò comportando possibili ingerenze delle autorità pubbliche americane nei diritti fondamentali delle persone, garantiti, in particolare, dagli articoli 7 e 8 della Carta di Nizza.

La decisione della Commissione 2000/520/CE risale al 26 luglio 2000, pochi mesi prima della proclamazione della Carta di Nizza, avvenuta il 7 dicembre 2000. L'entrata in vigore della Carta e il portato degli artt. 7 e 8 hanno influenzato notevolmente i recenti orientamenti giurisprudenziali della Corte che sembrano inclini a riconoscere una portata esclusiva ed ampia alla *privacy* e alla tutela dei dati personali[30]. È proprio la valorizzazione delle disposizioni della Carta che permette alla CGUE di elevare la valutazione generale sul livello di protezione offerto dalla Direttiva e lo *standard* di tolleranza per legittimare il trasferimento dei dati personali al di fuori dell'Ue, convertendo il parametro di adeguatezza, formalmente incardinato nell'art. 25, in quello della sostanziale equivalenza[31]. Emerge così una lettura espansiva che si era manifestata già in altre due pronunce che hanno ormai contribuito a definire lo statuto giurisprudenziale della *privacy* digitale: trattasi dei casi *Digital Rights Ireland*[32] e *Google Spain*[33].

In *Google Spain* la Corte riconosce espressamente che i diritti fondamentali derivanti dagli artt. 7 e 8 della Carta prevalgono, in linea di principio, sull'interesse economico. Nella sentenza *Schrems* si osserva che i trasferimenti di dati non possono aver luogo se non in presenza di un livello di protezione adeguato, dunque le ragioni del commercio non possono prevalere su quelle della *privacy*.

---

[30] Il recente orientamento giurisprudenziale della CGUE testimonia l'intento di costituzionalizzare i diritti di cui agli artt. 7 e 8 della Carta dei diritti fondamentali dell'Unione europea, rendendo la Corte un organo con poteri simili a quelli di una Corte costituzionale nell'ambito della data protection.

[31] "*La Carta dei Diritti Fondamentali dell'Unione europea nel reasoning dei giudici di Lussemburgo*", Oreste Pollicino e Marco Bassani.

[32] *Digital Rights Ireland Ltd. v. Minister of Communications Ireland and others*, causa C-293/12, sentenza della CGUE dell'8 aprile 2014.

[33] CGUE, C-131/12, *Google Spain v. Agencia Española de Protecciòn de Datos*, 13 maggio 2014.

Nel caso *Digital Rights Ireland*, la Corte ha dichiarato illegittima la Direttiva 2006/24/CE sulla *data retention*[34] per violazione non degli artt. 7 e 8, ma del criterio di proporzionalità stabilito dall'art. 52 par 1 della Carta di Nizza nel bilanciamento tra diritto alla protezione dei dati personali ed esigenze di pubblica sicurezza. Nella sentenza *Schrems* assistiamo ad un'argomentazione differente, in quanto, l'annullamento della Decisione 2000/520/CE è dovuto alla violazione dei diritti di cui agli artt. 7 e 8 addebitata non tanto alla Direttiva 95/46/CE, né alla Decisione stessa della Commissione, quanto piuttosto all'ordinamento statunitense[35].

Molti hanno considerato la sentenza del caso Schrems una risposta della Corte allo scandalo del *Datagate*. Le rivelazioni in merito alla sorveglianza di massa attuata dalla NSA hanno costituito, infatti, il più importante e drammatico episodio nell'ambito della regolamentazione transatlantica della protezione dei dati personali[36], creando un clima di *distrust* che ha avuto conseguenze rilevanti, prima fra tutte l'annullamento del *Safe Harbour* e la creazione del nuovo accordo *Privacy Shield*.

Il *Safe Harbour* era risultato da un compromesso economico e politico tra Ue e USA nel settore della *data protection*. Il valore assunto dai dati in tutti gli aspetti della vita economica ha reso impossibile per le imprese europee circoscrivere la loro operatività entro i confini dello spazio economico europeo; allo stesso modo era impensabile che, per non adempiere alle norme in materia di *data protection*, i *partners* commerciali delle imprese europee decidessero di rinunciare agli accordi negoziali posti in essere con esse, anzi hanno ritenuto vantaggioso adottare delle norme in materia di protezione dei dati personali conformi al modello comunitario, onde ridurre gli oneri in capo alle imprese locali in termini di adeguamento. In quest'ottica il *Safe Harbour* viene accolto favorevolmente da parte degli operatori economici sia europei che statunitensi, essendo ancora lontana una cultura diffusa della *data protection* come valore di impresa e fattore competitivo, prevalendo invece una lettura che ravvisa nella tutela dei dati una voce di merco costo.

La decisione della CGUE ha messo fine a tale compromesso, comportando conseguenze in particolare sui modelli di *business* degli operatori economici che nel breve

[34] In particolare, quelle disposizioni della Direttiva volte a garantire la conservazione di dati telefonici e telematici per fini di accertamento e repressione dei reati.
[35] O. POLLICINO – M. BASSINI, *La Carta dei Diritti Fondamentali dell'Unione europea nel reasoning dei giudici di Lussemburgo*, in *Diritto dell'informazione e dell'informatica*, XXXI, 2015.
[36] Cfr. F. BIGNAMI – G. RESTA, *Transatlantic privacy regulation: conflict and cooperation, 78 Law and Contemporary Problems*, 2015, 231-266.

periodo potranno riscontrare notevoli difficoltà di adeguamento, dovute al cambiamento delle logiche economiche in gioco.

Tuttavia, nel lungo periodo, l'investimento in tutela di dati sarà destinato a premiare le imprese e i maggiori oneri ed adempimenti si trasformeranno in vantaggio competitivo[37].

In particolare, negli USA, si sta assistendo ad una crescente domanda da parte dei consumatori circa l'innalzamento dei livelli di protezione dei dati personali, mentre, da parte delle imprese, vi è una richiesta di *standard* normativi maggiormente compatibili con quello europeo, tali da evitare uno svantaggio competitivo per le imprese statunitensi. In quest'ottica vanno lette le azioni intraprese da Microsoft[38] contro il governo americano a difesa dei dati contenuti sui propri *server* extraterritoriali, iniziativa che ha goduto dell'appoggio di molte imprese del settore ICT.

La questione riguardava la possibilità per le forze dell'ordine statunitensi di ordinare a provider statunitensi di esibire il contenuto di dati presenti in database del provider locati però al di fuori del territorio statunitense.

La vicenda giudiziaria è partita da una richiesta avanzata nel 2013 dal Dipartimento di Giustizia USA per ottenere dati depositati in un server di Microsoft situato in Irlanda e concernenti un utente indagato per traffico di droga. L'azienda si rifiutava di fornire al governo statunitensi dati non detenuti sul territorio nazionale, sostenendo che la rivelazione del contenuto delle mail dell'utente avrebbero minato la fiducia degli utenti nei servizi di *cloud computing* e avrebbe costituito un precedente pericoloso.

Si attende che la Corte Suprema degli USA decida se accogliere o respingere il ricorso del governo statunitense che lo oppone a Microsoft sulla validità del mandato richiedente dati locati in un contesto extraterritoriale. Recentemente ha dichiarato di intervenire anche la Commissione europea in veste di *amicus curiae*, considerando che il trasferimento di dati personali da Microsoft Irlanda agli USA ricade nell'ambito di operatività della normativa europea in materia di protezione dei dati personali; dunque

[37] A. MANTELERO, *I flussi di dati transfrontalieri e le scelte delle imprese tra Safe Harbour e Privacy Shield*, in AA.VV., *La protezione trasnazionale dei dati personali. Dai "Safe Harbour Principles" al "Privacy Shield"*, 2016, pp. 239-269.

[38] Si vedano a riguardo i documenti pubblicati dall'Electronic Frontier Foundation nella pagina dedicate al caso, consultabili al seguente indirizzo: *https:// www.eff.org/cases/re-warrant-microsoft-email-stored-dublin-ireland.* Cfr. anche Center for Democracy & Technology, *Microsoft Ireland Case: Can a US Warrant Compel A US Provider to Disclose Data Stored Abroad?*, 30 giugno 2014, *https://cdt.org/insight/ microsoft-ireland-case-can-a-us-warrant-compel-a-us-provider-to-disclose-data-stored- abroad/.*

è nell'interesse dell'Ue assicurarsi che la Corte Suprema prenda in dovuta considerazione tale circostanza, senza dimenticare poi che il nuovo Regolamento introdurrà regole ancora più stringenti che le società che si occupano di trasferimento dei dati personali di cittadini europei dovranno rigorosamente osservare.

IL PRINCIPIO DI ACCOUNTABILITY E LA SICUREZZA DEL TRATTAMENTO DEI DATI: UN FOCUS SULL'ANONIMIZZAZIONE E SULLE POTENZIALITÀ DELLA PSEUDONIMIZZAZIONE DEI DATI

di Lucrezia D'Avenia

SOMMARIO. 1. Premessa. 2. Pseudonimizzazione e anonimizzazione dei dati.pseudonimizzazione 3. La pseudonimizzazione nel GDPR. 4. Cenni sulle tecniche di anonimizzazione e pseudonimizzazione.

In a guaranteed key, the new European standard emphasizes the proactive role of the data controller (controller) and the processor (processor) rather than the data subject. This approach is embodied in the principle of accountability, referring to both the controller and the processor, whose translation could be "responsibility with the obligation to report on its own work". This principle becomes a pillar of the GDPR, as it represents a real qualitative leap from a formal conception of fulfillment of pre-established legal rules to a substantial protection of data, which requires the adoption of effective security measures that the owner himself identifies based on a preventive risk analysis of the individual treatment.

1. Premessa

Nella società digitale, con lo sviluppo dell'*Information Comunication Tecnology,* dominata dalle comunicazioni elettroniche, il diritto alla protezione dei dati, inteso come tutela delle informazioni personali, rappresenta una fondamentale garanzia di libertà.

La materia *data protection* risulta, quindi, al giorno d'oggi, un tema di grande attualità, in relazione al quale *"l'Europa vanta uno dei sistemi più all'avanguardia"*[39].

Già nel 1981, infatti, in ambito regionale europeo, il Consiglio d'Europa ha adottato uno strumento giuridico, la Convenzione n. 108, con lo scopo dichiarato di tutelare

[39] Sul punto la premessa del *Manuale sul diritto europeo in materia di protezione dei dati* elaborato nel 2014 da *European Union Agency for fundamental rights*, Corte EDU e Consiglio d'Europa.

il diritto al rispetto della vita privata, previsto dall'art. 8 CEDU (*Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali*), nei casi di trattamenti automatizzati dei dati personali.

In ambito comunitario, invece, la problematica in oggetto inizia ad essere avvertita dopo il Trattato Maastricht, quando per realizzare il Mercato Unico e l'abbattimento delle frontiere previsto dall'accordo di Schengen, si è resa fondamentale l'armonizzazione delle discipline nazionali degli Stati membri in materia di circolazione dei dati personali connessi agli scambi.

A tal fine, a seguito di trattative lunghe e difficili, è stata adottata la Direttiva 95/47/CE (cd. *Direttiva Madre*). Trattandosi di uno strumento di armonizzazione con la stessa sono stati imposti alcuni principi generali in materia di *data protection*, cui gli Stati Membri hanno dovuto adeguare la propria legislazione nazionale. Da un punto di vista giuridico, quindi, il più grande risultato raggiunto dall'atto comunitario in oggetto è stato quello di creare una netta separazione tra Europa e Paesi Terzi; in altre parole, le garanzie previste dalla Direttiva, sono diventate un muro insormontabile per i rapporti con quei paesi, come gli Stati Uniti, che non ne assicurano il rispetto.

Il quadro di tutela appena delineato si è ulteriormente rafforzato nel 2000 con l'adozione della Carta europea dei diritti fondamentali (cd. *Carta di Nizza*) che all'art. 8 riconosce ufficialmente il rango primario del diritto alla protezione dei dati di carattere personale, per poi completarsi nel 2009 con l'adozione del Trattato di Lisbona che, da un lato, riconosce valore giuridico di Trattato alla predetta Carta e, dall'altro, con l'art. 16 del TFUE (*Trattato sul funzionamento dell'Unione Europea*) proclama finalmente l'autonomia del diritto fondamentale alla protezione dati.

Questo riconoscimento formale ha avuto un impatto determinante nell'elaborazione del nuovo Regolamento 2016/679 *"sulla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati"* (identificato con l'acronimo *GDPR*: Regolamento generale sulla protezione dei dati) destinato ad abrogare e sostituire la Direttiva Madre, in quanto il presupposto che, come diritto fondamentale, la protezione dati non riguardi solo il singolo/ diretto interessato ma l'intera società ha consentito un mutamento sostanziale di prospettiva.

In una chiave garantista, infatti, la nuova norma europea pone l'accento sul ruolo proattivo del titolare del trattamento (*controller)* e del responsabile (*processor*) del trattamento piuttosto che sull'interessato (*data subject*).

Tale approccio si sostanzia nel principio di *accountability,* riferito sia al controller che al processor, la cui traduzione potrebbe essere *"responsabilizzazione con l'obbligo di rendicontazione del proprio operato".* Questo principio assurge a pilastro del GDPR, in quanto rappresenta un vero salto di qualità da una concezione formale di adempimento di regole giuridiche prestabilite ad una sostanziale tutela dei dati, che impone l'adozione di misure di sicurezza effettive che è il titolare stesso ad individuare sulla base di un'analisi preventiva dei rischi del singolo trattamento.

Si tratta dunque di un approccio *risk based* che, da un lato, ha il vantaggio di risultare più flessibile in quanto è rimesso alle valutazioni autonome dei titolari, si adatta allo stato della tecnologia e si commisura alla dimensione e all'organizzazione dell'azienda, ma dall'altro risulta gravoso per gli operatori in quanto richiede a titolari e responsabili del trattamento un impegno costante e multidisciplinare connesso a responsabilità e sanzioni.

Alla luce di quanto sin ora argomentato, appare evidente che con il Regolamento anche la sicurezza diventa un principio, *rectius*, un presupposto di ogni trattamento, con la conseguenza che le misure adottate per garantirla assumono un'importanza fondamentale ai fini di garantire il rispetto della normativa europea.

Tra le misure di sicurezza che trovano nel GDPR un riconoscimento giuridico formale pur essendo già utilizzate nella prassi, vi è la pseudonimizzazione (*pseudonymization*), tecnica relativa al trattamento dei dati personali che, con il tempo, si è dimostrata in grado di offrire una tutela *"tecnologica",* oltre che giuridica, dei dati personali.

A parere di chi scrive, infatti, alla luce del quadro di tutela rafforzato delineato dal nuovo Regolamento questa misura di sicurezza, che secondo recenti studi[40] è ancora poco compresa e valorizzata dalle aziende europee, assumerà un ruolo decisivo non solo per evitare le pesanti sanzioni previste dalla nuova normativa europea, ma

[40] Delphix è un'azienda fondata nel 2008 da Jedidiah Yueh che opera nel settore della virtualizzazione dei dati con un metodo innovativo che consente, tramite un software, di creare una sola copia virtualizzata dei dati, mascherando anche i dati sensibili. Nel luglio 2016 la società ha pubblicato i risultati di uno studio (la cui metodologia non è stata però resa nota), eseguito in Regno Unito, Germania, Francia e Italia volto a verificare se le aziende europee fossero a conoscenza dell'imminente introduzione da parte dell'UE del Regolamento per la Protezione dei Dati Personali. Fra gli Stati considerati, la Francia è quello meglio posizionato, vantando un 38% di rispondenti che dichiarano di avere "compreso perfettamente" il principio della pseudonimizzazione e le relative procedure implicate. Sia nel Regno Unito sia in Germania la quota di chi ritiene di avere le idee chiare scende al 21%, mentre per l'Italia non è stata realizzata una quantificazione percentuale ma Delphix ha parlato di una situazione "preoccupante" di scarsa comprensione e consapevolezza su questo principio al centro del Gdpr.

anche per migliorare le tecniche di raccolta e analisi dei dati, rafforzando così la fiducia del pubblico nel brand[41].

2. Pseudonimizzazione e anonimizzazione dei dati.

Per comprendere le ragioni di tale convinzione occorre in via preliminare fare chiarezza sul significato della pseudonimizzazione e la differenza relativa all'anonimizzazione dei dati.

La definizione unanimemente accolta di dato personale pone l'accento sulla circostanza che l'informazione sia riferibile ad una persona fisica identificata o identificabile. L'identificabilità dell'interessato è dunque un elemento essenziale affinchè si possa accedere alla tutela prevista dalle disposizioni vigenti in materia di *data protection* e costituisce la sostanziale differenza tra le due tecniche in esame.

Diversamente da quanto fino ad oggi ritenuto da (ahimè) molti responsabili, infatti, solo l'anonimizzazione (*anonymization*) garantisce la spersonalizzazione del dato e quindi una *"identificazione ragionevolmente impossibile"* dell'interessato, che va intesa anche in termini di correlabilità, deduzione ed individuazione[42].

Si tratta di un trattamento successivo del dato personale con un alto valore potenziale, in quanto consente il riutilizzo dei dati in deroga ai principi di finalità, consenso e conservazione.

In altre parole, laddove il titolare voglia conservare il dato oltre il necessario, operando un trattamento per una finalità diversa da quella per la quale lo stesso era stato raccolto, e non disponga del consenso dell'interessato o di una base giuridica (atto o norma) legittimante, dovrà rendere il dato personale anonimo, eliminando gli elementi identificativi che potrebbero far risalire all'identità della persona fisica.

In tal modo, quindi, i dati cd. *"aperti"* possono essere sfruttati a vantaggio della società, attenuando il rischio di lesione dei diritti degli interessati, al punto da giustificare l'inapplicabilità della normativa di *data protection*[43] .

---

[41] Cfr. sul punto una recente intervista a Mauro Trione, Vice President Sales Southern EMEA di Delphix, resa in occasione della pubblicazione dello studio citato sub 2 di cui è disponibile un estratto sul sito *http://www.cwi.it/attualita/norme-e-regolamenti/le-aziende-europee-pronte-la-pseudonimizzazione-92631*.

[42] L'espressione citata è stata estrapolata dal parere 5/2014 sulle tecniche di anonimizzazione del WP article 29 di cui si dirà nel prosieguo del testo. Sempre da tale fonte si ricavano le seguenti definizioni: correlabilità: possibilità di correlare almeno due dati sulla stessa persona o gruppo; deduzione: possibilità di desumere con elevata probabilità il valore di un attributo dai valori di un insieme di attributi; individuazione: Possibilità di isolare dei dati che identificano una persona in un insieme.

[43] cfr. sul punto art. 11 del Regolamento rubricato *"Trattamento che non richiede l'identificazione"*.

Le tecniche utilizzate sono molteplici (aggiunta di rumore statistico, permutazioni, privacy differenziale, aggregazione etc.) e si differenziano in due tipologie di approcci: la randomizzazione che consiste nel *"falsificare"* il dato eliminando la correlazione tra lo stesso e la persona (riferendolo ad esempio ad un interessato diverso) e la generalizzazione che consiste nel diluire gli attributi dei dati modificandone la scala o l'ordine di grandezza, cosicchè diventino potenzialmente riferibili ad una pluralità di interessati (ad esempio l'attributo identificativo riferito ad una città viene riferito ad una regione o una nazione).

Nonostante le tecniche di anonimizzazione siano già da tempo oggetto di studio e si siano notevolmente evolute con lo sviluppo della tecnologia informatica, ad oggi non esiste alcuna procedura che si sia dimostrata in grado di eliminare completamente il fattore di rischio di reidentificazione degli interessati. Il *Working Party article 29*[44] si è soffermato più volte sul tema e, nel parere 5/2014 (adottato il 10.04.2014), ha operato un'attenta analisi di ciascuna delle tecniche di anonimizzazione più diffuse nella prassi, per valutarne l'efficacia sulla base di tre criteri molto semplici: 1) è ancora possibile individuare una persona; 2) è ancora possibile collegare i dati ad una persona; 3) è possibile desumere informazioni su una persona. Il risultato cui si è giunti è che, come anticipato, nessuna procedura è in grado di garantire una risposta assolutamente negativa a tutti e tre i quesiti e che, dunque, allo stato attuale delle tecnologie, non esistono dati realmente anonimi, ma piuttosto dati resi sufficientemente anonimi da giustificare l'inapplicabilità del Regolamento al singolo trattamento specifico.

Da ciò si ricava la necessità che le procedure di anonimizzazione siano progettate in relazione al contesto ed agli obiettivi del trattamento, combinando diverse tecniche in base alle esigenze del caso ed effettuando periodici riesami al fine di attualizzare la procedura alle nuove tecnologie.

Questo risultato è stato di certo tenuto in debito conto dal Legislatore europeo e racchiuso dallo stesso nel considerando 26 del Regolamento nel quale si chiarisce che, per stimare l'identificabilità e, dunque, l'efficacia di una tecnica di anonimizzazione, occorre valutare la ragionevole probabilità che un terzo riesca ad individuare la persona, utilizzando le tecnologie disponibili, ed in rapporto ai costi e i tempi all'uopo necessari.

[44] Il Working Party Article 29 è un gruppo di lavoro formato da rappresentanti delle autorità garanti nazionali cui la Direttiva 95/46/CE ha attribuito il compito di formulare pareri, linee guida e documenti di indirizzo per una corretta attuazione delle norme dalla stessa previste ed il cui ruolo è risultato sino ad oggi determinante al fine di guidare nella pratica gli operatori giuridici del settore.

3. La pseudonimizzazione nel GDPR.

Alla luce di quanto sin qui argomentato, posto che sebbene sia preferibile, in un'ottica di protezione, raggiungere le finalità utilizzando dati anonimi, ciò non è sempre possibile in rapporto alla specifica finalità del singolo trattamento, tanto più quando, come accade di frequente, la raccolta di dati risponde a finalità molteplici ed eterogenee. In tali casi occorre, pertanto, avvalersi di altri strumenti che rendano quantomeno più faticoso risalire all'identità degli interessati.

Tra questi non può passare inosservata la considerazione del tutto nuova, rispetto alla precedente Direttiva, che il GDPR riserva alla pseudonimizzazione, che consiste nel mascheramento del dato mediante uno pseudonimo. In tal modo il dato resta identificabile, ma in via indiretta, e, quindi, con più difficoltà, a meno che non si possiedano delle informazioni aggiuntive che, fungendo da chiave di decifratura, devono essere conservate separatamente ai dati e protette con misure tecniche ed organizzative adeguate[45].

Nel settore della ricerca, ed in particolare di quella medica che coinvolge sempre il trattamento di dati sensibili, l'utilizzo di elementi identificativi mascherati o crittografati appare imprescindibile per ottenere le informazioni necessarie al raggiungimento delle finalità, tutelando il supremo diritto alla protezione della vita privata, già in fase di progettazione del trattamento. Restando in ambito sanitario, ad esempio, accade spesso che le strutture, titolari delle informazioni personali dei pazienti in quanto necessarie al raggiungimento delle proprie finalità istituzionali di cura, forniscano ai ricercatori dati sanitari già pseudonimizzati. Ciò in quanto, il più delle volte, ai fini della ricerca scientifica, non è necessario conoscere l'identità della persona fisica, essendo piuttosto sufficiente sapere che le informazioni riguardano uno stesso interessato, ovvero accedere a singoli attributi specifici dello stesso (e.g. età, peso, marker biologici).

La pseudonimizzazione costituisce, quindi, un valido presidio tecnologico per i diritti fondamentali, consentendo di operare un bilanciamento di tutti gli interessi coinvolti nei singoli trattamenti.

4. Cenni sulle tecniche di anonimizzazione e pseudonimizzazione.

[45] Cfr. articolo 4 (*definizioni*) punto 5 GDPR: "pseudonimizzazione": il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona identificata o identificabile.

Le tecniche più utilizzate sono il mascheramento, la crittografia con chiave segreta e l'utilizzo della funzione di hash che possono essere, peraltro, combinate tra loro per ottenere un risultato più efficace, come avviene ad esempio nel cd. hash cifrato[46].

La maschera dati dinamica (DDM) limita l'esposizione dei dati personali, nascondendoli agli utenti non autorizzati al trattamento; in questo modo tale tecnica impedisce l'accesso da parte di terzi ai dati personali, ed in particolare ai dati sensibili, senza modificarli nel database.

Ad esempio, ponendo il caso di un codice fiscale, è possibile creare una maschera che nasconda al pubblico, nel set dei risultati, tutte le cifre ad eccezione delle ultime quattro.

La crittografia è, invece, una tecnica di rappresentazione dell'informazione in una forma tale che la stessa possa essere recepita solo dal destinatario. A tal fine il dato personale viene sottoposto a trasformazioni, utilizzando un sistema di simboli che lo renda incomprensibile, fungendo da chiave segreta. In questo modo solo chi conosce la chiave può decifrare lo pseudonimo, risalendo all'identità dell'interessato.

La funzione di hash è una funzione iniettiva non invertibile in grado di trasformare un'immissione di dati (ad esempio un nome come Mario Rossi) in una emissione di dati di dimensione fissa, generata casualmente e composta di lettere e numeri (Mario Rossi diventerà ad esempio a5887a62d652d2b476e57f20bbbc8c2c).

Dalla combinazione delle ultime due tecniche descritte se ne ricava una terza denominata funzione di hash cifrato con cancellazione della chiave che, secondo il già citato studio del Gruppo di Lavoro art. 29[47], si è dimostrata particolarmente efficace, essendo in grado di ridurre sensibilmente il rischio di correlabilità.

Questa tecnica consiste nella selezione, mediante una funzione di hash caratterizzata dall'aggiunta di una chiave segreta, di un numero casuale quale pseudonimo di ciascun attributo contenuto nell'insieme di dati, seguita poi dalla cancellazione della chiave. In tal modo, non essendo disponibile l'elemento necessario a decifrare una parte della funzione, un intruso ha notevoli difficoltà per decifrare la stessa e risalire così all'identità dell'interessato.

A differenza dell'anonimizzazione, quindi, la pseudonimizzazione è un processo reversibile, sicchè anche i dati pseudonimizzati devono essere considerati personali e,

[46] Funzione di *hash* che utilizza una chiave segreta quale immissione aggiuntiva.
[47] cfr. sul punto il già citato parere n. 5/2014 del 10.04.2014.

in quanto tali, soggetti alla disciplina del Regolamento e delle altre normative di *data protection*.

I dati pseudonimizzati non sono esplicitamente menzionati nelle definizioni giuridiche contenute nella Convenzione n.108 del 1981 o nella Direttiva 95/46/CE anche se, nella relazione esplicativa del primo strumento giuridico citato, vi è un riferimento relativo al principio di conservazione, ove si precisa che *"dopo qualche tempo [...] non dovrebbe essere possibile collegare facilmente i dati e gli elementi identificativi"*[48].

Il Regolamento 2016/679, invece, come anticipato, non solo all'art. 4 n. 5 fornisce finalmente una definizione univoca di questa particolare modalità di trattamento, ma menziona più volte la pseudonimizzazione, sia nei considerando che in numerose disposizioni, tra le quali l'art. 6 (*liceità del trattamento*) l'art. 25 (*protezione dei dati fin dalla progettazione e protezione per impostazione predefinita*) nonché diversi articoli del Capo IV.

In particolare, la lettura dell'art. 32 (*sicurezza dei trattamenti*) in combinato con il considerando 83 consente di comprendere l'importanza potenziale della pseudonimizzazione, allorquando si afferma che la stessa costituisce la prima misura tecnico organizzativa di cui tener conto al fine di valutare se per un determinato trattamento il titolare e/o il responsabile garantiscono un livello di sicurezza adeguato al rischio di ledere i diritti e le libertà degli interessati.

Significativo in tal senso è anche il successivo art. 34 (*comunicazione di una violazione dei dati personali all'interessato*) che impone la comunicazione agli interessati degli eventi di cd. *data breach* (*violazioni dei dati personali*) e prevede, tra le deroghe a tale obbligo, proprio l'adozione di misure di sicurezza idonee a rendere l'identità degli interessati incomprensibile ai terzi.

L'art. 6, invece, per quanto ivi interessa, dopo aver enumerato le condizioni di liceità dei trattamenti, individua al punto 4 una clausola di salvaguardia, presumibilmente rivolta al trattamento dei big data, stabilendo che nel caso in cui il titolare, raccolti i dati personali, intenda poi trattarli per una finalità diversa da quella originaria e non abbia a disposizione il consenso dell'interessato ovvero una norma giuridica legit-

[48] Art 42: l'obbligo relativo ai termini per la conservazione dei dati in forma nominativa non significa che i dati debbano essere dopo qualche tempo irrevocabilmente separati dal nome della persona cui si riferiscono, ma soltanto che non dovrebbe essere possibile collegare facilmente i dati e gli elementi identificativi.

timante, dovrà valutare che questa ulteriore finalità sia compatibile con la prima, tenendo conto, tra l'altro, *"dell'esistenza di misure adeguate che possono comprendere la cifratura e la pseudonimizzazione".*

Quanto, infine, all'art. 25, nello stesso si trovano codificati i principi di *data protection by default and by design* che impongono al titolare, tenuto conto delle conoscenze tecniche disponibili, dei relativi costi e delle caratteristiche specifiche del trattamento, di adottare misure adeguate al fine di tutelare i diritti degli interessati, *"quali la pseudonimizzazione"*, già in fase di progettazione del trattamento e come impostazione predefinita dello stesso.

Tutto quanto argomentato consente di affermare che la pseudonimizzazione vada intesa come una misura di sicurezza di grande rilievo pratico di cui i titolari ed i responsabili possono avvalersi per limitare i rischi connessi ai trattamenti nel rispetto del principio di accountability che come già argomentato permea l'intero strumento giuridico[49].

Ciò non significa sicuramente che la pseudonimizzazione possa rappresentare di per sé una misura di sicurezza sufficiente. Già nel parere 6/2013 (relativo ai dati aperti e al riutilizzo delle informazioni del settore pubblico) seppure in relazione ai dati anonimizzati, il Gruppo di Lavoro art. 29 aveva evidenziato l'esigenza di affrontare il rischio di re identificazione, attraverso l'utilizzo di test di penetrazione effettuati periodicamente al fine di rilevare le vulnerabilità delle procedure utilizzate in relazione all'evoluzione degli strumenti tecnologici disponibili.

Un suggerimento dello stesso tipo, in rapporto stavolta proprio alla pseudonimizzazione, si rinviene, inoltre, anche nell'art 32 del Regolamento ove, tra le misure *"adeguate"* a garantire un livello di sicurezza rapportato al rischio preventivato, si consiglia (alla lettera d) l'adozione di *"una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche ed organizzative al fine di garantire la sicurezza del trattamento".*

Oltre all'utilizzo dei *penetration tests* generalmente intesi, anche l'adesione ai codici di condotta di cui all'art. 40 o ai meccanismi di certificazione di cui al successivo art. 42 potrà essere utilizzata dai titolari e dai responsabili per dimostrare la conformità

[49] Considerando 28: l'applicazione della pseudonimizzazione ai dati personali può ridurre i rischi per gli interessati e aiutare i titolari del trattamento e i responsabili del trattamento a rispettare i loro obblighi di protezione dei dati. L'introduzione esplicita della pseudonimizzazione nel presente regolamento non è quindi intesa a precludere altre misure di protezione dei dati.

delle misure di sicurezza (tra le quali la pseudonimizzazione) agli *standards* imposti dal regolamento.

In conclusione, alla luce di tutto quanto sin qui esposto, a parere di chi scrive, la pseudonimizzazione, opportunamente coniugata, nel caso di contesti innovativi, con i principi di *privacy by design*, è destinata a diventare una prassi consueta quasi imposta dal principio di accountability.

Se è vero, infatti, che i dati pseudonimizzati sono sottoposti all'applicazione del GDPR, è pur vero che le regole dallo stesso previste (come innanzi esposto ad esempio in relazione all'obbligo di comunicazione in caso di *data breach*), essendo flessibili e proporzionali al rischio, saranno più permissive in relazione a dati pseudonimizzati, rispetto a quelle che riguardano i dati direttamente riconducibili a una persona.

L'adozione e lo sviluppo da parte delle aziende delle tecniche di pseudonimizzazione per proteggere i dati, inoltre, rappresenta un investimento in grado di favorire la disponibilità di dati sicuri e dunque l'opportunità di migliorare i processi IT e aziendali, oltre che di ridurre il rischio di violazioni, con un evidente vantaggio anche sotto il profilo di incrementare il rapporto fiducia da parte dei cittadini o dei consumatori.

LA TUTELA DELLA PROPRIETÀ INTELLETTUALE E GLI INTERNET SERVICE PROVIDER

di Giulio Riccio

SOMMARIO. 1. Premessa. 2. La responsabilità per violazione dei diritti di proprietà intellettuale. 3. Le "opere digitali" e gli Internet Service Provider (ISP). 4. Conclusioni

With the birth and the rise of the digital world, new forms of fruition of works and contents developed as the new possibilities to establish unlawful conducts against the intellectual property rights of the owners of the works themselves. In this scenario, it was (and it will be) necessary to create new tools for the online protection of the intellectual property rights.

1. Premessa.

Internet è un'entità che si è evoluta in maniera rapida e continua nel corso degli anni grazie alle nuove tecnologie: mentre agli albori della c.d. Società dell'Informazione[5051] i computer erano connessi in rete in maniera "point to point", con l'avvento del Web[52] si è giunti ad una rete di informazioni in grado di veicolare istantaneamente dati su scala mondiale[53].

In tale scenario il numero di soggetti la cui attività – consapevole o meno – è in grado di violare i diritti di proprietà intellettuale su opere digitali e/o digitalizzate è cresciuto in maniera esponenziale così come il numero dei mezzi di condivisione a disposizione degli utenti della Rete[54].

---

[50] S. CRAWFORD, *The Origin and Development of a Concept: The Information Society*, 1983, *Bull. Med. Libr. Assoc*, 71(4) October, 380.

[51] La società moderna è spesso denominata "Società dell'Informazione" in quanto caratterizzata da tecnologie in grado di elaborare dati e scambiare informazioni in ogni momento da un capo all'altro del globo e ad altissima velocità.

[52] Il termine *web* significa letteralmente "ragnatela globale" ed oggi costituisce il principale strumento di informazione. È stato concepito alla fine degli anni '80 dall'informatico inglese Tim Berners-Lee come mezzo di condivisione dei documenti all'interno degli uffici del CERN di Ginevra, presso cui lavorava. In poco meno di un decennio, dopo essere stata resa pubblica, il Web è diventato un mezzo di informazione e conoscenza che ha integrato e talvolta soppiantato quelli tradizionali.

[53] M. HARDT, A. NEGRI, *Multitude: War and Democracy in the Age of the Empire*, New York: Hamish Hamilton, 2005, 108.

[54] Ai sensi dell'art. 1, lett. p), Regolamento Agcom, si parla di "opere digitali" in presenza di «u*n'opera, o parti di essa, di carattere sonoro, audiovisivo fotografico, videoludico, editoriale e letterario, inclusi*

È stata avvertita, pertanto, la necessità di aggiornare gli strumenti di controllo e repressione delle violazioni dei predetti diritti in Internet che, negli ultimi anni, se da un lato ha favorito la circolazione di idee e conoscenza, ha dall'altro contribuito in maniera allarmante alla contrazione dei proventi derivanti dall'attività di sfruttamento delle opere protette, oltre che ad un approccio privo della necessaria educazione a temi come la nascita e la lecita fruizione delle stesse.

2. La responsabilità per violazione dei diritti di proprietà intellettuale

2.1 Forme di responsabilità "classiche" previste dalla Legge sul diritto d'autore

La legge 22 aprile 1941, n. 633, sulla protezione del diritto d'autore e di altri diritti connessi al suo esercizio, contiene al capo III le «Difese e sanzioni giudiziarie», ovvero le modalità di protezione del diritto d'autore in ambito civile e penale (che possono definirsi "classiche"). Tale capo si articola in due sezioni: sezione I «Difese e sanzioni civili», sezione II «Difese e sanzioni penali»; gli strumenti di tutela ivi previsti sono stati oggetto di aggiornamento da parte del legislatore nazionale al fine di adeguarne il contenuto e la portata alle direttive europee successivamente emanate oltre che ai nuovi pericoli per la tutela della proprietà intellettuale online.

L'art. 156 LdA, che apre la prima delle due sezioni, prevede il rimedio del ricorso giudiziale per la richiesta dell'accertamento del diritto d'autore ovvero dell'interdizione a seguito di un'accertata violazione; tale disposizione precisa, inoltre, che l'azione civile è regolata dalle norme contenute nella stessa sezione e da quelle contenute nel codice di procedura civile.

I seguenti articoli regolano condizioni, forme e casi di istanza al giudice e i relativi poteri, con particolare attenzione ai casi di urgenza e pericolo nel ritardo.

La sezione II, invece, contiene disposizioni di diritto penale ed è aperta dall'art. 171 che prevede la multa per colui che «senza averne diritto, a qualsiasi scopo e in qualsiasi forma» diffonde un'opera altrui; la lettera a-*bis*[55]si riferisce, in particolare, ai casi in cui un'opera dell'ingegno protetta (o parte di essa) sia messa a disposizione del pubblico «immettendola in un sistema di reti telematiche, mediante connessioni di qualsiasi genere», prevedendo che il reo sia «ammesso a pagare, prima dell'apertura

i programmi applicativi e i sistemi operativi per elaboratore, tutelata dalla Legge sul diritto d'autore e diffusa su reti di comunicazione elettronica».

[55] Disposizione introdotta con legge 31 marzo 2005, n. 43.

del dibattimento, ovvero prima dell'emissione del decreto penale di condanna, una determinata somma di denaro e che tale pagamento estingua il reato.

L'art. 171-*bis* contempla le pene relative alle attività di duplicazione di programmi per elaboratore (software) ovvero importazione, distribuzione, vendita, detenzione a scopo commerciale o imprenditoriale, concessione in locazione di programmi contenuti in supporti non contrassegnati dalla SIAE oltre alle attività di riproduzione, trasferimento, distribuzione, comunicazione, presentazione o dimostrazione in pubblico, attraverso supporti non contrassegnati SIAE, del contenuto di una banca dati, ovvero l'estrazione, il reimpiego, la distribuzione, la vendita e la concessione in locazione di una banca dati.

La condizione per l'applicabilità delle sanzioni previste dall'art. 171-*bis* è che le condotte previste siano poste in essere al fine di trarre un illecito profitto mentre il successivo art. 171-*ter* individua i casi in cui sono previste le pene della multa e della reclusione, operando una classificazione in categorie di gravità diversa. I successivi articoli prevedono i casi di sequestro, distruzione e confisca del materiale, degli strumenti e dei supporti coinvolti nell'illecito.

Un regime di parziale esenzione dalla pena è previsto dall'art. 171-*nonies* secondo cui, nei casi di denuncia spontanea della violazione all'Autorità giudiziaria o di individuazione del promotore o organizzatore dell'attività illecita ovvero di sequestro di una notevole quantità di supporti e strumenti serviti o destinati alla commissione di reati, le pene previste dai precedenti articoli sono ridotte e le pene accessorie non sono applicate se la denuncia avviene prima che la violazione sia stata specificamente contestata.

Tali numerose disposizioni, dunque, hanno lo scopo di tipizzare il numero più alto possibile di condotte perpetrabili e, come anticipato, prevedono gli strumenti "classici" di tutela dei diritti di proprietà intellettuale sulle opere da parte dei legittimi titolari.

Come può immaginarsi, molteplici sono state le modifiche e gli aggiornamenti nel corso dei decenni apportati alla Legge sul diritto d'autore, risalente ad ormai quasi ottant'anni fa; i riferimenti alle reti telematiche contenuti nelle predette disposizioni della LdA sono il risultato proprio di tali successivi interventi.

Il riferimento alle reti telematiche crea un collegamento diretto con i più recenti strumenti di repressione di illeciti previsti dal nostro ordinamento giuridico, su impulso

dell'Unione europea, come la possibilità di intervento dell'Autorità garante per le comunicazioni (Agcom) azionabile dal soggetto che lamenta una violazione dei propri diritti d'autore online.

2.2 Internet e le "nuove" forme di responsabilità. Il Regolamento Agcom

Con l'evoluzione di Internet, i tradizionali sistemi di tutela sono andati incontro a modifiche ed aggiornamenti per favorire l'adeguamento ai nuovi canali di comunicazione e di condivisione, assecondando «l'esigenza di adeguare le disposizioni normative al rapido progredire delle tecniche di riproduzione, comunicazione, messa a disposizione e distribuzione delle opere protette dal diritto d'autore e degli altri materiali cui si riferiscono i diritti connessi. Nella "Società dell'Informazione", la globalizzazione e la dematerializzazione dello sfruttamento di opere e materiali tutelati pongono alla legislazione nuove sfide, che debbono essere raccolte a livello internazionale»[56].

Legislatore e dottrina sono stati entrambi impegnati, dunque, l'uno modificando le disposizioni esistenti, l'altra interpretando le disposizioni contenute nella Legge sul diritto d'autore in maniera tale da far ricadere nel campo di applicazione delle norme i nuovi tipi di illeciti perpetrabili in Internet.

Alla luce dell'impatto delle nuove tecnologie sulla tradizionale concezione del diritto d'autore e dei diritti ad esso connessi, tangibile nella potenzialità, velocità, portata ed innovatività delle nuove modalità di condivisione dei contenuti (tra cui, in materia di diritto d'autore, emergono le opere dell'ingegno implicate nel fenomeno di "digitalizzazione"[57], ovvero le opere digitali) è stato necessario considerare nuovi strumenti e nuovi soggetti nei meccanismi tesi alla tutela dei predetti diritti.

Tra i rimedi messi a disposizione dei titolari dei diritti di proprietà intellettuale su opere digitali e/o digitalizzate è da annoverarsi quello di tipo amministrativo previsto dal Regolamento Agcom di cui all'allegato A della delibera n. 680/13/CONS del 12 dicembre 2013[58].

Tale Regolamento contiene misure di natura diversa rispetto ai provvedimenti emanabili al termine dei procedimenti dinanzi l'Autorità giudiziaria ordinaria ed il

[56] Direttiva 2001/29/CE, 5° considerando.
[57] Con tale termine si fa riferimento alle opere materiali tradizionalmente oggetto di protezione dei diritti di proprietà intellettuale a cui si affiancano nuove tipologie di opere che nascono già completamente dematerializzate.
[58] Consultabile all'URL *https://ddaonline.agcom.it/AllegatoA.html.*

procedimento paragiurisdizionale ivi previsto risulta caratterizzato da celerità ed immediatezza, peculiarità fondamentali per assicurare l'effettività del provvedimento amministrativo emanato a tutela del diritto d'autore online.

Esaminate le sanzioni previste per le tipologie di illecito tradizionalmente prese in considerazione dal legislatore, occorre, quindi, concentrare l'attenzione sulle violazioni perpetrabili a mezzo Internet su cui l'Autorità amministrativa è competente ai sensi dell'art. 2 del predetto Regolamento.

«Il diritto d'autore ed i diritti connessi in Internet tutelano anzitutto le opere dell'ingegno tradizionali rispetto alla loro utilizzazione in formato digitale ed alla loro circolazione in questo specifico ambito. Anche il regolamento Agcom si prefigge di tutelare opere […] rispetto ad un loro uso in formato digitale ovvero, secondo una terminologia creata *ad hoc* dall'autorità, le cosiddette opere "digitali"»[59].

Il peculiare procedimento previsto per la tutela del diritto d'autore online dinanzi l'Agcom, dunque, si avvia con un'istanza da parte del soggetto che ritiene lesi i propri diritti da una condotta posta in essere online e procede con l'attività istruttoria a cura della Direzione servizi media audiovisivi dell'Autorità.

Nel rispetto dei principi del giusto procedimento e del contraddittorio, i prestatori di servizi, l'uploader e i gestori delle pagine e del sito Internet coinvolti possono adeguarsi spontaneamente alla richiesta del soggetto istante dandone comunicazione alla Direzione che dispone l'archiviazione oppure presentare controdeduzioni allegando ogni elemento utile ai fini del relativo accertamento.

Tale fase termina con la formulazione di una proposta di archiviazione, ovvero di adozione di particolari misure.

La successiva fase decisoria è svolta di fronte l'organo collegiale che, ai sensi dell'art. 8 del Regolamento, dopo aver esaminato gli atti ne dispone l'archiviazione qualora non ritenga sussistente la violazione oggetto di istanza ovvero adotta le misure nei confronti dei prestatori di servizi destinatari della comunicazione al fine di impedire o porre fine alla violazione.

Tali misure consistono in "ordini" emanati nel rispetto dei criteri di gradualità, proporzionalità e adeguatezza che devono essere ottemperati entro 3 giorni dalla notifica. Gli ordini previsti dal secondo comma fanno riferimento agli artt. 14, co. 3, e 16, co. 3, del D.lgs. 9 aprile 2003, n. 70, i quali prevedono che «l'autorità giudiziaria o

[59] AA.VV., *Il regolamento Agcom sul diritto d'autore*, a cura di L. C. UBERTAZZI, Torino, 2014, 73.

quella amministrativa avente funzioni di vigilanza può esigere anche in via d'urgenza, che il prestatore, nell'esercizio delle attività […], impedisca o ponga fine alle violazioni commesse»; le attività a cui si fa riferimento sono quelle di mere conduit[60] e di hosting[61].

Il terzo comma prevede l'ordine di rimozione selettiva delle opere digitali in violazione del diritto d'autore in capo ai prestatori di servizi svolgenti attività di hosting[62]; le opere devono essere rese disponibili o devono essere ospitate su un server ubicato nel territorio nazionale. Nei casi più gravi, in cui le violazioni assumono carattere massivo, è stabilito che l'ordine possa prevedere la disabilitazione all'accesso delle opere digitali invece che la rimozione selettiva delle stesse.

Se il server è ubicato fuori dal territorio nazionale, l'organo collegiale può ordinare ai prestatori di servizi che svolgono attività di mere conduit di provvedere alla disabilitazione dell'accesso al sito.

«Qualora adotti le misure previste ai commi 3, secondo periodo, e 4, l'organo collegiale ordina ai prestatori di servizi […] di procedere a reindirizzare automaticamente verso una pagina Internet redatta secondo le modalità indicate dall'Autorità le richieste di accesso alla pagina […] su cui è stata accertata la presenza di opere digitali diffuse in violazione del diritto d'autore o dei diritti connessi». In caso di mancata ottemperanza degli ordini dell'Autorità la stessa applica le sanzioni previste dall'art. 1, co. 31, della legge 31 luglio 1997, n. 249, dandone comunicazione agli organi di polizia giudiziaria ai sensi dell'art. 182-*ter* della Legge sul diritto d'autore.

I provvedimenti esaminati sono adottati entro trentacinque giorni dal ricevimento dell'istanza; tale breve termine, seppur potenzialmente lesivo dei diritti di difesa dei soggetti coinvolti nella procedura, ha l'obiettivo di garantire gli interessi che il Regolamento si prefigge di tutelare.

In particolari casi previsti dall'art. 9 del Regolamento, l'Autorità procede con un procedimento ancora più snello e celere denominato procedimento abbreviato.

3. Le "opere digitali" e gli Internet Service Provider (ISP).

3.1 Nuove normative per nuovi strumenti di comunicazione.

[60] Attività di trasmissione e di fornitura di accesso includenti la memorizzazione automatica, intermedia e transitoria delle informazioni trasmesse, a condizione che questa serva solo alla trasmissione sulla rete di comunicazione e che la sua durata non ecceda il tempo ragionevolmente necessario a tale scopo.
[61] Memorizzazione di informazioni fornite da un destinatario del servizio.
[62] Vd. *infra*

In Internet, le modalità di fruizione delle opere dell'ingegno senza il consenso del titolare dei diritti sono rappresentate dalla riproduzione, dal caricamento (upload), dalla diffusione (sharing) e dal download dei dati riproducibili da appropriati dispositivi elettronici multimediali che rappresentano il contenuto informativo delle opere stesse.

La fruizione delle "opere digitali"[63] è possibile secondo modalità molteplici ed in continua evoluzione e tra queste si ricorda: linking, torrent, download, peer-to-peer e streaming.

Il link (da cui il c.d. linking[64]) è un collegamento ipertestuale che riconduce ad un contenuto digitale: grazie ad un link, infatti, si può raggiungere direttamente un sito cliccando su una parola attiva (c.d. hotword), nel caso in cui a questa sia collegato un indirizzo Internet (URL, Uniform Resource Locator). I link sono, in pratica, vere e proprie rotte di "indirizzamento" verso URL che altrimenti sarebbe difficilmente raggiungibili. Il torrent è un file di dimensioni modeste in grado di contenere informazioni che permettono il download di dati mediante apposite applicazioni. Il download è l'attività di ricezione e memorizzazione dell'opera digitale attraverso il collegamento ad un server. Il peer-to-peer consiste nello scambio di dati tra utenti di una rete in cui ognuno di essi può sia inviare sia ricevere contenuti. Lo streaming, infine, è un flusso audio-video trasmesso da un server a vari client e riprodotto man mano che i dati arrivano a destinazione e che permette, dunque, la condivisione di file (c.d. file sharing) evitando il download dell'intero contenuto all'utente.

L'interpretazione delle disposizioni vigenti in materia da parte degli studiosi non è stata semplice, soprattutto precedentemente alla formulazione ed al recepimento di normative di settore i cui obiettivi sono stati creare strumenti di tutela al passo con le nuove tecnologie.

Un importante contributo alla ridefinizione di concetti ed alla variazione della terminologia contenuti nella Legge sul diritto d'autore n. 633/1941 è stato quello apportato dal decreto legislativo 9 aprile 2003, n. 68, che ha recepito la direttiva europea 2001/29/CE.

[63] Vd. nota n. 5 per una definizione di "opere digitali".
[64] AA.VV., *Diritto delle nuove tecnologie informatiche e dell'Intenet*, a cura di G. CASSANO, I ed., Milano, 2002, 936.

L'art. 1 del predetto decreto ha ridefinito il concetto di riproduzione contenuto nell'art. 13 della legge n. 633/1941 contemplante il divieto «di riprodurre […] in maniera diretta o indiretta, temporanea o permanente, in tutto o in parte» le opere dell'ingegno «in qualunque modo o forma» e «con ogni altro procedimento di produzione» senza il consenso dell'autore.

La nozione di riproduzione è stata arricchita dal riferimento a nuove modalità della stessa e tale impostazione riflette la volontà della direttiva europea di fornire una definizione quanto più ampia possibile al fine di garantire la certezza del diritto.

Rilevante risulta, inoltre, il concetto di riproduzione temporanea che, in Internet, indica una serie di modalità di memorizzazione dei contenuti ottenuti online, quali il proxy caching, il mirroring e il buffering, modalità che si contrappongono alla riproduzione permanente esperibile attraverso procedure di upload e di download. Infine la riproduzione indiretta si caratterizza come forma a distanza e si identifica con ogni forma di comunicazione o trasmissione dell'opera, di cui Internet rappresenta l'esempio più importante.

Altra nozione direttamente riconducibile al fenomeno Internet è quella contenuta nell'art. 16 della Legge sul diritto d'autore: il diritto di comunicazione dell'opera al pubblico su filo o senza filo.

La portata di tale diritto esclusivo, comprendente «la messa a disposizione del pubblico dell'opera in maniera che ciascuno possa avervi accesso dal luogo e nel momento scelti individualmente», è stata chiarita dalla Corte di giustizia dell'Unione europea laddove ha affermato che tale nozione non è esaustiva e che deve essere contestualizzata, precisandone il senso e la portata, ribadendo che si riferisce a «qualsiasi trasmissione o ritrasmissione di un'opera al pubblico non presente nel luogo in cui esse hanno origine, su filo o senza filo»[65].

La giurisprudenza ha quindi avuto modo di precisare che anche la riproduzione via Internet è una forma di utilizzazione economica dell'opera dell'ingegno per cui dev'essere sempre previsto il consenso del titolare dei diritti per ogni forma di comunicazione al pubblico effettuata con qualsiasi mezzo.

Al medesimo articolo sono state ricondotte anche le già citate modalità di fruizione delle opere via web, quali: upload in un sito web, download, file-sharing attraverso attività di linking, peer-to-peer e streaming.

[65] CGUE, C 607-11, *ITV Broadcasting*, 7 marzo 2013.

Secondo un altro orientamento, formulato dalla Corte di Giustizia dell'Unione europea in una controversia in materia di "software", la distribuzione di opere in Internet non sarebbe riconducibile all'art. 16 bensì al successivo art. 17, secondo cui la distribuzione in Internet di opere è solo una modalità di messa a disposizione delle stesse, idonea quindi a determinare l'esaurimento del diritto di comunicazione al pubblico al pari della prima vendita o del primo atto di trasferimento della proprietà, conseguenza profondamente diversa da quella precedentemente illustrata, per cui il diritto non si esaurisce con alcun atto di comunicazione al pubblico.

Infine, l'art. 32-*bis* del Testo Unico della Radiotelevisione[66] include i fornitori di SMAV (Servizi Media Audiovisivi) come soggetti vincolati al rispetto dei diritti d'autore e diritti connessi, specificando che questi ultimi sono tenuti a trasmettere le opere nel rispetto dei termini temporali e delle condizioni concordate con i titolari dei diritti oltre a dover astenersi dal mettere comunque a disposizione degli utenti, su qualsiasi piattaforma e qualunque sia la tipologia del servizio offerto, programmi oggetto di diritti di terzi (o parti di essi) senza il consenso dei titolari dei diritti stessi, salve le disposizioni in materia di brevi estratti di cronaca.

Nella "Società dell'Informazione", i beneficiari della tutela di questi diritti sono, in base al dettato della direttiva 2001/29/CE, i titolari dei diritti e non solo gli autori (benché manchi una definizione chiara di tali nozioni).

Per alcuni si è voluto in questo modo includere anche i titolari di diritti connessi ai quali sono riconosciute prerogative in buona parte coincidenti con quelle degli autori, tracciando il passaggio a un diritto d'autore teso alla protezione di produttori, investitori e tutti coloro che contribuiscono alla nascita dell'opera, non tanto sotto il profilo creativo quanto piuttosto sotto quello economico-finanziario.

In tale mutato scenario è stato, dunque, necessario adottare nuovi modelli di enforcement rifacendosi, in particolare, all'esperienza statunitense relativa al DMCA (Digital Millennium Copyright Act).

3.2 I modelli di enforcement online

In mancanza di un elenco di soggetti che possono essere ritenuti responsabili per le violazioni del diritto d'autore e dei diritti connessi in Internet, è possibile individuare alcune figure a cui tale responsabilità può essere ricondotta; in particolare, l'uploader

[66] D.lgs. 31 luglio 2005, n. 177.

è colui che mette a disposizione un contenuto protetto in rete permettendone la fruizione ad altri utenti; tale soggetto non è facilmente individuabile senza la collaborazione dell'Internet Service Provider (ISP) che, pertanto, può essere destinatario di sanzioni inibitorie e può, in alcuni casi, essere considerato corresponsabile nell'illecito.

In particolare, gli ISP possono essere classificati in: (a) content provider, fornitori di contenuti; (b) network provider, fornitore di accesso alla rete; (c) access provider, consente l'accesso alla rete attraverso mezzi tecnici come la connessione; (d) host provider, fornisce ospitalità a siti Internet; (e) service provider, fornisce servizi di mero accesso alla rete; (f) cache provider, immagazzinano dati in un'area di allocazione temporanea.

Tali soggetti possono essere considerati "intermediari" in quanto «svolgono il fondamentale ruolo di facilitare lo svolgimento delle attività che hanno luogo in ambiente digitale» ed hanno un impatto economico, poiché partecipano a gran parte delle attività imprenditoriali in Intenet, nonché socio-culturale, in quanto permettono la condivisione di informazione e conoscenza e, quindi, la distribuzione digitale di opere dell'ingegno e sono, pertanto, figure chiave nelle «operazioni di rimozione e prevenzione degli illeciti che si realizzano in rete»[67].

Tali intermediari sono considerati (indirettamente) responsabili per la circolazione non autorizzata di materiale sulle proprie piattaforme nella fattispecie in cui non compiano gli atti reputati necessari per godere dell'esenzione offerta dai c.d. safe harbors ovvero non procedano a rimuovere i contenuti della cui provenienza illecita sono a conoscenza[68].

Alcune modalità di repressione di tali illeciti mutuate dall'esperienza statunitense sono le procedure di "notice and takedown" e di "notice and disconnect".

La procedura di "notice and takedown" si collega all'azione di monitoraggio sulle opere in Rete da parte degli stessi titolari del diritto d'autore che possono richiedere la rimozione dei contenuti illegalmente ospitati sulle piattaforme pubblicamente accessibili. Tale procedura non è prevista dal Regolamento Agcom nonostante nella fase di discussione e dibattito prodromica all'emanazione dello stesso se ne fosse ipotizzata l'introduzione.

---

[67] M.L. MONTAGNANI, *Primi orientamenti in materia di responsabilità dei fornitori di servizi cloud per violazione del diritto d'autore in rete*, in *Riv. dir. ind.*, 3, 2014, 177.
[68] Con l'espressione "*safe harbors*" si fa riferimento ad un'area di esenzione dalla punibilità in cui i fornitori di servizi Internet rientrano in determinate circostanze.

Altra procedura prevista dalle direttive europee (sullo schema offerto dall'esperienza statunitense) è la cd. procedura di "notice and disconnect" (o "graduated response"): la disconnessione dell'utente che ha posto in essere una condotta illecita non è immediata ma progressiva e avviene sulla base di tre o più passaggi al termine dei quali si commina la sanzione finale rappresentata dalla sospensione della connessione Internet.

L'utente, che viene dunque a conoscenza dell'avvio di una procedura per effetto degli avvertimenti inviatigli, dovrebbe essere in grado di sospendere la condotta illecita in modo da evitare la relativa sanzione.

Più in generale, i modelli di enforcement generalmente adottati in tema di diritto d'autore sulle reti telematiche sono tra loro ordinati incrociando l'operare di tre criteri distinti, che procedono: dal tipo di misure che essi prevedono per contrastare gli illeciti online, dalla relazione instaurata tra queste misure, dalla natura degli organi ai quali è devoluta la loro amministrazione[69].

In riferimento alla lett. a) assumono particolare rilievo i sistemi di limitazione della responsabilità civile in cui gli ISP possono rientrare collaborando nella prevenzione e nella repressione degli illeciti.

Tali soggetti possono essere ricompresi nei già citati safe harbors e godere, quindi, dell'esenzione dalla responsabilità risarcitoria, qualora si attivino tempestivamente per impedire la continuazione o la ripetizione della condotta illecita.

Un secondo genere di misure prevede l'istituzionalizzazione di procedure private di moral suasion: in questi casi il titolare del diritto ritenuto leso può trasmettere agli ISP una "notizia qualificata" di violazione in base a cui tali soggetti dovranno attivarsi per disabilitare l'accesso ai contenuti protetti che si assumono oggetto di violazione e, contemporaneamente, dare comunicazione all'uploader su cui grava l'onere di rispondere in maniera tempestiva e dettagliata circa il titolo all'utilizzazione dell'altrui opera protetta se vorrà che il suo collegamento sia ripristinato.

Il terzo genere di misure comprende le c.d. "injunctions" ed i già citati provvedimenti di sospensione dell'accesso ai servizi telematici.

[69] AA.VV., *Il regolamento Agcom sul diritto d'autore*, a cura di L. C. UBERTAZZI, Torino, 2014, 13.

Le injunctions sono irrogate «nei confronti dei diversi soggetti disposti lungo la filiera dell'illecito, tra le quali rientrano ordini inibitori contro gli ISP mirati a far cessare o addirittura prevenire il loro concorso negli illeciti altrui», i provvedimenti sospensivi invece sono rivolti agli utenti autori materiali degli illeciti[70].

Quarto ed ultimo genere di misure sono quelle destinate a favorire il reperimento, da parte del titolare dei diritti d'autore, delle informazioni relative all'identità degli autori degli illeciti telematici.

I diversi modelli esistenti possono prevedere l'impiego coordinato delle suesposte misure ovvero l'applicazione di tutte o solo alcune di esse.

L'Unione europea, con la direttiva 2000/31/CE, ha previsto un sistema basato su guidelines flessibili destinate a fungere da schema per le norme di dettaglio predisposte dai legislatori degli Stati membri.

La disciplina si limita a imporre agli Stati membri: a) un sistema di safe harbors; b) il divieto di imporre obblighi generali di sorveglianza sui comportamenti dei propri utenti; c) il divieto di ricerca attiva degli illeciti in capo agli ISP; d) un'ampia esenzione della responsabilità civile per carriers ed esercenti attività di caching; e) un regime di esenzione da sanzioni risarcitorie (a determinate condizioni) degli host provider.

Il legislatore, con il decreto legislativo n. 70/2003, ha provveduto a recepire e ad integrare la disciplina interna come previsto dalla predetta direttiva europea e prevede all'art. 16, come condizione per l'esenzione della responsabilità civile dei provider, l'immediata azione successiva alla ricezione dell'informazione riguardante la presenza online di un contenuto lesivo del diritto d'autore; in seguito a tale comunicazione inviata dall'autorità competente, il provider è tenuto ad impedire immediatamente l'accesso ai contenuti lesivi presenti in rete[71].

Il meccanismo appena illustrato esclude l'insorgere di un obbligo di rimozione prima della valutazione di illiceità da parte di un'autorità che nell'ordinamento italiano sono, come detto, l'Agcom, per una tutela amministrativa dotata di maggiore celerità, ovvero l'Autorità giudiziaria, in ambito civile e penale.

4. Conclusioni

Alla luce di quanto esposto, in un mondo sempre più digitalizzato, le nuove tecnologie rappresentano uno strumento in grado di mettere a disposizione nuovi stru-

[70] *Ibidem*.

menti per lo sfruttamento dei diritti di proprietà intellettuale su opere digitali e/o digitalizzate da parte dei titolari, ma anche nuovi e seri pericoli legati alla natura stessa di Internet.

Soggetti nuovi, dunque, sono oggi presi in considerazione dalla normativa vigente in materia: gli Internet Service Provider la cui attività di intermediazione è fondamentale per permettere l'utilizzo della rete da parte degli utenti.

In un mondo in costante e rapida evoluzione come quello digitale, però, il diritto è chiamato ad uno sforzo ancora maggiore rispetto alla previsione degli strumenti di tutela contro gli illeciti perpetrabili in Internet: aggiornare tali strumenti costantemente in modo da garantirne l'efficacia e l'effettività.

Pertanto, anche se molto è stato fatto per assicurare una effettiva tutela dei diritti di proprietà intellettuale su opere digitali e/o digitalizzate, non può considerarsi abbastanza, atteso che l'inarrestabile progredire delle tecnologie continua tuttora.

BLOCKCHAIN E DIRITTO ITALIANO: UNO SGUARDO D'INSIEME.

di Rita Di Marco

SOMMARIO: 1. Premessa 2. Il procedimento 3. Le caratteristiche principali. 4 Il bitcoin 5. L'applicazione al campo del diritto

The blockchain is information technology, which allows for the certification of transactions between subjects. The blockchain is applied in contract law, in banking, financial, insurance and IT law.

A smart contract is the "translation or transposition in code of a contract in order to automatically verify the fulfillment of certain conditions (control of basic data of the contract) and to automatically perform actions (or make available so that they can perform certain actions) when the specific conditions between the parties are reached and verified".

1. Premessa.

La *blockchain* è la tecnologia informatica, che consente di certificare transazioni tra persone. Nell'uso più noto, essa è alla base del Bitcoin e serve a verificare lo scambio di criptovaluta tra due utenti.

2. Il procedimento

Una transazione, nel mondo reale e sul web, necessita di "una terza persona di fiducia"[72] a garanzia dello scambio. Di contro, l'obiettivo della blockchain è l'eliminazione dell'intermediario, con la possibilità di effettuare operazioni criptate completamente anonime e archiviando tutte le transazioni in un registro pubblico distribuito in rete. I dati di una transazione sono memorizzati su più macchine collegate tra loro. Si definiscono, pertanto, "nodi" tutti i computer fisici partecipanti alla blockchain. In questo senso, pertanto, la blockchain può essere definita come una catena di blocchi di dati che si riferiscono a transazioni e che devono poi essere verificati. La conferma da parte della rete è un meccanismo di garanzia. In una blockchain l'intermediario è

[72] M. MORICI *La Blockchain, spiegata bene*, in *http://Panorama//19 gennaio 2018.*

sostituito da un protocollo di comunicazione in grado di certificare, approvare e archiviare le transazioni che avvengono all'interno della "catena": basta avere la conferma del 50%+1 dei nodi. Una volta verificate dalla "rete", le transazioni vengono archiviate in un *ledger*, vale a dire una sorta di registro pubblico. Il processo di approvazione (*mining*) fa eseguire a un computer fisico dei calcoli matematici molto complessi che sono necessari per dare la conferma alle operazioni. I *"minatori"* possono poi incassare commissioni dalle transazioni. La blockchain permette, quindi, di archiviare tutti gli scambi in una sorta di libro contabile condiviso e sicuro: i blocchi, infatti, una volta approvati, sono immodificabili.

I dati relativi agli scambi sono salvati all'interno di blocchi crittografici, collegati in maniera gerarchica l'uno all'altro. In tal modo si viene a creare un'infinita catena di blocchi di dati, che consente di risalire e verificare tutte le transazioni fatte.

3. Le caratteristiche principali

Le principali caratteristiche della tecnologia blockchain possono, pertanto, così riassumersi:

- immutabilità del registro
- tracciabilità delle transazioni
- alto livello di sicurezza basato su tecniche crittografiche

La *blockchain* vive una grande diffusione in svariati campi, perché comporta numerosi vantaggi. Essa, infatti, è digitale e, dunque, adattabile a qualsiasi ambito; è sicura grazie al processo di crittografia; è attendibile, atteso che viene organizzata cronologicamente; è affidabile, poiché le sue caratteristiche tecniche ne impediscono il danneggiamento e la possibile perdita dei dati; è veloce, perché non richiede la presenza di un'entità centrale che ne verifichi la validità ed, in quanto tecnologia digitale, i tempi di qualsiasi operazione si comprimono. "*Una volta che una transazione viene certificata e salvata all'interno di uno dei blocchi della catena, non può più essere modificata né manomessa"*[73].

Ogni blocco è composto da un puntatore che lo collega al blocco precedente, un *timestamp*, vale a dire la marca temporale che conferma la data certa, e i dati della transazione.

[73] G. MOSCA *Che cos'è la blockchain, come funziona e perché funziona bene* in *http://www.wired.it.*

Questi tre elementi garantiscono che ogni elemento della *blockchain* sia univoco e immutabile: un'eventuale richiesta di modifica del *timestamp* o del contenuto stesso del blocco andrebbe a modificare anche tutti i blocchi successivi.

Se un hacker volesse violare un blocco della *blockchain*, dovrebbe violare tutti i blocchi costituenti la catena associata a quel blocco, eseguendo delle azioni non autorizzate su ciascuno dei *ledgers* associati ad ogni dispositivo-nodo, il cui numero è di fatto sconosciuto a priori e può essere elevato rendendo impossibile eseguire un qualsivoglia tentativo di corruzione dati.

4. La *bitcoin*

Nell'uso più noto, come sopra anticipato, la *blockchain* è il sottostante informatico della criptovaluta digitale *Bitcoin*. Quest'ultima è un database distribuito che sfrutta la tecnologia peer-to-peer: chiunque può prelevarlo dal web, diventando così un nodo della rete.

Ogni blocco viene liberato dai minatori, dotati di un'enorme potenza di calcolo utile a risolvere l'algoritmo che li protegge. Chi libera un blocco incassa 25 Bitcoin che può riversare sul mercato e quindi conseguire un guadagno. Anche i nodi, le maglie della catena che supervisionano e approvano le transazioni, incassano una piccola percentuale del totale delle transazioni stesse.

Il sistema di *Bitcoin* funziona, perché tutti coloro che vi partecipano guadagnano[74].

L'orientamento maggioritario definisce le criptovalute come una specie del più ampio genere delle valute digitali, ossia quelle che nella definizione più classica non hanno un equivalente fisico.

Le criptovalute sono beni immateriali aventi natura scritturale, sono sostanzialmente emesse da privati e prive di autorità di regolamentazione in senso classico, in quanto tali autorità sono rappresentate dagli stessi utenti, che procedono allo sviluppo tecnico della regolamentazione medesima, sottoposta, poi, al giudizio della comunità che intende utilizzarla. Occorre, pertanto, che un numero significativo di utenti ne acquisti e, soprattutto, ne faccia uso. Le criptovalute, in particolare, possono essere anche un utile strumento per raccolte fondi relative a progetti senza scopo di lucro riguardanti istruzione e ricerca.

[74] C. MORELLI, *Risolvere controversie non è mai stato così facile: basta la blockchain* in *http://Altalex.it*, 2018.

5. L'applicazione al campo del diritto – lo *Smart Contract.*

La *blockchain* viene applicata nel diritto contrattuale nel diritto bancario, finanziario, assicurativo ed informatico.

Uno *smart contract* è la "*traduzione* o *trasposizione in codice di un contratto in modo da verificare in automatico l'avverarsi di determinate condizioni* (*controllo di dati di base del contratto*) *e* di *auto-eseguire in automatico azioni* (*o dare disposizione affinché si possano eseguire determinate azioni*) *nel momento in cui le condizioni determinate tra le parti sono raggiunte e verificate*"[75]: è basato su un codice che "*legge*" sia le clausole concordate sia la condizioni operative, nelle quali devono verificarsi le condizioni concordate. Lo *smart contract* si auto-esegue automaticamente nel momento in cui i dati riferiti alle situazioni reali corrispondono ai dati riferiti alle condizioni e alle clausole concordate. Esso, dunque, ha bisogno di un supporto legale per la sua stesura, ma non ne ha bisogno per la sua verifica e per la sua attivazione.

L'obiettivo della tecnologia *blockchain* è, pertanto, quello di rendere eseguibili le clausole di un contratto tra più parti mediante un codice o set di transazioni opportunamente criptate le quali specificano (mediante un opportuno protocollo interno) le condizioni contrattuali pattuite tra le parti. Le clausole contrattuali, criptate in transazioni da eseguire nella *blockchain*, saranno lette ed automaticamente interpretate dai relativi nodi-dispositivi della rete, le quali, pertanto, attraverso il meccanismo dei miners sopra descritto, saranno eseguite ed alla fine convalidate con *timestamp*. Dopo l'esecuzione e la distribuzione nella *blockchain*, le transazioni, inglobate in blocchi con relativo *timestamp*, aggiorneranno i vari *ledgers* dei singoli nodi-dispositivi partecipanti alla rete, divenendo di fatto "irrevocabili", sicure ed aventi data certa[76].

L'adozione degli *smart contracts* e della rete *blockchain* ha lo scopo di consentire nei procedimenti giudiziari in maniera sicura e semplice l'acquisizione della data certa dell'esecuzione contrattuale (*time-stamp del nodo*), la certezza di esecuzione della clausola da parte dei contraenti (*validazione del blocco*), la successione temporale delle esecuzioni contrattuali (*cronologia temporale dei blocchi memorizzata nel ledger dei dispositivi-nodi*).

---

[75] A. AZZARITI *Cos'è il Bitcoin? Il ruolo del diritto nella regolamentazione delle criptovalute* in *http://Cyberlaws.it.*

[76] F. RUNDO, S. CONOCI, *Tecnologia "Blockchain": dagli smart contracts allo smart driving* in *http://Sicurezza e Giustizia.it.*

Nei procedimenti giudiziari civili e penali, infatti, e, in particolare, in quelli riguardanti casi di sinistri stradali, l'utilizzo della tecnologia *blockchain* può migliorare sensibilmente la gestione del contenzioso, in quanto, attraverso l'utilizzo dei dati memorizzati nei nodi della *blockchain*, sarà possibile ricostruire in maniera precisa ed accurata la dinamica dell'incidente oggetto del contendere. Il sistema sarà, dunque, in grado di fornire una soluzione veloce del contenzioso riducendo al minimo i rischi di una decisione errata.

Ora, posto che nel nostro ordinamento giuridico, la conclusione dei contratti richiede delle precise formalità previste, come noto, dalla normativa codicistica e, talvolta, dalla normativa specifica di settore, l'applicazione degli *smart-contracts* attraverso la tecnologia *blockchain*, nonostante i vantaggi sopra descritti, si scontra con una normativa che non ne consente un'applicazione agevole. Affinchè uno *smart contract* possa definirsi equiparabile giuridicamente ad un contratto classico, dovrebbe contenere in maniera chiara, puntuale e precisa, gli elementi di cui all'articolo 1325 c.c., vale a dire l'accordo delle parti, la causa, l'oggetto e la forma, se prevista. In uno *smart contract* generato su una rete *blockchain*, questi elementi risultano di difficile individuazione e interpretazione. Di conseguenza, la loro individuazione sia in regime di verifica della loro validità che in sede di contenzioso risulta complessa, in quanto sia il giudice che un eventuale CTU dovrebbero essere in grado di ricavare i requisiti previsti ex art. 1325 c.c. dall'analisi dei blocchi della *blockchain*.

Ad ogni modo, l'aspetto più problematico da considerare è quello relativo al fatto che uno *smart contract*, che per definizione è immodificabile ed eseguito secondo un algoritmo deterministico, potrebbe rivelarsi incapace di eseguire correttamente le clausole contrattuali aggiuntive o ad applicazione differita nel tempo o al verificarsi di determinate condizioni, come nei contratti bancari e finanziari, in quanto non tutte le variabili possono trovare opportuna trasposizione algoritmica.

Coordinamento editoriale:
Gruppo di lavoro *Data Protection Law*

This work is published under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License (CC BY-NC-ND 4.0). You may freely download it but you must give appropriate credit to the authors of the work and its publisher, you may not use the material for commercial purposes, and you may not distribute the work arising from the transformation of the present work.