Rivista Semestrale

Luglio – Dicembre 2021

N. 2/2021

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

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.

PIETRO DE ROSA, Tutela del diritto all'anonimato on-line e responsabilità civile degli internet service providers: ricerca di un equilibrio tra libertà di espressione e accountability.

Pag. 3

TIZIANA DI PALMA, Le necessità di contemperamento tra le finalità di marketing e la tutela del trattamento dei dati personali: Tecniche di marketing e adempimenti del titolare del trattamento.

Pag. 40

LIVIA SMORALDI, MARTA STRAZZULLO, *"Prevenire è meglio che curare"*: il compito dell'avvocato in caso di *data breach.*

Pag. 57

GAETANO GUARINO, Trattamento dei dati personali in ambito scolastico.

Pag. 73

LORENZO BAUDINO BESSONE, Gli obblighi di notifica al Garante e comunicazione agli interessati: peculiarità e criticità nella gestione *ex post* della *data breach* in Italia

Pag. 94

TUTELA DEL DIRITTO ALL'ANONIMATO ON-LINE E RESPONSABILITÀ CIVILE DEGLI INTERNET SERVICE PROVIDERS: RICERCA DI UN EQUILIBRIO TRA LIBERTÀ DI ESPRESSIONE E ACCOUNTABILITY

Di Piero De Rosa

SOMMARIO. 1. Considerazioni introduttive sull'anonimato *on-line*. – 2. Anonimato, libertà di informazione e tutela della personalità in Rete. – 3. Anonimato e responsabilità degli *Internet Service Providers*. – 4. Conclusioni. – 5. Note bibliografiche.

"The new freedom of expression brought by the Internet goes far beyond politics. People relate to each other in new ways, posing questions about how we should respond to people when all that we know about them is what we have learned through a medium that permits all kinds of anonymity and deception." — Peter Singer

Abstract

The use of anonymity (and of on-line pseudonyms) allows a greater security for users to navigate the web: it represents a digital tool to protect their privacy and to ensure the sharing of information and opinions without any interference traditionally related to the "real world".

However, the issue raised by on-line anonymity involves new challenges that government authorities have recently faced in different ways and, the different regulatory approaches to this phenomenon, explain a closer relationship between authority and freedoms and between individual rights and collective needs. Anonymity on the Internet not only is a pre-requisite for exercising freedom of expression, but often represents, especially in illiberal legal systems, a democratic tool for those who want to express freely their opinion and fight in defence of human rights to obtain a greater redistribution of power among social classes and exert more pressure on public institutions.

Therefore, the purpose of this work is to answer to the following questions: is freedom of expression necessarily linked to the recognition of those who express themselves? Is the use of anonymity justified in the exercise on-line activities? Who is responsible for the illegal conduct that are anonymously carried out on the web? And above all, who is in charge to recognize those users who expresses themselves in anonymity and when?

1. Considerazioni introduttive sull'anonimato *on-line*.

Nell'esaminare il tema dell'anonimato in Internet, con particolare attenzione alle questioni legate all'esercizio della libertà di espressione in forma anonima, si rende necessario anzitutto soffermare la nostra riflessione sul concetto stesso di anonimato e sui problemi – di ordine economico, politico e tecnico – che sono ad esso, tradizionalmente, collegati.

Preliminarmente, per "anonimo" possiamo generalmente intendere tutto ciò che è privo di nome e ciò che non è associabile ad un determinato soggetto, ma il "dato anonimo" è anche ciò che non è concepito come un dato personale e che può divenire tale se è possibile risalire, in qualche modo, all'identità dell'interessato[1].

Già a partire dagli anni '50 del secolo scorso, i giuristi e gli studiosi del diritto si erano occupati della materia dell'anonimato nell'ambito del diritto alla riservatezza promuovendo una riflessione sistematica sul tema e riconducendo l'anonimato sostanzialmente all'esercizio del diritto alla protezione dei dati personali[2]. Negli ultimi anni, infatti, l'anonimato ha rappresentato sempre più un punto di riferimento essenziale nella c.d. "società dell'informazione" per l'applicazione delle norme sulla protezione

[1] Cfr. Garante Privacy 23.01.1998, doc. web. n. 39568, in https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1044151

[2] Sul concetto di anonimato si veda, a riguardo, A. CANDIAN, *Anonimato (diritto all')*, in Enc. dir., II, Milano, 1958, e G. FINOCCHIARO (a cura di), *Diritto all'anonimato. Anonimato, nome e identità personale*, in Tratt. Galgano, XLVIII, Padova, 2008.

dei dati personali (intesa come difesa della propria personalità *on-line*[3]) ai fini della tutela del soggetto a cui tali dati sono riferiti[4].

Senza dubbio, la crescita della rilevanza e del valore delle informazioni ha prodotto un contestuale incremento dell'importanza dell'anonimato quale strumento essenziale per un esercizio effettivo del diritto alla riservatezza e della protezione dei dati personali.

Tuttavia, il problema dell'anonimato si pone con maggiore evidenza proprio in rapporto alle reti telematiche e alla creazione dei primi *database* che hanno consentito una più agevole raccolta e conservazione dei dati e la contestuale esigenza di una loro effettiva tutela[5].

In merito all'evoluzione della Rete (e dei problemi ad essa collegati) non si può non ricordare come già Lawrence Lessing, nel saggio "*The Architecture of Innovation"* (2001), abbia per primo esaminato i rapporti tra Internet e il potere, affrontando il tema complesso dell'evoluzione dell'architettura originale della Rete e della sua trasformazione come volano dell'informazione[6].

La struttura originale di Internet, infatti, era stata pensata e progettata per la condivisione dei contenuti e delle informazioni, vale a dire una Rete liberamente accessibile anche nei linguaggi di programmazione e nei codici sorgente delle diverse applicazioni dal momento che, in questa fase embrionale, gli utenti principali erano prevalentemente accademici, centri di ricerca ed università che utilizzavano le potenzialità offerte da Internet per fini di ricerca e di studio[7].

---

[3] Con l'avvento della Rete, i motori di ricerca e le piattaforme di condivisione dei contenuti generati dagli utenti hanno permesso una circolazione capillare delle notizie da cui, peraltro, deriva la principale fonte di pregiudizio per la genuina rappresentazione dell'identità personale degli individui. Un simile elenco di dati va a comporre una sorta di biografia *on-line* della propria identità digitale che non necessariamente corrisponde a quella reale. Sul punto, cfr. C. MELZI e G. E. VIGEVANI, *Lo statuto dell'informazione su Internet*, in T. E. FROSINI, O. POLLICINO, M. BASSINI (a cura di), *Diritti e libertà in internet*, Mondadori Education, Milano, 2017.

[4] Cfr. G. FINOCCHIARO e F. DELFINI (a cura di), *Diritto all'anonimato*, UTET, 2014.

[5] Cfr. G. MUSELLA, *Diritto all'oblio e revisionismo storico: due facce della stessa medaglia?*, Media-Laws, 2015.

[6] Sul tema si guardi anche a L. LESSING, *Cultura libera*, APOGEO, 2005.

[7] Internet rappresenta il frutto indiretto della Guerra Fredda tra Stati Uniti e Russia. Nei primi anni Sessanta del secolo scorso si era diffuso nel mondo il terrore di una guerra nucleare e, per tale motivo, il Ministero della Difesa americano aveva avviato un progetto di ricerca allo scopo di preservare le comunicazioni in caso di attacco. Per la realizzazione di questo progetto nacque l'agenzia governativa ARPA che coordinava e finanziava la ricerca nel campo delle telecomunicazioni militari. Nel 1983, la sezione militare si staccò da questo nuovo macrorganismo e nacque Internet.

Secondo Lessing, oggi si pone nuovamente la necessità di recuperare e difendere le caratteristiche originali di Internet, che, all'inizio, era stato creato proprio allo scopo di tutelare e proteggere la libertà di parola, la *privacy* degli utenti e la libera circolazione dei contenuti da una più stringente regolamentazione locale[8]:

"*The innovation of the Internet — built into its architecture — is an innovation in the ways in which culture gets made (...) The crucial feature of this new space is the low cost of digital creation, and the low costs of delivering what gets created."*

Ciò è strettamente collegato al tema della c.d. *net neutrality*, ovvero l'idea in base alla quale gli Internet Service Provider (i fornitori di accesso ad Internet e dei servizi di Internet) devono rendere ugualmente accessibili a tutti, in condizioni di *par condicio*, i contenuti e le applicazioni del *web* a, prescindere dallo strumento utilizzato, senza alcun pregiudizio, privilegio o discriminazione:

"The idea is that a maximally useful public information network aspires to treat all content, sites, and platforms equally. This allows the network to carry every form of information and support every kind of application. The principle suggests that information networks are often more valuable when they are less specialized – when they are a platform for multiple uses, present and future."[9]

All'inizio, la struttura di Internet rendeva difficile — se non impossibile — l'identificazione degli utenti perché pensata e progettata per garantirne la loro massima libertà e per assicurare la totale apertura della Rete ai fini della diffusione delle informazioni e della conoscenza[10]. Al momento della sua ideazione, Internet era cioè disegnato come un *luogo aperto* in cui tutti potevano esprimere liberamente le proprie idee.

L'attenzione, pertanto, non si concentrava sulla sicurezza dei dati e delle informazioni che, anzi, venivano scambiati senza impedimenti dagli utenti, soprattutto per

[8] Cfr. L. LESSING, *Strutturare l'innovazione*, trad. it. B. Giovanetti, 2001, in https://pws.winston-smith.info/Architecting_innovation_Lawrence_Lessig.html

[9] Cfr. T. WU, *Network Neutrality, Broad and DiscriminationI*, Journal of Telecommunications and High Technology Law, Vol. 2, p. 141, 2003, in http://www.timwu.org/network_neutrality.html

[10] Nel suo nucleo originario, Internet nasce come un protocollo per scambiare a distanza files (FTP) che poi si evolve per consentire lo scambio anche di messaggi elettronici (SMTP). Sul punto, cfr. A. SIMONCINI, *Sovranità e potere nell'era digitale*, in T. E. FROSINI, O. POLLICINO, M. BASSINI (a cura di), *Diritti e libertà in internet*, Mondadori Education, Milano, 2017.

la necessità di favorire e semplificare gli scambi tra ricercatori e gli studiosi, senza perseguire ulteriori finalità[11].

Se inizialmente tale dibattito era stato caratterizzato da profonde connotazioni ideologiche – e l'apertura della Rete veniva correlata, anche nella dinamica politica, alle garanzie di libertà e di pluralismo – negli ultimi anni l'attenzione si è focalizzata sempre di più sulla dimensione economica di Internet, della concorrenza degli operatori del mercato e della contestuale esigenza della tutela dei consumatori.

Si è passati progressivamente ad una nuova concezione di Internet, caratterizzata dallo sfruttamento economico e commerciale delle potenzialità offerte dalla Rete: la quantità dei dati che viene condivisa dagli utenti *on-line* genera una serie di informazioni (mai viste prima con gli altri *media* tradizionali) di notevole valore dal punto di vista economico dal momento che le aziende traggono profitto da queste informazioni allo scopo di catturare l'attenzione degli utenti, presentando agli stessi messaggi pubblicitari "su misura" e più adatti a stimolarne gli acquisti e orientarne le scelte di consumo.

Una volta superato il metodo di comunicazione originale mono-direzionale, il progresso tecnologico si è evoluto nella fornitura di servizi *on-line* rispetto ai quali l'utente non è più un mero spettatore passivo, ma un vero e proprio attore dinamico, capace di generare e modificare il contenuto del messaggio in base alle proprie esigenze ed interessi e da cui derivano informazioni precise sulle sue propensioni personali[12].

La Rete, dunque, perde la sua caratteristica di spazio riservato e diviene un *bene di massa*, un *mare magnum* interconnesso e aperto[13], in cui l'accesso degli utenti deve essere necessariamente controllato e regolato da chi ne gestisce le sue infrastrutture: quanto più il *web* si diffonde, tanto più aumentano gli utenti e il valore connesso alla diffusione delle informazioni e dei pericoli legati alla sicurezza dei dati e dei sistemi. Vengono così introdotte tecnologie capaci da limitare le inziali libertà di accesso che

[11] La natura aperta e non discriminatoria di Internet si basava su un approccio di *"innovation without permission"*. Sul punto, cfr. G. NAVA, *Net neutrality: tra tutela del consumatore e della concorrenza*, in G. CASSANO, G. SCORZA, G. VACIAGO (a cura di), *Diritto dell'internet. Manuale operativo. Casi, legislazione, giurisprudenza*, Cedam, 2013.

[12] La digitalizzazione delle informazioni e la tecnologia informatica hanno permesso di realizzare la "multimedialità", ovvero la fruizione di testi, immagini, suoni, animazioni grazie alla compresenza ed interazione di più linguaggi.

[13] Un sistema aperto è un sistema informatico operante in connessione con altri ambienti, anche eterogenei rispetto alla tecnologia e alle piattaforme utilizzate.

consentono di individuare agevolmente l'utente e il contenuto delle transazioni che egli realizza *on-line*, registrando ogni attività compiuta sui siti *web*.

Ciò comporta, per un verso, un maggiore controllo dei dati e delle informazioni – e, conseguentemente, un interesse diffuso per le attività realizzate dagli utenti sulla Rete – che deve trovare un proprio limite nella disciplina sulla riservatezza e della protezione dei dati personali. I soggetti detentori dei siti Internet (c.d. "gestori del sito"[14]) sono costretti, infatti, ad investire pesantemente sui sistemi informatici dedicati alla protezione dei dati e delle infrastrutture allo scopo non soltanto di difendersi dalle debolezze tecniche (tipiche di Internet) e da eventuali attacchi compiuti deliberatamente da soggetti esterni, ma anche per tutelare i dati personali degli utenti, ovvero tutte quelle informazioni, che da sole o congiunte ad altre, consentono di indentificare una persona[15].

Tra l'altro, non sembrano sussistere ragioni perché, rispetto ad altri mezzi analoghi, per Internet dovrebbe configurarsi un diritto alla sua libera utilizzazione in senso assoluto: alla libertà di manifestazione del pensiero esercitata dai singoli non si accompagna un simile diritto sugli strumenti che ne permettono l'esercizio. Nel silenzio del legislatore, che dimentica di occuparsi della Rete e dell'esercizio dei diritti legati al nuovo mezzo, la giurisprudenza ha esteso, per analogia, una serie di limiti e principi alla libertà di manifestazione del pensiero *on-line*.

Allo stesso tempo, però, la fisionomia della Rete deve essere concepita nei termini di garantire un più alto livello di pluralismo e di evitare, possibilmente, forme inaccettabili ed invasive di sorveglianza e di controllo diffuso sulle attività realizzate dagli utenti.

In altri termini, l'anonimato *on-line* rappresenta una caratteristica essenziale della Rete, costituendo uno strumento necessario per limitare forme pervasive di controllo da parte dei poteri pubblici o privati.

Da qui, l'ipotesi di inquadrare il diritto all'anonimato *on-line* come un diritto fondamentale dell'individuo al fine di consentire a tutti di esprimere le proprie idee senza temere ripercussioni, discriminazioni o esclusioni dai circuiti comunicativi. Le

[14] Il termine *(platform)* è preferito dalle *Big Tech* per definire la propria attività, allo scopo di apparire neutrali e operare con minori vincoli normativi anche se intendono al tempo stesso esercitare il potere decisionale assoluto sulla *content moderation*. Questo paradosso è stato rilevato da N.P SUZOR, *Lawless. The secret rules that govern our digital lives*, Cambridge University Press, 2019

[15] Comincia ad apparire una contraddizione tra il desiderio di comunicazione assolutamente aperta e il diritto alla *privacy*, inteso come difesa necessaria ad una intrusione autoritaria. Cfr. D. BUNNELL, *Mondo 2000*, Controculture, Roma, 2000.

considerazioni sull'evoluzione di Internet rappresentano il nucleo centrale dell'intera riflessione dal momento che Internet è stato plasmato inizialmente dalla comunità scientifica e gradualmente si è trasformato in un progetto libertario fondato sulla cooperazione e sulla fiducia nello sviluppo di una "intelligenza collettiva"[16].

Ciò, tra l'altro, è connaturato alle stesse nuove tecnologie che, rendendo possibile un controllo diffuso sulle attività e sulle vite degli individui, hanno imposto l'esigenza di un vero e proprio diritto all'anonimato su Internet al fine di controbilanciare dette forme di sorveglianza.

Sul punto, l'ex Segretario Generale delle Nazioni Unite, Ban Ki-Moon, durante il *forum* sulla sicurezza di Internet del 2014, ribadiva come il tema delle libertà in Internet sia strettamente collegato al quadro dei diritti umani:

"I am disturbed by how States abuse laws on Internet access. I am concerned that surveillance programmes are becoming too aggressive. I understand that national security and criminal activity may justify some exceptional and narrowly tailored use of surveillance, but that is all the more reason to safeguard human rights and fundamental freedoms. Some argue that they need to curtail freedoms to preserve order. I say they need to protect freedom, or they will undermine order."[17]

È evidente come il commento di cui sopra sottolinea il bisogno, sempre più avvertito, di trovare un necessario bilanciamento tra la libertà degli utenti e la loro sicurezza sulla Rete che può essere garantito soltanto da un sistema liberal-democratico votato ad una efficace manutenzione e promozione dei diritti e delle libertà fondamentali.

A ciò si aggiunge la necessità di attuare una disciplina antimonopolistica internazionale che ha toccato lo stesso strumento di Internet la cui applicazione è volta a garantire una più vasta e leale concorrenza tra i grandi gruppi economici che detengono le infrastrutture di accesso alla Rete e che esercitano un rilevante potere nel mercato di riferimento.

---

[16] Cfr. A. PUTINI, *Al di là di Internet: fra recupero e dissoluzione della democrazia*, in Rivista Quadrimestrale di Scienze Storiche e Sociali, Vol. 2, 2013.
[17] Cfr. UN SECRETARY-GENERAL, *Curtailing freedom does not preserve order, but undermines it*, trascrizione del video-messaggio della Fourth Annual Freedom On-line Coalition Conference: Free and Secure Internet for All, Tallinn, Estonia, 29 Aprile 2014.

La dimensione politica, in questo senso, avrebbe dovuto svilupparsi grazie all'influsso di un nuovo tipo di cultura e, proprio Internet, avrebbe dovuto appianare la frattura tra il mercato e le esigenze di democrazia.

Non vi è dubbio che l'opportunità di ricorrere a simili tecniche di controllo e di gestione dei dati – quando le stesse appaiono funzionali a garantire un uso efficiente delle risorse e ad ottimizzare la qualità complessiva della trasmissione dei dati e delle informazioni – permette un buon funzionamento della Rete e forme di controllo della congestione del traffico degli utenti, rendendosi indispensabili per evitare la commissione di illeciti e la diffusione di contenuti illegali *on-line*. Da qui la necessità di ricorrere, da un lato, a regole idonee e controlli efficaci per evitare la concentrazione del potere a vantaggio di pochi gruppi economici monopolistici e, dall'altro, di configurare l'accesso ad Internet secondo i principi di un "servizio universale", ovvero come un vero e proprio diritto sociale, al pari di altre prestazioni pubbliche che, anzi, deve essere incentivato dall'intervento delle autorità pubbliche.

Il problema, dunque, diviene quello di trovare un punto di equilibrio tra l'interesse alla condivisione collettiva dei dati e delle informazioni e il diritto alla loro commercializzazione dal momento che questi vengono raccolti e utilizzati dai fornitori di accesso ad Internet sulla base delle attività che gli stessi utenti compiono sulla Rete.

Questa evoluzione richiede nuovi strumenti capaci di adattarsi alla nuova architettura di Internet, ponendo una serie di problemi relativi alla sua regolamentazione in quanto, dopo una prima fase caratterizzata da una "libertà assoluta" degli utenti, si rende necessaria una *governance* di Internet che, tradizionalmente, era stata concepita come una Rete *"senza testa"* della quale nessuno poteva rivendicarne la direzione o la gestione in maniera arbitraria.

Considerare Internet una sorta di "*prateria senza norme"*, senza limiti e senza regole, porterebbe, infatti, ad una serie di problemi che inevitabilmente ricadrebbero sui suoi utilizzatori.

Tra l'altro, la circostanza che, in alcuni casi, le informazioni che vengono pubblicate su alcuni siti Internet risultano fortemente offensive e diffamatorie per la dignità e l'onore di individui o di determinati gruppi sociali, comporta che la Rete venga sfruttata anche come strumento per la commissione di illeciti lesivi dei diritti e delle

libertà fondamentali, per la di diffusione di materiale pornografico e per la commissione di una varietà di reati da parte di organizzazioni criminali o terroristiche[18].

Le vecchie categorie giuridiche – frutto di una cultura prevalentemente classica sotto il profilo giuridico ed economico – non riescono più a rappresentare i nuovi fenomeni e a regolarli e gli strumenti fino ad oggi utilizzati risultano assolutamente obsoleti e non adeguati.

Tuttavia, nonostante le criticità di cui sopra, appare evidente come l'architettura tecnologica dell'infrastruttura globale dell'informazione deve necessariamente poggiare su fondamenta di libertà sui cui non devono esistere barriere all'esercizio del diritto di accesso all'informazione e al diritto di libertà di espressione.

L'uso di una architettura basata su un controllo invasivo delle attività in Rete può rappresentare, certamente, uno strumento che capace di realizzare una forte limitazione degli accessi ma, proprio nella Rete, questi ostacoli possono divenire ancor più pericolosi, in quanto le barriere sono invisibili e possono portare ad una lesione delle libertà fondamentali.

Un ulteriore problema è collegato proprio all'utilizzo dell'anonimato in Rete dal momento che, molto spesso, i soggetti che agiscono su Internet non sono identificabili e il tentativo del legislatore di regolamentare l'utilizzo dell'anonimato *on-line*, adottato dai diversi ordinamenti giuridici, risulta non omogeneo ed estremamente frammentato, caratterizzato da soluzioni differenti a seconda dei valori che il legislatore nazionale ha inteso, di volta in volta, perseguire e tutelare.

Muovendo da queste riflessioni, dunque, si rende necessaria la ricerca di un bilanciamento volto a garantire, da un lato, il rispetto della legge e la tutela dei diritti degli utenti che compiono lecitamente le loro attività *on-line* e, dall'altro, di impedire che una regolamentazione della Rete, basata eccessivamente sul controllo e sulla censura preventiva, possa causare danni indiretti (e non previsti) ai diritti e alle libertà fondamentali[19].

Tra l'altro, la possibilità di inviare messaggi in forma anonima, per certi versi, presenta più elementi positivi che negativi in quanto permette agli utenti di esprimere il proprio parere e le proprie idee senza il pericolo di rappresaglie, ponendoli al riparo

[18] Sul punto, si segnala la recente proposta di regolamento del Parlamento europeo e del Consiglio relativo alla prevenzione della diffusione di contenuti terroristici *on-line*, in https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:52018PC0640&from=EN

[19] Sul problema della *private* e *collateral censorship* si veda, cfr. M. BASSINI, *Fundamental rights and private enforcement in the digital age*, European Law Journal, 2019.

dai rischi di intimidazione e di stigmatizzazione propri del mondo reale. Tuttavia, l'altra faccia della medaglia concessa dallo schermo dell'anonimato può consistere nell'utilizzo di tale strumento per realizzare la commissione di illeciti, di diffamazione a basso costo, di incitazione all'odio razziale e ideologico (c.d. *hate speech*)[20].

D'altro canto, non è la tecnologia a costituire di per sé un pericolo – considerata al pari di una pistola che, in quanto pericolosa, deve essere appositamente conservata nella sua apposita custodia – bensì è l'utilizzo che se ne potrebbe fare dal momento che, accanto agli indubbi benefici per gli individui e la comunità, essa può anche costituire la fonte di nuove minacce e rischi per l'esercizio dei diritti e delle libertà fondamentali.

Occorre, dunque, che il diritto valuti la realtà tecnologica e stabilisca quali dei suoi usi e obiettivi vadano considerati antigiuridici alla luce della tutela dei diritti fondamentali: stabilire il limite che si può concedere ad un soggetto di restare anonimo significa, infatti, garantire l'esercizio di un diritto fondamentale a chi lo vuole attuare secondo principi di legalità e nel pieno rispetto dell'esercizio dei diritti altrui e, contemporaneamente, tutelare il soggetto nei confronti di coloro che possono impiegare lo stesso diritto come un'arma verso gli altri.

Ne consegue che, oggi, anche se Internet conserva tutte le sue potenzialità in termini comunicativi, siamo di fronte a tre fenomeni che hanno contribuito a reindirizzare le sue prerogative originarie: la concentrazione del potere, sotto forma di controllo dell'informazione e di maggiore sorveglianza di quanto gli utenti svolgono sulla Rete, esercitata dai grandi gruppi aziendali sorti dalla *net economy* (lo strapotere dei motori di ricerca come Google o l'enorme potere di controllo dei *social networks* come Facebook), l'utilizzo commerciale, ludico e sociale della Rete da parte degli utenti; la frammentazione dell'interesse collettivo, che ha creato delle "camere di risonanza", moltiplicando gli interessi e gli spazi di conflitto.

2. Anonimato, libertà di informazione e tutela della personalità in Rete.

A fronte delle precedenti considerazioni introduttive, dobbiamo ora soffermare la nostra indagine sulla questione dell'anonimato *on-line* come strumento di esercizio delle libertà di espressione dal momento che l'utilizzo di tale strumento investe temi e

[20] Cfr. G. RESTA, *L'anonimato in Internet*, in Diritti e libertà in internet (a cura di) T. E. FROSINI, O. POLLICINO, M. BASSINI, Mondadori Education, Milano, 2017.

sfide che, nel corso degli ultimi anni, i governi nazionali hanno affrontato difformemente.

Il diverso approccio degli ordinamenti giuridici ci consente di esaminare la relazione tra *autorità* e *libertà* e tra *diritti individuali* ed *esigenze collettive* dal momento che l'utilizzo di tecniche di anonimato (o di pseudonimizzazione) sulla Rete permette di esprimere liberamente la propria opinione e, di converso, di tutelare i diritti e le libertà fondamentali ad essa sottesa.

Il dibattito riguardo all'anonimato *on-line*, infatti, non risulta circoscritto, come descritto in precedenza, al solo scenario economico o alle fasi dell'evoluzione di Internet, ma anche alla politica e all'orientamento dei diversi attori pubblici (nazionali e internazionali) che sono coinvolti, direttamente, nel controllo o nel blocco della pubblicazione di determinati contenuti sulla Rete.

Tale censura può essere effettuata dai governi nazionali, ma anche da società private su richiesta di enti governativi e dalle autorità di controllo internazionale, variando da paese a paese[21].

L'avvento di un nuovo mezzo di comunicazione come Internet riapre, inevitabilmente, il discorso sulla libertà di manifestazione del pensiero e del suo valore nel quadro dei principi costituzionali e, proprio il tema dell'anonimato, appare particolarmente rilevante nel tentativo di conciliare lo sviluppo tecnologico e le categorie giuridico-culturali fin qui elaborate dagli ordinamenti liberali e democratici[22].

In effetti, l'affermazione di Internet come strumento principale nella comunicazione a livello globale – in quanto basata sulla velocità dello scambio dei dati e delle informazioni – viene considerata dai governi nazionali come una possibile minaccia alla loro posizione di potere, con la conseguenza che, soprattutto nei regimi autoritari, si registra una tendenza nel controllare e nel regolamentare l'accesso ad Internet[23].

[21] Le diverse libertà vengono oggi esercitate attraverso un unico mezzo che è la Rete, ma ci sono Paesi illiberali che hanno costruito barriere architettoniche per evitare l'accesso a parte della rete globale, cancellando parole, nomi e frasi chiavi dai motori di ricerca, oppure violando la *privacy* dei cittadini. Questo però conferma la vocazione liberale di Internet e la paura che di questa libertà globale mostrano di avere quei Paesi intolleranti alla tecnologia perché vista come una minaccia al loro potere assoluto. Sul punto, cfr. T. E. Frosini, *Il diritto di accesso ad Internet*, in T. E. FROSINI, O. POLLICINO, M. BASSINI (a cura di), *Diritti e libertà in internet*, Mondadori Education, Milano, 2017.

[22] Sul punto, cfr. M. MANETTI, *Libertà di pensiero e anonimato in Rete*, 2016.

[23] Cfr. E. PFÖSTL, *Sicurezza e libertà fondamentali*, Editrice Apes, 2008.

A riguardo, David Kaye, relatore speciale per la libertà di espressione, nel 2015, in occasione della riunione del Consiglio delle Nazioni Unite sui diritti Umani, sottolineava la necessità di garantire la tutela dell'anonimato in Rete al fine di consentire il pieno esercizio della libertà di espressione e di opinione:

"Encryption and anonymity, today's leading vehicles for on-line security, provide individuals with a means to protect their privacy, empowering them to browse, read, develop and share opinions and information without interference and enabling journalists, civil society organizations, members of ethnic or religious groups, those persecuted because of their sexual orientation or gender identity, activists, scholars, artists and others to exercise the rights to freedom of opinion and expression."[24]

La differenza tra il diritto di detenere un'opinione e il diritto di esprimerla, stabilisce uno spazio personale in cui un soggetto decide di esplorare le proprie idee e di formulare le sue convinzioni che non dovrebbero essere violate dai governi nazionali in nome della sicurezza e dell'ordine pubblico. L'utilizzo di tecniche di crittografia e dell'anonimato permette di preservare questo spazio, mentre una loro eccessiva regolamentazione "may interfere with the ability of individuals to hold opinions"[25].

Tuttavia, la volontà di un utente di non mostrare la propria identità o il proprio nome non può essere esercitata in maniera incondizionata perché ciò risulta strettamente connaturato all'esercizio dei diritti della propria personalità: non si può rinunciare totalmente alla propria identità personale che rimane, in ogni caso, un diritto assoluto, inviolabile e indisponibile[26].

---

[24] Cfr. UNITED NATIONS (DAVID KAYE, SPECIAL RAPPORTEUR), 22/05/2015, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, Human Rights Council, 29th Session, in https://www.justsecurity.org/wp-content/uploads/2015/06/Kaye-HRC-Report-Encryption-Anonymity.pdf

[25] Ibidem.

[26] In merito, cfr. Cass. Civ., Sez. I, 22 giugno 1985, n. 3769 in cui i giudici di merito si sono riferiti alla figura soggettiva dell'identità personale ritenendo meritevole di tutela giuridica il diritto alla verità di sé stessi nell'ambito della collettività. Risulta, dunque, con chiarezza la differenza con il diritto alla riservatezza: il diritto all'identità personale è "(...) relativo alla tutela dell'immagine pubblica della persona, o comunque, dell'immagine di sé che il soggetto intende proiettare nel mercato delle relazioni sociali (...) il diritto alla riservatezza attiene alla protezione di una sfera intangibile di intimità e riserbo dell'individui, da mettere al riparo da intrusioni altrui consistendo, quest'ultimo, in una sorta di *ius excludendi alios* rispetto a fatti e circostanza che i terzi non hanno diritto di conoscere". Sul punto, cfr. R. PANETTA, *Libera circolazione e protezione dei dati personali*, Giuffrè, Milano, 2006.

Il diritto all'identità personale rappresenta una formula riassuntiva che va oltre l'esigenza estrinseca del potere pubblico (per motivi di polizia o tributari) di identificare un soggetto. L'identità personale costituisce un "bene sostanziale", inteso come una corretta raffigurazione pubblica della propria personalità, indipendentemente dalla condizione personale e sociale e dai pregi e dai difetti dell'individuo[27].

Si rende necessario, dunque, stabilire il limite che si può concedere ad un soggetto di restare anonimo, garantendo l'esercizio di tale diritto fondamentale nel rispetto della legalità e dell'esercizio dei diritti da parte degli altri consociati.

Il diritto all'identità personale, così definito, assurge a livello di diritto fondamentale per il suo stretto legame con gli altri valori costituzionali della dignità personale e sociale, dell'uguaglianza e del libero sviluppo della personalità (artt. 2 e 3 della Costituzione), nonché quale chiarimento del più generale principio di inviolabilità della libertà personale (art. 13 Cost.) e del diritto alla libertà di espressione (art. 21 Cost.).

In altre parole, il diritto all'identità personale, inteso come diritto di essere sé stessi e di non subire illegittime ingerenze nella manifestazione pubblica della propria individualità, sembra presiedere ad un interesse simmetrico, opposto al diritto alla riservatezza, inteso, al contrario, come il diritto a che determinate informazioni personali non possano circolare liberamente[28].

A ciò risulta strettamente collegato il problema del furto di identità in ambito digitale (c.d. *identity theft*) e del relativo interesse del soggetto, vittima dell'illecito, a non vedere modificato o comunque alterato il proprio patrimonio intellettuale, ideologico, etico e professionale[29].

Negli ultimi anni, il fenomeno dei furti di identità si è accentuato anche grazie all'utilizzo delle nuove tecnologie di *deepfake*[30], ovvero tramite l'utilizzo di foto, vi-

[27] In questo senso il rilievo giuridico dell'identità personale consiste nell'insieme dei segni distintivi di una persona quali il nome, le caratteristiche somatiche, l'indirizzo di residenza e in tutto ciò che può rendere quella persona identificabile. Cfr. G. PINO, *L'identità personale*, in S. RODOTÀ e M. TALLACCHINI (a cura di), *Ambito e fonti del biodiritto*, Giuffrè Editore, 2010.

[28] Sul punto, cfr. A. PACE, *Problematica delle libertà costituzionali. Parte generale. Introduzione allo studio dei diritti costituzionali*, CEDAM, 2003.

[29] In Cass. Civ., 7.2.1996, n. 978, in Corr. giur., 1996.

[30] La parola *deepfake* è un neologismo nato dalla fusione dei termini *"fake"* (falso) e *"deep learning*", una particolare tecnologia di Intelligenza Artificiale. Le tecniche usate dai *deepfake* sono simili a quelle delle varie applicazioni con cui è possibile modificare la morfologia del volto, a invecchiarlo, a fargli

deo e audio creati appositamente grazie all'impiego di *software* di Intelligenza Artificiale che, partendo da contenuti reali (come immagini e audio) sono in grado di modificare o di ricreare, in modo estremamente realistico, le caratteristiche e i movimenti di un volto o di un corpo e di imitare fedelmente una determinata voce.

Si tratta di una forma particolarmente grave di furto di identità dal momento che la persona, vittima di un *deepfak*e, a sua insaputa non solo subisce una perdita di controllo sulla sua immagine, ma viene privata anche del controllo sulle sue idee e sui suoi pensieri che possono essere travisati e alterati in base ai discorsi e ai comportamenti falsi che vengono espressi nei video.

Le persone vittime di *deepfake* potrebbero, inoltre, essere rappresentate in luoghi o contesti o con persone che non hanno mai frequentato (o che non frequenterebbero mai) oppure in situazioni che potrebbero apparire estremamente compromettenti e imbarazzanti.

In sostanza, quindi, una tecnologia di *deepfake* è in grado di ricostruire contesti e situazioni mai effettivamente avvenuti e, se ciò non è voluto dai diretti interessati, può rivelarsi una grave minaccia per la riservatezza e la dignità delle persone coinvolte in quanto immediatamente lesiva di una corretta rappresentazione della loro personalità[31].

A ben guardare, però, si tratta di due facce della stessa medaglia dal momento che, proprio per quanto concerne il diritto all'identità personale, la riservatezza gioca una funzione ad essa strumentale: se l'identità personale consiste nella possibilità di professare e di rivendicare *ciò che si è*, in assenza di possibili interferenze esterne, la riservatezza garantisce che l'individuo possa sviluppare e mantenere tale identità al riparo da eventuali discriminazioni o lesioni.

La Rete offre la possibilità di comunicare in anonimato, sia secondo le forme previste dall'art. 15 della Costituzione, sia in relazione agli altri tipi di manifestazione del pensiero offerti da Internet, al punto che si è posto l'interrogativo se l'utilizzo delle tecniche di anonimato consista in un vero e proprio abuso o, al contrario, possa rap-

cambiare sesso e altro ancora. La materia di partenza sono sempre i veri volti, i veri corpi e le vere voci delle persone, trasformati però in "falsi" digitali.

[31] Per maggiori approfondimenti sulle attività illecite legate all'utilizzo della tecnologia *deepfake* si rimanda a https://www.garanteprivacy.it/temi/intelligenza-artificiale/deepfake.

presentare uno strumento che deve essere in qualche modo protetto in quanto strumentale all'esercizio della libertà di espressione (e, in questo secondo caso, si pone la questione se, oltre alla tutela, possa anche essere oggetto di una qualche limitazione[32]).

Ragionando della Rete, infatti, non si può ignorare come essa impatti, a diverso titolo e in maniera tangibile, sui diritti fondamentali, ora promuovendoli, ora collocandoli in una situazione di pericolo e, pertanto, risulta necessario realizzare un equo contemperamento tra i diversi diritti individuali inviolabili e, in alcuni casi, contrapposti.

Si tratta di un equilibrio assai delicato, avendo riguardo al rango degli interessi in gioco e che, sull'onda del contesto storico-politico, ha portato a diverse soluzioni regolamentari[33].

Tra l'altro, la possibilità non solo di raccogliere dati e informazioni, ma anche di diffonderli, rappresenta l'effetto più visibile di Internet nella vita quotidiana delle persone.

Senza dubbio, l'utilizzo massiccio del *web* – come strumento che facilita l'ingresso nel circuito dell'informazione di soggetti che non svolgono l'attività di informazione come professione e che permette loro di diffondere *attivamente* il proprio pensiero – ha modificato ed esteso ulteriormente il diritto alla libertà di espressione e di manifestazione del pensiero, ma con conseguenze non sempre positive per il diritto all'informazione.

La stessa Carta dei diritti di Internet, licenziata il 14 luglio 2016 dalla Commissione per i diritti e i doveri relativi ad Internet, all'art. 10 prevede che ogni persona "può accedere alla rete e comunicare elettronicamente usando strumenti anche di natura tecnica che proteggano l'anonimato ed evitino la raccolta di dati personali, in particolare per esercitare le libertà civili e politiche senza subire discriminazioni o censure"[34].

È evidente, pertanto, come il *web* è per antonomasia il luogo deputato al dibattito sociale e politico e come l'utilizzo dell'anonimato abbia un valore emblematico per l'esercizio della libertà di pensiero. Lo snodo fondamentale, tuttavia, è che gli Stati diano regole chiare sull'utilizzo di tale strumento.

---

[32] Suggerendo, in tal modo, forme di "anonimato protetto". Cfr. P. COSTANZO, *Profili costituzionali di Internet*, in E. TOSI (a cura di), *I problemi giuridici di Internet*, I vol., III ed., Milano, 2003.

[33] Si pensi, esemplarmente, alla Dichiarazione dei diritti fondamentali in Internet del 2016 che tutela espressamente il diritto all'anonimato.

[34] In http://www.interlex.it/2testi/altridocumenti/dich-diritti-internet.pdf

A titolo esemplificativo, tra i temi di maggiore attualità connessi all'utilizzo dell'anonimato in Rete, si annovera quello delle c.d. *"fake news"*, cioè delle notizie interamente o parzialmente false, prodotte da pratiche di mala-informazione.

In Italia, una delle proposte in tema di *fake news* prevedeva l'introduzione di un divieto assoluto di anonimato in Rete, imponendo ai gestori delle piattaforme, le cui attività si sostanziavano nella pubblicazione e diffusione di informazioni, di creare un sistema finalizzato ad impedire a chi non fosse registrato con certezza di identità di immettere qualsivoglia contenuto *on-line*[35].

A ben vedere, il fenomeno delle *fake news* non è recente, ma nasce con il c.d. *"yellow journalism"*[36] di Joseph Pulitzer (1847-1911), celebre editore e giornalista (al quale fu dedicato, più tardi, il Premio Pulitzer[37]) il quale, al fine di risollevare le sorti del quotidiano *The New York World*, che si trovava in bancarotta, puntò alla pubblicazione di servizi scandalosi e sensazionalistici, facendo leva sulla curiosità del pubblico, nonché alla pubblicazione di annunci di lavoro e di richieste di ogni tipo, così da puntare alla grande platea di immigrati che arrivavano negli Stati Uniti in cerca di nuove opportunità di impiego.

Durante la guerra ispano-americana del 1898, Pulitzer, per sconfiggere il *New York Times*, il principale quotidiano antagonista del *World*, dette spazio anche a vere e proprie *fake news*, gonfiando le notizie del conflitto con la Spagna e dipingendo a forti tinte le crudeltà dei soldati spagnoli ai danni della popolazione inerme di Cuba[38].

Pertanto, le *fake news* non nascono grazie all'avvento di Internet, ma con la Rete diventano virali e chi ne viene a conoscenza, persuaso anche dalle condivisioni che le

[35] Nella stessa proposta si chiedeva che venisse sancito l'obbligo di rintracciabilità degli utenti, ovvero che chiunque interagisse *on-line* non potesse avvalersi di una forma qualsiasi di anonimato e, non da ultimo, un allineamento dell'Italia alle norme europee per l'applicazione del diritto all'oblio. Il testo della proposta è consultabile in https://www.camera.it/leg17/126?idDocumento=4692

[36] Tale definizione deriva, forse, da un popolare fumetto pubblicato sul *New York World* che vedeva protagonista un giovanotto vestito con un camicione da notte di colore giallo sul quale erano trascritte le frasi che pronunciava.

[37] Sul rapporto fra giornalismo e *fake news*, cfr. E. SCARPANTI, *Bufale: Post-verità, linguaggio e fascinazione dai falsi storici al web*, Libreriauniversitaria.it Edizioni, Padova, 2018.

[38] Negli Stati Uniti d'America le *fake news* sono tutelate dal Primo Emendamento della Costituzione Americana secondo il paradigma del *free marketplace of ideas* dal momento che non esiste *"no such thing as a false idea"* (US Supreme COURT, GERTZ V. WELCH, 1974) e che i destinatari dell'informazione (ottimisticamente) dovrebbero avere tutti gli strumenti necessari distinguere le notizie vere da quelle che non sono convincenti o false. Ciò costituisce una espressione di piena fiducia nella capacità di autocorrezione del mercato dell'informazione. Sul punto, cfr. O. POLLICINO, *Fake News, Internet and Metaphors (To Be Handled Carefully)*, MediaLaws, 2018.

stesse hanno ricevuto da altri utenti ignari, le ritiene attendibili e, a sua volta, le diffonde[39].

Il rischio è che Internet, da strumento di informazione, si tramuti in uno strumento privilegiato di disinformazione, con effetti nocivi sulla libertà di espressione e di manifestazione del pensiero e con conseguenze negative sul mondo reale, tale da accentuare in misura esponenziale gli effetti prodotti da una qualsiasi falsa informazione messa in Rete[40]: la tutela di un bene piuttosto che un altro può comportare la compressione di un diverso diritto fondamentale con la conseguenza che l'esigenza di assicurare la diffusione di notizie vere si scontra con la garanzia del pluralismo dell'informazione di cui Internet rappresenta la massima espressione[41].

Il tema non è semplice e si presenta assai delicato.

La disinformazione mette in dubbio lo scopo e l'efficacia di una corretta informazione e cede il passo ad un "populismo emotivo", non consentendo più di discernere il vero dal falso.

Si rende, dunque, preliminarmente necessario migliorare la qualità dell'informazione *on-line* in quanto essa una ha rilevanza sociale e si pone come strumento essenziale nell'interesse della società nel suo insieme:

---

[39] Ciò comporta un ulteriore problema collegato al c.d. *"effetto di rete"* dal momento che gli intermediari, in particolare i motori di ricerca e le piattaforme partecipative ricche di contenuti e connessioni, hanno interesse ad attrarre e trattenere gli utenti i quali continueranno ad utilizzare i servizi offerti nella misura in cui quei servizi rispondano ai loro bisogni informativi e relazionali. Il tentativo di trattenere gli utenti porterà gli intermediari a proporre soltanto i contenuti loro graditi, vicini alle preferenze e alle ideologie degli utenti, realizzando una *"filter bubble"*, vale a dire un ambiente informativo che ne riproduce gli interessi e le opinioni e che non propone stimoli critici. Sul punto, cfr. G. SARTOR, *La responsabilità degli intermediari e i diritti fondamentali*, in T. E. FROSINI, O. POLLICINO, M. BASSINI (a cura di), *Diritti e libertà in internet*, Mondadori Education, Milano, 2017.

[40] Cfr. G. PITRUZZELLA, *La libertà di informazione nell'era di Internet*, in G. PITRUZZELLA, O. POLLICINO, S. QUINTARELLI (a cura di), *Parole e potere. Libertà di espressione, hate speech e fake news*, Egea Editore, 2017.

[41] Ci si deve domandare se la natura globale della nuova tecnologia digitale – e il fatto che chiunque può creare e diffondere messaggi e informazioni – consenta davvero un confronto delle idee e la verifica delle fonti delle notizie o, piuttosto, amplifichi in modo esponenziale e potenzialmente dannoso l'impatto delle notizie false. La libertà di espressione non è senza limiti ma, ai sensi dell'art. 10 della Convenzione Europea dei Diritti Umani, il suo esercizio comporta oneri e responsabilità che appaiono particolarmente giustificati quando il veicolo delle opinioni espresse è quello potente e principale di Internet. Nella giurisprudenza della Corte europea dei diritti umani, in K.U. C. FINLANDIA, 2 dicembre 2008, DELFI AS C. ESTONIA, 16 giugno 2015; PIHL C. SVEZIA, 9 marzo 2017, MAGYAR JETI ZRT C. UNGHERIA, 4 dicembre 2018.

"A functioning press and democracy require criticism, transparency, and consequences for journalistic mistakes. They also require that we are able to collectively distinguish them from lies and deception. Otherwise, real information will be painted as fake, and manufactured (rubbish) gets presented as fact."[42]

Mentre per le testate giornalistiche (tradizionali e digitali) il problema va affrontato in termini diversi – dal momento che i giornalisti professionisti e gli imprenditori del settore sono tenuti al rispetto delle regole deontologiche concernenti la verità dell'informazione e il diritto di cronaca – la questione viene avvertita con maggiore sensibilità per quanto concerne la diffusione di informazioni *on-line*, soprattutto quando le notizie vengono veicolate dietro lo schermo protettivo dell'anonimato, richiedendosi, nel settore dell'informazione e della comunicazione digitale, l'attivazione di risposte "immunitarie" immediate.

Così, negli ultimi anni, sono iniziati a proliferare vere e proprie attività di verifica delle notizie in Rete, di *fact-checking* e di *debunking*, volte ad appurare la veridicità o la falsità di un determinato contenuto *on-line* e finalizzate a smascherare definitivamente le *fake news* e i suoi autori celati dietro *alias* o nomi falsi.

Le stesse piattaforme, in alcuni casi, hanno volontariamente posto in essere attività di *fact-checking* per "smascherare" le notizie false, invitando al contempo gli utenti a segnalare e a denunciare i contenuti ritenuti non affidabili in modo che questi ultimi possano essere etichettati *(flagged)* e rimossi celermente[43].

È chiaro come si tratti di un argomento sensibile in quanto tocca direttamente la questione della libertà di manifestazione del pensiero e della censura sul *web* e, soprattutto, perché la diffusione di notizie false sarebbe teoricamente vietata dai principi costituzionali europei all'art. 10 della Convenzione Europea dei Diritti Umani e all'art. 11 della Carta dei Diritti Fondamentali dell'Unione Europea, stabilendosi un diritto ad essere informati inteso però come "social interest to avoid disinformation"[44].

[42] Cfr. C. SILVERMAN, (2018), *I Helped Popularize The Term Fake News And Now I Cringe Every Time I Hear It*, BuzzFeed, in https://www.buzzfeed.com/craigsilverman/i-helped-popularize-the-term-fake-news-and-now-i-cringe

[43] Si tratta di una vera e propria forma di auto-responsabilizzazione delle piattaforme, finalizzata ad assicurare l'accesso ad informazioni vere e verificate.

[44] M. BASSINI, *Fundamental rights and private enforcement in the digital age*, European Law Journal, 2019.

Tuttavia, mentre questi diritti vengono tutelati attraverso un'attività di bilanciamento (che avviene *ex-ante* da parte del legislatore ed *ex-post* da parte dei giudici), non esiste per i *provider* un obbligo generalizzato di identificazione degli utenti che veicolano tali contenuti in Rete[45]. Sotto questo profilo, anzi, lasciano perplessi i tentativi di auto-regolamentazione e di co-regolamentazione proposti recentemente dal legislatore europeo per i grandi colossi del *web* che sembrano corrispondere più a forme censorie dei contenuti generati dagli utenti e che potrebbero prestarsi ad uno esercizio distorto della libertà dell'informazione *on-line*[46].

Altrettanto dubbie appaiono le proposte di una limitazione al divieto di diffusione di notizie non riconducibili ad un autore ben indentificato che potrebbero non soltanto ridurre il pluralismo delle fonti informative, ma anche scoraggiare la diffusione di notizie e di idee alternative con la conseguenza di una rinuncia allo spirito critico, alla polarizzazione delle opinioni e alla omogeneità dei gruppi di discussione.

Andrebbero, allora, rafforzati gli strumenti per combattere la diffusione di idee e notizie lesive dei valori costituzionali e adattare detti strumenti alle specificità della comunicazione *on-line* (incluso l'utilizzo delle tecniche di anonimato) dal momento che l'idea di affidare a soggetti pubblici e privati il compito di vagliare la verità o l'attendibilità di una notizia riflette essenzialmente una logica autoritaria che, almeno in teoria, dovrebbe rimanere del tutto estranea ai modelli liberal-democratici del diritto alla manifestazione del pensiero[47].

Si aggiunga, tra l'altro, che la conformazione naturale di Internet sostiene spesso l'anonimato e, di riflesso, comporta l'impunità per gli autori di questi atti per via, soprattutto, delle considerevoli difficoltà di stabilire la paternità delle idee e dei discorsi,

---

[45] A riguardo, l'art. 15 della Direttiva 2000/31/CE sul commercio elettronico prevede che "(...) gli Stati membri non impongono ai prestatori un obbligo generale di sorveglianza sulle informazioni che trasmettono o, memorizzano né un obbligo generale di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite". Si veda https://eur-lex.europa.eu/legal-content/IT/ALL/?uri=CELEX%3A32000L0031

[46] Un esempio è dato dal *Network Enforcement Act* tedesco che ha rafforzato la protezione contro i contenuti illegali pubblicati sui *social networks* richiedendo espressamente agli *Internet Service Providers* di cooperare per rimuovere o bloccare l'accesso a contenuti manifestamente illegali in un tempo massimo di 24 ore, prevedendosi multe salate in caso di non ottemperanza; o dall'HADOPI francese che, a seguito di segnalazione di un illecito, può avviare una procedura di "tre avvertimenti" per l'applicazione delle leggi a tutela del diritto d'autore, vietando agli *Internet providers* di fornire l'accesso alla Rete agli abbonati inseriti nella lista nera.

[47] Tra le soluzioni prospettare per risolvere tale conflitto di valori si segnala quella che ha proposto un "anonimato parziale", vale a dire l'obbligo dei *provider* di comunicare l'identità dell'utente quando i contenuti pubblicati si rivelino lesivi. Cfr. G. E. VIGEVANI, *Anonimato, responsabilità e trasparenza nel quadro costituzionale Italiano,* Osservatorio Costituzionale, 2014.

proprio in virtù di garantire l'esigenza di promuovere la libertà di espressione e la libera circolazione delle informazioni[48].

Emerge, pertanto, la necessità di comprendere se l'utilizzo dell'anonimato per l'esercizio del diritto alla libera manifestazione del pensiero in Rete – e che, in alcuni casi, può rivelarsi offensiva e lesiva dell'altrui decoro e onore – possa dirsi scriminato e a quali condizioni.

3. Anonimato e responsabilità degli *Internet Service Providers*.

Alla luce di quanto sopra, risulta evidente la necessità di individuare un punto di equilibrio tra l'esigenza di offrire rimedi effettivi alle violazioni più gravi che sono perpetrate nella Rete[49] e quella, contrapposta, di garantire la tutela dei diritti e delle libertà fondamentali, con riguardo soprattutto all'esercizio della libertà di espressione *on-line* che, sulla base dell'effettiva somiglianza tra alcune manifestazioni del pensiero tradizionali, appare tendenzialmente analoga a quella del mondo "reale"[50].

Risulta evidente come i *providers* contribuiscano all'esercizio dei valori costituzionali semplicemente rimanendo "neutrali"[51], vale a dire consentendo a chiunque di accedere alla Rete e trasferire su di essa qualsiasi contenuto.

Da qui l'interrogativo sull'opportunità di imporre agli intermediari una serie di obblighi e di responsabilità sulla liceità dei contenuti pubblicati da soggetti terzi *on-line*.

[48] La vocazione naturale di Internet è l'extra-territorialità, in quanto esso travalica i confini degli Stati nazionali, supera le barriere doganali, elimina le differenze culturali tra i popoli, realizzando un modello olistico di libertà. Sul punto, cfr. T.E. Frosini, *Il diritto di accesso a Internet,* in T. E. FROSINI, O. POLLICINO, M. BASSINI (a cura di), Diritti e libertà in internet, Mondadori Education, Milano, 2017.

[49] Negli ultimi anni il termine *serious crimes* ha acquisito una sempre maggiore importanza nella politica dell'Unione Europea in materia di sicurezza interna, ma la definizione di "reato grave" varia notevolmente tra gli Stati Membri ed è stata inclusa per definire semplicemente l'ambito di applicazione delle disposizioni di cooperazione internazionale Si veda, a riguardo https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:111:0011:0014:EN:PDF

[50] Cfr. Sul punto, cfr. C. MELZI e G. E. VIGEVANI, *Lo statuto dell'informazione su Internet,* in T. E. FROSINI, O. POLLICINO, M. BASSINI (a cura di), Diritti e libertà in internet, Mondadori Education, Milano, 2017.

[51] In senso opposto, si segnalano le iniziative di *deplatforming* da parte di Facebook e Twitter che hanno bloccato gli account dell'ex presidente degli Stati Uniti d'America Donald Trump in seguito a dei post che istigavano alla violenza e alla insurrezione relativamente al risultato delle nuove elezioni, in aperta violazione dei *terms of service* delle piattaforme, che sono sfociati nell'assalto di Capitol Hill, sede del Congresso americano.

A riguardo, il panorama comparatistico evidenzia le diverse sensibilità degli ordinamenti giuridici in ordine alle politiche di promozione della Rete al fine di migliorare le condizioni di esercizio delle libertà "classiche" e, di converso, quello di contrastare la commissione di reati da parte degli utenti e degli stessi operatori della Rete.

In effetti, le posizioni della dottrina e della giurisprudenza sul tema della regolamentazione delle comunicazioni in forma anonima attraverso Internet hanno sollevato, già dalla nascita della Rete, un acceso dibattito che si presenta, ai nostri giorni, ancora più attuale per lo sviluppo di una nuova stagione della comunicazione digitale interattiva (c.d. *"Web 2.0"*)[52]. L'effetto emancipatore dell'anonimato *on-line* nell'espressione delle proprie idee e opinioni – in assenza di appropriati contrappesi istituzionali – rischia così di determinare una generale irresponsabilità degli autori degli illeciti perpetrati in forma anonima dal momento che, a causa della mancanza di una loro imputazione soggettiva, può tradursi in una "area grigia" di incertezza giuridica[53].

È indubbio che la partecipazione massiva degli utenti nella creazione di contenuti sul *web* ha notevolmente agevolato la diffusione di idee, notizie e informazioni, anche in forma anonima, con la conseguenza di un generale senso di impotenza del legislatore nel contrastare efficacemente la diffusione degli illeciti realizzati nella Rete e la tentazione di introdurre forme sempre più invasive di controllo preventivo o di corresponsabilità degli stessi *providers*, estranee al patrimonio costituzionale degli ordinamenti democratici[54].

L'impossibilità di determinare con precisione gli autori degli illeciti in forma anonima ha posto, dunque, l'attenzione del legislatore sul ruolo degli stessi intermediari – in particolare sugli *host providers* – quali unici soggetti agevolmente identificabili dalla vittima del messaggio lesivo, nonché generalmente dotati di una maggiore solvibilità economica ai fini del risarcimento dei danni patrimoniali e non patrimoniali collegati alla commissione dell'illecito[55].

---

[52] Sul punto, cfr. M. L. MONTAGNANI, *Internet, contenuti illeciti e responsabilità degli intermediari*, Egea, Milano, 2018.

[53] Sul punto, cfr. G. RESTA, *L'anonimato in Internet*, in T. E. FROSINI, O. POLLICINO, M. BASSINI (a cura di), *Diritti e libertà in internet*, Mondadori Education, Milano, 2017.

[54] Spesso i fornitori di contenuti *on-line* optano per l'anonimato e ciò rende economicamente e tecnicamente complesso e onerose rintracciarne l'identità.

[55] Anche nel caso in cui gli autori dell'illecito vengano individuati è spesso difficile per i danneggiati ottenere un risarcimento del danno poiché si tratta di frequente di soggetti che, grazie alla potenzialità offerte dalla Rete, hanno causato danni enormi che non sono in grado di ristorare.

Si è posto così l'interrogativo se il ruolo del gestore del sito *web*, rispetto ai contenuti forniti da terze parti, potesse essere assimilato a quello di un direttore di un giornale, vale a dire ad una forma di responsabilità rafforzata dell'intermediario, oppure a quello di un mero distributore dei messaggi pubblicati sulla piattaforma, con una relativa ridotta responsabilità fino a giungere, in alcuni casi, ad una vera e propria immunità per gli illeciti perpetrati sulla piattaforma.

La responsabilità del *provider* per il fatto illecito degli utenti ha visto, con varietà di argomentazioni e di interpretazioni, diverse posizioni, da quella favorevole ad una sostanziale irresponsabilità dell'intermediario a quella opposta, incline ad accollare a quest'ultimo un obbligo risarcitorio sulla base di criteri certi e oggettivi[56].

Il tema, tuttavia, non riguarda tanto l'imputabilità della condotta antigiuridica direttamente al *provider*, quanto piuttosto il fatto che il servizio offerto in Rete sia stato lo strumento per la commissione dell'illecito da parte degli utilizzatori del servizio[57], comportando una ricostruzione della responsabilità dell'intermediario per fatto altrui o per una omessa vigilanza sulla condotta degli utenti[58]. Se l'utente si è reso responsabile di tali illeciti, si pone il dubbio di come qualificare giuridicamente la condotta dell'*internet provider*, dato che la pubblicazione del materiale è avvenuta tramite il *provider* stesso, in qualunque forma ammessa dalle modalità di funzionamento delle piattaforme.

In altri termini, ci si è chiesti se non fosse opportuno ipotizzare una maggiore responsabilizzazione degli intermediari – soprattutto in riferimento a quei gruppi economici che detengono un monopolio di fatto – anche sulla base dell'aumento delle violazioni commesse sulla Rete e della sempre più stringente esigenza di un intervento immediato per porre fine alle conseguenze negative dell'illecito.

C'è da dire però che un sistema di responsabilità troppo severo, oltre a comportare l'espulsione dal mercato degli operatori meno solidi, spingerebbe quelli rimasti ad un capillare controllo delle informazioni che viaggiano su Internet che, per il timore di

[56] Per uno studio comparato sull'emergere della responsabilità degli intermediari, cfr. T. VERBIEST, G. SPINDLER, G. M. RICCIO, *Study on the Liability of Internet Intermediaries*, 2007, in https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2575069

[57] Cfr. L. NIVARRA, *Responsabilità del provider*, in Digesto delle discipline privatistiche, sezione civile, Aggiornamento II, Torino, 2003.

[58] Sul punto, cfr. F. DI CIOMMO, *Internet, diritti della personalità e responsabilità aquiliana del provider*, in Danno e resp., 1999.

venire coinvolti in azioni risarcitorie, saranno inevitabilmente spinti ad esercitare penetranti poteri di censura preventiva sulla base di un equilibrio tra costi e benefici, arrecando, di converso, un grave pregiudizio alla libertà di espressione e di manifestazione del pensiero espressa *on-line*.

La scelta di un criterio di imputazione piuttosto che di un altro risulta motivata anche da ragioni di tipo *economico* dal momento che, da un lato, parte della dottrina sostiene la necessità di assicurare il massimo impulso possibile allo sviluppo della Rete, non gravando ulteriormente i *providers* che ne garantiscono il corretto funzionamento, degli obblighi relativi al risarcimento del danno[59], e dall'altro, proprio per la potenzialità offensiva di Internet, è necessario non lasciare il danneggiato privo di strumenti di ristoro, anche in assenza di una diretta responsabilità dell'intermediario[60].

Proprio a causa delle criticità sollevate dalla liceità o dall'illiceità del ricorso all'anonimato e delle sfumature delle diverse posizioni dottrinali, l'approccio regolatorio al problema è stato affrontato in maniera difforme sia negli ordinamenti di *common law* (specificamente in Nord America) che in quelli di *civil law* (in particolare nell'Unione Europea).

La responsabilità dei soggetti che concorrono alla violazione dei contenuti generati da terze parti, infatti, è stata definita dal legislatore federale statunitense e da quello comunitario europeo tra il 1996 e il 2000[61] sulla base di un generale ripudio del modello di responsabilità oggettiva dal momento che ciò si sarebbe inevitabilmente tradotto in un disincentivo allo svolgimento delle attività cruciali non solo per la *net economy*, ma per ogni comparto della vita associata espressa sulla Rete[62].

Con riguardo agli Stati Uniti d'America, la responsabilità del *provider* per i contenuti anonimi di terze parti è stata sostanzialmente esclusa per effetto di un modello c.d. "a doppio binario" che ha portato alla cristallizzazione di un insieme di regole che

[59] Per la responsabilità del *provider* si rinvia a P. SANNA, *Il regime di responsabilità dei providers intermediari di servizi nella società dell'informazione*, in Resp. civ. e prev., 2004; A. PIAZZA, *La responsabilità civile dell'Internet Provider*, in Contr. e impr., 2004; G. FACCI, *La responsabilità extracontrattuale dell'Internet Provider*, in Resp. civ. e prev., 2002; L. RUGGIERO, *Individuazione nel ciberspazio del soggetto penalmente responsabile e ruolo dell'Internet Provider*, in Giur. di merito, 2001.
[60] Cfr L. BUGIOLACCHI, *La responsabilità dell'host provider alla luce del D.lgs. 70/03: esegesi di una disciplina dimezzata*, in Responsabilità civile e previdenza, pp. 200 e ss., 2005.
[61] Sulle sfide dell'era digitale del costituzionalismo statunitense e su quello europeo, cfr. O. POLLICINO, *La prospettiva costituzionale sulla libertà di espressione nell'era di Internet*, in MediaLaws, 2018.
[62] Sul punto, cfr. C. CASTRONOVO, *Responsabilità civile*, Milano, 2018.

investono direttamente le imprese poste al centro della diffusione delle informazioni *on-line*.

In estrema sintesi, detto modello si basa, in prima battura, sulla *Section 230* del *Communication Decency Act* (adottato a livello federale nel 1996) quale baluardo della protezione degli intermediari contro la responsabilità per fatto altrui al fine di incoraggiare lo sviluppo della libertà di parola su Internet, garantendo, al contempo, l'esenzione dalla responsabilità sia per il *provider* che per l'utilizzatore dei servizi offerti.

In particolare, il primo comma prevede espressamente che:

"No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[63]

Ne consegue che gli intermediari sono esonerati nella maniera più ampia da qualsiasi tipo di responsabilità di controllare i contenuti immessi in Rete e riconducibili a soggetti terzi, anche per quelli pubblicati in forma nominativa o anonima.

Ciò garantisce una completa immunità per tutti quei servizi intesi a facilitare l'accesso ai contenuti trasmessi da terzi ed eliminare la possibilità di concepire la responsabilità dei *provider* alla stregua di una responsabilità oggettiva, tipica dei direttori dei quotidiani, e di realizzare un controllo, pressoché impossibile, sul materiale pubblicato sulla piattaforma.

Il secondo comma, invece, contiene la c.d. *"clausola del buon samaritano"* e stabilisce che:

"No provider or user of an interactive computer service shall be held liable on account of any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected."[64]

[63] In https://www.law.cornell.edu/uscode/text/47/230
[64] Ibidem.

La disposizione prevede una sorta di *"self regulation"* dell'intermediario il quale sarà incentivato a rimuovere dalla piattaforma quei contenuti manifestamente illeciti senza che ciò possa tradursi in una effettiva lesione alla libertà di espressione tutelata dal Primo Emendamento della Costituzione statunitense[65] che difende il diritto di critica, anche quando espresso in maniera verbalmente aggressiva.

La "clausola del buon samaritano" (*good samaritan duties*) ha così permesso la creazione una cultura basata sulla libertà di manifestazione del pensiero – il diritto al *"free speech"* – che protegge con l'immunità il *provider* che, in buona fede, blocca tutti quei contenuti "osceni, impudichi, lascivi, ripugnanti, eccessivamente violenti, molesti o altrimenti sgradevoli" con la chiara intenzione di proteggere maggiormente tutti i soggetti deboli (e con particolare riguardo alla tutela dei minori).

La diffusa convinzione di garantire una protezione effettiva alla libera manifestazione del pensiero di ciascuno, anche quando ciò risulti fortemente problematico o politicamente inopportuno, trova così riscontro in precise garanzie accordate dalla stessa Costituzione, comprendendo quelle circostanze in cui altri sistemi nazionali limiterebbero viceversa quella libertà. Tuttavia, il sistema statunitense, pur apparentemente estremamente rispettoso della libertà di pensiero e di parola – ossia di qualunque opinione espressa, non importa se politicamente inopportuna, scomoda o lesiva dei sentimenti altrui –, nel corso degli anni, ha saputo limitare (e anche molto pesantemente) quella libertà tutte le volte che ciò è stato ritenuto politicamente necessario[66].

Al *Communication Decency Act*, nel 2000 si è, successivamente, affiancato il Titolo II del *Digital Millennium Copyright Act* che, alla *Section 512*, prevede una più limitata responsabilità del *provider* per gli illeciti di terze parti concernenti la violazione del diritto d'autore.

A riguardo viene stabilito quanto segue:

"A service provider shall not be liable for monetary relief, or (...), for injunctive or other equitable relief, for infringement of copyright by reason of the storage at the

[65] A riguardo, il Primo Emendamento della Costituzione americana stabilisce che "Congress shall make no law respecting an establishment of religion or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances", in https://www.law.cornell.edu/constitution/first_amendment

[66] Si guardi alla recente e contestata cancellazione permanente dell'account Twitter dell'ex presidente degli Stati Uniti d'America Donald Trump a seguito della pubblicazione di alcuni suoi post sulla piattaforma che hanno istigato i c.d. *"proud boys"* ad assaltare la sede del Congresso a Capitol Hill, in https://tg24.sky.it/mondo/2021/01/07/donald-trump-twitter

direction of a user of material that resides on a system or network controlled or operated by or for the service provider, if the service provider

(A)

i. does not have actual knowledge that the material or an activity using the material on the system or network is infringing.

ii. in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent.

iii. or upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material.

(B) does not receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity; and

(C) upon notification of claimed infringement (...), responds expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity."[67]

È, dunque, previsto una sorta di *"safe harbor"* per i fornitori di servizi *on-line* contro la responsabilità per violazione del diritto d'autore a condizione che vengano soddisfatti alcuni specifici requisiti per consentire all'operatore di conoscere con esattezza quali siano i contenuti illeciti oggetto o meno di rimozione.

In particolare, il fornitore dei servizi che intende beneficiare della limitazione di responsabilità sarà tenuto alla rimozione del contenuto abusivo quando abbia maturato una *"actual knowledge"* dell'illecito, vale a dire una conoscenza specifica, autentica ed effettiva della condotta abusiva altrui, obiettivamente manifesta ad una "persona ragionevole"[68].

Il *provider*, anche sulla base di un *simple fact of notice*, dovrà bloccare prontamente l'accesso al materiale (o rimuoverlo speditamente dalla piattaforma) quando riceve la segnalazione di un reclamo per violazione del diritto d'autore da parte del titolare del diritto secondo un sistema di *"notice and take down"* (nota e rimuovi): l'intermediario informa il fornitore del contenuto dell'intimazione a cancellarlo e,

[67] In https://www.law.cornell.edu/uscode/text/17/512

[68] I confini tra *"actual knowledge" e "general knowledge"* sono stati meglio definiti nella sentenza VIACOM INTERNATIONAL INC. V. YOUTUBE INC., in https://cyber.harvard.edu/people/tfisher/cx/2012_Viacom.pdf

quest'ultimo, decide se accettare l'intimazione o contestarla. Il materiale rimane bloccato se il titolare del diritto agisce in giudizio conto il fornitore del contenuto, altrimenti l'intermediario ne ripristina l'accessibilità.

La richiesta di rimozione risponde, quindi, ad una garanzia della procedura a favore del *provider* che dovrà intervenire efficacemente individuando il contenuto oggetto della segnalazione della cui responsabilità sostanziale risponderà però il soggetto terzo che ha pubblicato il contenuto abusivo o fraudolento.

Inoltre, anche per il futuro, l'intermediario sarà tenuto a contrastare la reiterazione dell'illecito sulla propria infrastruttura secondo un meccanismo di *"notice and stay down"*, impedendo in ogni caso il caricamento di quel contenuto illecito senza la necessità di ulteriori notifiche[69].

Questa precisazione è spesso utilizzata per escludere il *safe harbor* per quegli *hosting providers*, i quali svolgono attività, che i giudici ritengono eccedere quella di ruolo automatico e passivo: in particolare perché indicizzano, organizzano e promuovono i materiali caricati dagli utenti proponendoli ad altri navigatori allo scopo di trarre profitto, soprattutto in tema di violazione del diritto d'autore.

Peraltro, la Sezione 512 DMCA ha costituito il modello del *safe harbor* europeo che non si discosta di molto dall'approccio statunitense[70].

In effetti, la direttiva 31 dell'8 giugno 2000 (anche nota come direttiva *e-Commerce*), recepita dal nostro ordinamento con il Decreto Legislativo n. 70 del 9 aprile 2003, si ispira ad un principio analogo a quello che informa l'architettura del DMCA, prevedendo, all'articolo 15, l'esclusione di un obbligo generale di sorveglianza a carico dell'intermediario che non sia a conoscenza dell'illeceità dei contenuti immessi in Rete da soggetti terzi:

"(...) gli Stati membri non impongono ai prestatori un obbligo generale di sorveglianza sulle informazioni che trasmettono o memorizzano né un obbligo generale di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite."[71]

[69] Sul punto, cfr. J.M. URBAN, J. KARAGANIS, B.L. SCHOFIELD, *Notice and Takedown in Everyday practice*, 2016.

[70] La dottrina ha evidenziato la maggior certezza offerta dalle due discipline statunitensi (rispettivamente la Sezione 230 CDA e la Sezione 512 DMCA) rispetto a quella europea, ove si deve tener conto delle circostanze del caso concreto, cfr. R. PETRUSO, *La responsabilità degli intermediari della rete telematica*, Giappichelli, 2019.

[71] In https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32000L0031&from=ET

Tuttavia, la disciplina europea, a differenza di quella statunitense, non distingue le violazioni del diritto d'autore da altri tipi di illiceità, ma distingue essenzialmente tre tipi di servizi, cui limita l'esenzione da responsabilità: il semplice trasporto *(mere conduit)* consistente nella trasmissione o nella fornitura dell'accesso; la memorizzazione automatica, intermedia e temporanea delle informazioni *(caching)*; la memorizzazione delle informazioni fornite da un destinatario del servizio *(hosting)*.

In particolare, per il servizio di trasporto si stabilisce che:

"(...) il prestatore non sia responsabile delle informazioni trasmesse a condizione che egli:

a) non dia origine alla trasmissione;

b) non selezioni il destinatario della trasmissione; e

c) *non selezioni né modifichi le informazioni trasmesse."*[72]

Per il servizio di *hosting*, invece, si prevede la non responsabilità del *provider* a condizione che quest'ultimo non fosse a conoscenza dell'illiceità dell'attività o dell'informazione ospitata, né di fatti o di circostanze che rendessero manifesta l'illiceità dell'attività o dell'informazione e che, una volta avuta tale conoscenza, abbia agito prontamente nel rimuovere le informazioni lesive o bloccarne l'accesso:

"Gli Stati membri provvedono affinché (...) il prestatore non sia responsabile delle informazioni memorizzate a richiesta di un destinatario del servizio, a condizione che detto prestatore:

a) non sia effettivamente al corrente del fatto che l'attività o l'informazione è illecita e, per quanto attiene ad azioni risarcitorie, non sia al corrente di fatti o di circostanze che rendono manifesta l'illegalità dell'attività o dell'informazione, o

b) non appena al corrente di tali fatti, agisca immediatamente per rimuovere le informazioni o per disabilitarne l'accesso.

(...) Il presente articolo lascia impregiudicata la possibilità, per un organo giurisdizionale o un'autorità amministrativa, in conformità agli ordinamenti giuridici de-

[72] Cfr. Art. 12 Direttiva 2000/31/CE.

gli Stati membri, di esigere che il prestatore ponga fine ad una violazione o la impedisca nonché la possibilità, per gli Stati membri, di definire procedure per la rimozione delle informazioni o la disabilitazione dell'accesso alle medesime."[73]

Si può notare, dunque, come la disciplina europea differisca da quella statunitense per quanto concerne il momento della conoscenza della condotta illecita del terzo dal momento che si attribuisce espressamente all'autorità giudiziaria o all'autorità amministrativa competente di ordinare all'intermediario di porre fine alle violazioni e a condizione che tali ordini non impongano un obbligo generale di controllo.

In altri termini, per qualunque tipo di *provider*, l'esimente opererà quando il ruolo dell'intermediario è meramente "tecnico automatico e passivo".

A riguardo è stato affermato che le deroghe alla responsabilità stabilite nella direttiva 31/200/CE "riguardano esclusivamente il caso in cui l'attività di prestatore di servizi della società dell'informazione si limiti al processo tecnico di attivare e fornire accesso ad una rete di comunicazione sulla quale sono trasmesse o temporaneamente memorizzate le informazioni messe a disposizione da terzi al solo scopo di rendere più efficiente la trasmissione. Siffatta attività è di ordine meramente tecnico, automatico e passivo, il che implica che il prestatore di servizi della società dell'informazione non conosce né controlla le informazioni trasmesse o memorizzate"[74].

È evidente come le norme sull'immunità degli intermediari siano però state elaborate in un contesto tecnologico, economico e sociale che si presentava profondamente diverso da quello attuale[75] e, conseguentemente, ci si è interrogati sulla necessità di individuare una maggiore responsabilizzazione del ruolo del *provider* e all'esigenza di fornire una risposta rapida alla commissione dell'illecito che le autorità competenti non riescono a fornire in tempi brevi[76].

Resta il problema di determinare se il comportamento dell'intermediario che abbia favorito la commissione dell'illecito possa in ogni caso trovare una propria giustificazione nel caso in cui la valutazione giuridica dell'informazione o della condotta lesiva si presenti controversa – o comunque di difficile interpretazione – dal momento

[73] Cfr. Art. 14 Direttiva 2000/31/CE.
[74] Cfr. Cons. 42 Direttiva 2000/31/CE.
[75] Oggi i grandi gruppi economici sono dotati di sistemi capaci di rilevare automaticamente il contenuto illecito e di bloccare immediatamente l'accesso a detto contenuto.
[76] Sul punto, in maniera più ampia, cfr. G. SARTOR, *La responsabilità degli intermediari e i diritti fondamentali*, in T. E. FROSINI, O. POLLICINO, M. BASSINI (a cura di), Diritti e libertà in internet, Mondadori Education, Milano, 2017.

che un contenuto *prima facie* contrario alla legge possa, al contrario, costituire la pretesa di una protezione di un diritto fondamentale di pari rango che dovrà necessariamente trovare tutela da parte dell'ordinamento.

Tale bilanciamento non potrà che trovare attuazione se non attraverso l'interpretazione dell'autorità nazionale competente che sarà chiamata a dare o meno conferma dell'ordine di rimozione del contenuto.

La questione della responsabilità dei *service provider* – e della necessità di un bilanciamento tra i differenti diritti costituzionalmente garantiti – è stata oggetto della discussa pronuncia *Delfi AS v. Estonia* (richiesta n. 64569/09)[77] della Corte europea dei diritti dell'uomo che, richiamandosi ai precedenti in materia, ha precisato l'estensione del diritto alla libertà di espressione in ambito CEDU muovendosi, tuttavia, nella direzione opposta rispetto al modello sopra descritto[78].

La sentenza concerneva un ricorso presentato dalla società estone Delfi – titolare di un portale di informazione *on-line* – condannata in prima battuta dalla Corte Suprema estone per non aver impedito la pubblicazione di *"clearly unlawful comments"* che avevano leso la reputazione di un privato cittadino che, di conseguenza, aveva attivato, contro la società un contenzioso per ottenere il risarcimento dei danni subiti dall'attacco alla sua reputazione.

In particolare, Delfi aveva proceduto alla pubblicazione (sul suo portale) di un articolo concernente la deviazione di alcune rotte navali da parte della *Saaremaa Shipping Company*, una società pubblica di trasporto marittimo che collegava la terraferma estone con alcune isole, i cui traghetti viaggiavano da una rotta ad una altra rompendo le lastre di ghiaccio (nell'articolo veniva aspramente criticato l'operato dell'amministratore della società).

La notizia aveva ricevuto circa 185 commenti, di cui una ventina anonimi e contenenti minacce personali e linguaggio diffamatorio nei confronti del dirigente.

[77] A riguardo, in https://www.federalismi.it/nv14/articolo-documento.cfm?Artid=29862

[78] La sentenza si colloca in un filone di casi che riguardano la tutela della libertà d'espressione su Internet che, finora, è stata bilanciata con il rispetto del diritto d'autore. Sul punto, cfr. A. SPAGNOLO, *Bilanciamento tra libertà d'espressione su Internet e tutela del diritto d'autore nella giurisprudenza recente della Corte europea dei diritti dell'uomo*, in federalismi.it

A seguito della segnalazione, Delfi provvedeva alla rimozione di tutti i contenuti offensivi, rifiutandosi però di corrispondere alla società alcuna somma a titolo risarcitorio in ragione della predisposizione di adeguati meccanismi difensivi rispetto all'inserimento dei contenuti diffamatori da parte degli utenti[79].

Dall'episodio sorgeva una controversia davanti all'autorità giudiziaria estone che si concludeva con l'accoglimento della domanda risarcitoria della società di navigazione.

Secondo i giudici, il meccanismo di rimozione predisposto da Delfi doveva ritenersi insufficiente e inidoneo a garantire una protezione adeguata ai diritti dei terzi: la libertà di espressione non avrebbe potuto estendersi fino a coprire la pubblicazione di commenti diffamatori e, peraltro, il portale avrebbe avuto il pieno controllo del flusso dei commenti, potendo scegliere quali pubblicare. Conseguentemente, accanto ai materiali commentatori, anche Delfi doveva ritenersi autrice dei contenuti diffamatori.

A seguito della pronuncia, la società Delfi presentava ricorso alla Corte europea dei diritti dell'uomo, sostenendo la violazione dell'art. 10 della Convenzione europea dei diritti dell'uomo[80].

La Corte rilevava che l'articolo pubblicato affrontava un argomento di un certo grado di interesse pubblico, tuttavia, nel ragionamento dei giudici assume grande rilievo l'idea di un *obbligo positivo di protezione* gravante sul portale:

"When examining whether there is a need for an interference with freedom of expression in a democratic society in the interests of the protection of the reputation or rights of others, the Court may be required to ascertain whether the domestic authorities have struck a fair balance when protecting two values guaranteed by the Convention which may come into conflict with each other in certain cases, namely on

[79] Delfi aveva, infatti, previsto dei meccanismi difensivi al fine di limitare la diffusione di commenti diffamatori: in primo luogo, un algoritmo rendeva non pubblicabile un certo numero di parole volgari e offensive; in secondo luogo, un sistema di *notice and take down* consentiva agli utenti di segnalare agli amministratori la presenza di tali contenuti; in terzo luogo, gli amministratori stessi potevano attivarsi spontaneamente per eliminare i commenti diffamatori, In ogni caso, Delfi declinava ogni responsabilità in ordine al contenuto dei commenti postati dai propri lettori sul portale.

[80] In particolare, l'Articolo 10 CEDU prevede che "Ogni persona ha diritto alla libertà d'espressione. Tale diritto include la libertà d'opinione e la libertà di ricevere o di comunicare informazioni o idee senza che vi possa essere ingerenza da parte delle autorità pubbliche e senza limiti di frontiera (...)". In https://www.echr.coe.int/documents/convention_ita.pdf

the one hand freedom of expression protected by Article 10, and on the other the right to respect for private life enshrined in Article 8."[81]

Certamente la società Delfi AS avrebbe dovuto esercitare una maggiore prudenza nella pubblicazione della notizia, ciò al fine di evitare di essere ritenuta a sua volta responsabile per la violazione della reputazione di altre persone. Il portale non soltanto aveva il controllo dei contenuti pubblicati, ma aveva anche invitato gli utenti a trasmetterli, integrandoli nel sito, oltre ad avere la possibilità di bloccare o rimuovere il commento, senza che l'autore potesse fare nulla per eliminarlo.

Questa combinazione di fattori escludeva che Delfi potesse rivendicare un ruolo puramente tecnico, tipico dei *providers*, proprio per il controllo da essa esercitato e, di conseguenza, non risultava contrario alla Convenzione considerare il portale responsabile per i commenti manifestamente illegittimi. A ciò aggiungasi che l'esercizio della libertà di espressione deve essere correttamente bilanciato con il diritto alla tutela della propria reputazione previsto anch'esso all'articolo 8 della Convenzione dei diritti dell'uomo[82].

Non è prevista alcuna protezione dell'articolo 10 che, di certo, non tutela la diffusione di messaggi di odio o diffamatori di cui, anzi, risulta necessario prevenire la diffusione[83].

Sulla base di tali elementi, in relazione alla natura offensiva e minacciosa delle osservazioni, il fatto che i commenti sono stati inviati in reazione ad un articolo pubblicato sul portale della società, l'insufficienza delle misure adottate dalla società per evitare i danni causati alla reputazione di altre persone, la Corte di Strasburgo ha ritenuto che, nel caso di specie, la società Delfi AS fosse responsabile per i commenti diffamatori pubblicati dai lettori sul suo portale di notizie, potendosi rappresentare una limitazione giustificata e proporzionata alla libertà di espressione:

---

[81] In https://hudoc.echr.coe.int/app/conversion/pdf/?library=ECHR&id=001-155105&filename=001-155105.pdf

[82] In particolare, l'Articolo 8 CEDU prevede che "Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza (...)". In https://www.echr.coe.int/documents/convention_ita.pdf

[83] Il sempre più agevole e generalizzato accesso da parte del singolo individuo a strumenti di comunicazione che consentono, anche avvalendosi dell'anonimato, di raggiungere una vasta e potenzialmente illimitata categoria di destinatari impone di riconsiderare il diritto alla libertà di espressione alla luce della necessità di contemperare tale diritto con quelli dei soggetti destinatari suscettibili di essere aggrediti e ritenuti altrettanto meritevoli di tutela. Cfr. Parlamento europeo, *La libertà di espressione, una prospettiva di diritto comparato*, in https://www.europarl.europa.eu/RegData/etudes/STUD/2019/644172/EPRS_STU(2019)644172_IT.pdf

"The Court has considered that where the right to freedom of expression is being balanced against the right to respect for private life, the relevant criteria in the balancing exercise include the following elements: contribution to a debate of general interest, how well known the person concerned is, the subject of the report, the prior conduct of the person concerned, the method of obtaining the information and its veracity, the content, form and consequences of the publication, and the severity of the sanction imposed."[84]

Il caso concerne, dunque, gli obblighi e le responsabilità dei portali di informazione su Internet che forniscono, a fini commerciali, una piattaforma destinata alla pubblicazione dei commenti degli utenti su informazioni pubblicate in precedenza: alcuni utenti, identificati o anonimi, possono lasciare frasi chiaramente illecite che ledono i diritti della personalità dei terzi.

In ogni caso, l'imputabilità in capo al gestore del sito di una responsabilità per i danni arrecati dai contenuti anonimi – conformemente ad un principio *cuius commoda et eius incommoda*[85] – potrebbe realizzare forme di censura preventiva adottate dagli intermediari sulla base di una logica meramente economica basata su un rapporto di costi e di benefici: il *provider* preferirà rimuovere preventivamente il commento potenzialmente illecito allo scopo di evitare una futura ed eventuale condanna in sede giudiziale.

L'adozione di una forma simile di responsabilità troverebbe allora la sua giustificazione unicamente di fronte all'esigenza della tutela dei valori fondamentali dell'ordinamento[86].

Tuttavia, la figura dell'*hosting attivo* dovrebbe inquadrarsi maggiormente in uno schema di responsabilità dell'intermediario in linea con il progresso tecnologico e della disponibilità di strumenti innovativi finalizzati ad individuare i casi di illiceità realizzati da terzi sulla piattaforma (si pensi, ad esempio, alle nuove tecnologie per

[84] In https://hudoc.echr.coe.int/app/conversion/pdf/?library=ECHR&id=001-155105&filename=001-155105.pdf
[85] Vale a dire, una sorta di responsabilità per rischio di impresa.
[86] Si pensi, ad esempio, al valore della salute nella responsabilità ambientale sulla base del principio "chi inquina paga".

l'identificazione dei contenuti che consentono di identificare immediatamente le copie o i frammenti del materiale protetto dal diritto d'autore[87]).

4. Conclusioni.

Da quanto analizzato nelle pagine che precedono, risulta evidente come la complessità e la vastità della materia presa in esame sollevi una serie di complesse criticità, soprattutto per i risvolti della liceità dell'anonimato sulle situazioni giuridiche altrui.

In effetti, la caratteristica intrinseca di Internet – che permette che qualsiasi dato, anche quello apparentemente anonimo, riveli l'identità di una persona qualora non si proceda a forme idonee di trattamento – è rappresentata dall'anonimato che può essere definito come una *condizione giuridica normale* per chi naviga nella Rete[88].

L'anonimato rappresenta uno spazio di libertà e una forma di tutela effettiva per la propria identità digitale e per il proprio patrimonio informativo e, anzi, l'anonimato si pone come un vero e proprio diritto della persona che potrà esercitare su Internet i suoi diritti di cittadino digitale[89].

Non è un caso se negli Stati Uniti d'America, la Corte Suprema ha chiarito come:

"Anonymity is a shield from the tyranny of the majority (...) It thus exemplifies the purpose behind the Bill of Rights and of the First Amendment in particular: to protect unpopular individuals from retaliation (...) at the hand of an intolerant society."[90]

In altri termini, l'anonimato degli utenti riceve, di regola, una sua tutela giuridica per gli effetti pratici che produce sulla stessa *Information Society*, mentre, al contrario, l'identificazione dell'utente è posta come una *eccezione*.

In linea di principio, il ricorso alle tecniche di anonimato dovrebbe reputarsi non soltanto lecito, ma persino incoraggiabile dal punto di vista normativo in quanto strumentale rispetto alla salvaguardia del diritto alla protezione dei dati personali[91].

---

[87] Un esempio è dato dall'algoritmo di riconoscimento di YouTube che, negli ultimi anni, è migliorato in maniera esponenziale ed è ora in grado di identificare la canzone come coperta dal diritto d'autore.
[88] Cfr. E. BASSOLI (a cura di), *Come difendersi dalla violazione dei dati su Internet. Diritti e responsabilità*, Maggiori Editore, 2012.
[89] Sul punto, D. BIANCHI, *Anonimato in Rete, libertà di espressione e identità personale. La Corte Suprema di Israele: l'anonimato rende Internet ciò che è*, in *Persona e Danno*, (a cura di) P. CENDON.
[90] Cfr. MCINTYRE V. OHIO ELECTIONS COMMISSION, 514 U.S. 334 (1995)
[91] Sul punto, cfr. G. RESTA, *L'anonimato in Internet*, in T. E. FROSINI, O. POLLICINO, M. BASSINI (a cura di), *Diritti e libertà in internet*, Mondadori Education, Milano, 2017.

La premessa è costituita da un tradizionale rifiuto nei confronti di tutte quelle tecniche di sorveglianza che erano originariamente collegate all'utilizzo della Rete che consentivano agli utenti di poter navigare liberamente senza preoccuparsi dei siti visitati o dei commenti pubblicati.

La situazione, tuttavia, appare radicalmente mutata.

Oggi Internet non è più uno spazio totalmente aperto e libero, ma l'accesso viene intermediato da società specializzate nel trasporto dei pacchetti di dati e dei cavi di collegamento (*Internet Service Providers*) che consentono alle persone di connettersi e di sfruttare appieno le potenzialità offerte dalla Rete. Tutto ciò che facciamo *on-line* viene memorizzato e catalogato dai gestori dei siti Internet e gli stessi utenti, volontariamente, rivelano una parte considerevole della loro vita privata, condividendo *on-line* ogni momento della loro giornata.

Se da un lato gli Stati condannano tali comportamenti e richiedono una maggiore trasparenza ai fornitori del servizio nelle attività di raccolta e di utilizzazione dei dati, dall'altro lato ricercano la loro collaborazione al fine di contrastare la commissione di una varietà di reati atti ad offendere i diritti fondamentali (*fake news* e *hate speech*), anche nella prospettiva di assicurare una maggiore sicurezza collettiva contro la commissione di reati più gravi.

Pertanto, l'esigenza di identificare i soggetti che operano nella Rete appare imprescindibilmente legata all'individuazione di una responsabilità individuale o di impresa.

Se uno degli aspetti della libertà è quello di poter agire con una propria identità virtuale diversa da quella reale, deve essere possibile, in ogni caso, individuare una responsabilità quando tali comportamenti si sostanziano nella violazione dei diritti altrui[92]. L'anonimato di commettere attività illecite sulla Rete può essere allora equiparato a chi lancia dei sassi da un cavalcavia contro le auto in corsa o a chi spacca la vetrina di un negozio coperto dal passamontagna: l'intento evidente è quello di provocare un incidente e realizzare un danno che, in alcuni casi, può risultare fatale[93].

[92] Sul punto, cfr. S. SICA e V. ZENO-ZENCOVICH, *Manuale di diritto dell'informazione e della comunicazione*, CEDAM, 2019.
[93] A riguardo, si ricordano i recenti fatti di cronaca concernenti la sfida lanciata sul *social network* TikTok di coprirsi totalmente il volto in modo tale da non poter respirare (*blackout challenge*) che ha provocato già due vittime tra i giovanissimi. In https://www.reccom.org/blackout-game-luomo-nero-di-tik-tok-e-altri-mostri/

Da ciò derivano complessi problemi giuridici, rispetto ai quali la riflessione si trova ancora in uno stato embrionale[94].

Di certo l'analisi che si è svolta in queste pagine non intende necessariamente offrire risposte certe, ma quanto soprattutto la volontà di suscitare una discussione critica tra i professionisti del settore con l'auspicio di contribuire a ravvivare l'interesse verso una tematica esposta ad un continuo mutamento e caratterizzata da un approccio del legislatore ancora non definito in senso univoco, ma che si profila come argomento primario nel contesto tecnologico del prossimo futuro.

Risulta, allora, con tutta evidenza come "there is no guarantee that an anonymity-free Internet would be a kinder, gentler Internet"[95].

5. Note bibliografiche.

G. FINOCCHIARO (a cura di), *Diritto all'anonimato. Anonimato, nome e identità personale*, in Tratt. Galgano, XLVIII, Padova, 2008.

T. E. FROSINI, *Tecnologie e libertà costituzionali*, in *Diritto dell'informazione e dell'informatica*, 2003.

L. CASINI, *Lo Stato nell'era di Google. Frontiere e sfide globali*, Mondadori, 2020.

M. MANETTI, *Libertà di pensiero e anonimato in rete*, in *Diritto dell'informazione e dell'informatica"* 2014.

G. PITRUZZELLA e O. POLLICINO, *Disinformation and hate speech. A European Constitutional Perspective*, Egea, 2020.

O. POLLICINO e E. BIETTI, *Truth and deception across the Atlantic: a roadmap of disinformation in the US and Europe*, in *Italian Journal of Public Law*, 2019.

O. POLLICINO e M. BASSINI, *Free speech, defamation, and the limits to freedom of expression in the EU: a comparative analysis*, in Research handbook on EU Internet Law, edited my Andrej Savin and Jan Trzaskowski, Edward Edgar, Cheltenham-Northampton, 2014.

G. M. RICCIO, *La responsabilità civile degli Internet Providers*, Giappichelli, Torino, 2002.

J. RIFKIN, *L'era dell'accesso. La rivoluzione della new economy,* Mondadori, Milano, 2001.

[94] La latitanza, il ritardo o l'inadeguatezza di tale riflessione e valutazione è paradigmatica del più cospicuo effetto sociale degli avanzamenti tecnologici registrati nei ultimi anni.

[95] Cfr. W. PHILLIPS, *This Is Why We Can't Have Nice Things: Mapping the Relationship between Online Trolling and Mainstream Culture*, 2016.

V. ZENO-ZENCOVICH, *La libertà di espressione. Media, mercato, potere nella società dell'informazione*, Il Mulino, Bologna, 2004.

LE NECESSITÀ DI CONTEMPERAMENTO TRA LE FINALITÀ DI MARKETING E LA TUTELA DEL TRATTAMENTO DEI DATI PERSONALI: TECNICHE DI MARKETING E ADEMPIMENTI DEL TITOLARE DEL TRATTAMENTO

di Tiziana Di Palma

SOMMARIO: 1. Le finalità di marketing con l'accesso al web. La pubblicità comportamentale – 2. Profilazione: pratiche di tracciamento e di mappatura – 3. L'attività di profilazione alla luce del GDPR e gli adempimenti del titolare del trattamento. Gli adempimenti aggiuntivi di *Privacy-by-design* e *Privacy-by-default*

1. Le finalità di marketing con l'accesso al web. La pubblicità comportamentale

L'accesso quotidiano se non costante al web offre la possibilità di comprendere l'importanza che assume la vetrina di Internet per imprese e professionisti che intendono promuovere le proprie attività, prodotti e servizi.

Si pensi, pertanto, all*'email marketing*, ai concorsi a premio, ai *banner* pubblicitari, all'invio di sms o di messaggi attraverso varie piattaforme, alla pubblicazione di post "*sponsorizzati*" sugli *account social*, da parte di produttori ed imprenditori, contenenti promozioni, offerte, al fine di acquisire e di fidelizzare la clientela finale.

È di immediata evidenza, inoltre, che l'impiego di tali strumenti si profila in maniera sempre più mirata, modulandosi attraverso le preferenze in vario modo manifestate da parte dell'utenza, suscitando ragionevoli dubbi circa l'ossequio alla disciplina in materia di protezione dei dati personali, dato il sottilissimo perimetro entro il quale l'utente conserva il suo privato in seguito all'uso smodato dei dispositivi intelligenti e dei *social network*.

Concentrando il discorso sugli aspetti relativi all'attività di *marketing* e al trattamento dei dati personali che deve operare nel rispetto della normativa *privacy* vigente nel nostro ordinamento, in estrema sintesi, appare utile richiamare l'art. 4 del Regolamento (UE) 2016/679 del 27.04.2016 che, relativamente alla definizione di

"*trattamento*", descrive "*qualsiasi operazione o insieme di operazioni, compiute con o senza ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione*".

In tale contesto, dunque, poiché tutte le operazioni che comportano la conoscenza di informazioni relative a persone fisiche, identificate o identificabili, si configurano come attività di trattamento di dati personali, l'invio di comunicazioni commerciali tramite posta elettronica comporta trattamento di dati personali, in quanto l'indirizzo *email* dell'utente utilizzato per l'iscrizione al servizio di newsletter offerto da una società è, appunto, un dato personale.

Ugualmente, nel caso di finalità di *marketing* perseguite attraverso l'invio di messaggi promozionali tramite sms; anche in tale ipotesi, infatti, la società o il professionista che intende utilizzare tale canale gestirà dati personali, quali sono i numeri di telefono dei destinatari cui indirizzare i messaggi.

Le finalità di marketing, tuttavia, si realizzano anche attraverso la cd. *pubblicità mirata*, che mostra gli annunci più pertinenti in base al profilo dell'utente che visualizza la pagina, il cui esempio più evidente è rappresentato dalle offerte automatiche durante il caricamento di una pagina web, senza che l'utente se ne accorga.

Si parla, così, di pubblicità comportamentale (*behavioural advertising*) rappresentata dal tracciamento delle attività degli internauti con lo scopo di offrire una pubblicità mirata e quindi più efficace per le finalità di marketing.

Il Parere dei Garanti Europei riuniti ex art. 29 della dir. N. 95/46/CE del Parlamento europeo e del Consiglio del 24.10.1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, offre la puntuale definizione di pubblicità comportamentale, la quale utilizza le informazioni raccolte sul comportamento di navigazione degli internauti, ad esempio le pagine visitate o le ricerche effettuate allo scopo di selezionare le pubblicità da offrire.

Si tratta, indubbiamente, di un'attività di profilazione, consistente in una "*tecnica di trattamento automatico mediante algoritmi di molteplici tipologie di dati personali relativi a quantità numericamente elevatissime di persone, per attribuire a ciascuna*

di queste ultime un profilo, ovvero una categoria predefinita e delineata attraverso parametri che il responsabile del trattamento considera necessari alla sua ricerca, al raggiungimento del suo scopo; il target è studiato nelle sue abitudini di consumo e negli stili di vita che ne rivelano attitudine e capacità di spesa, gusti per alcuni prodotti o servizi e disinteresse per altri, caratteristiche legate alla sua identità personale" [96].

La dinamica che consente la creazione della categoria specifica prevede un sistema di "*aggregazione in clusters*" che avviene tramite l'incrocio e l'associazione di alcuni dati personali degli utenti con le informazioni elaborate mediante algoritmo.

Tali informazioni oggetto di incrocio, valutazione ed associazione possono essere di natura geografica (*Geotageting*), socio-demografica (*tarketing* sociodemografico) o economica della popolazione presente nel relativo luogo di residenza.

Il *cluster* può essere paragonato ad una lente di ingrandimento. Quanto più il *cluster* risulta individuato per dettaglio, quanto maggiore le informazioni possono essere rivelatrici degli aspetti sensibili della vita dei soggetti profilati. La finalità della profilazione, quindi, è una tecnica in stretta connessione funzionale al concetto di identificazione/identificabilità della persona[97].

Relativamente alla questione della necessaria protezione dei dati, secondo il citato parere, l'editore si considera *"titolare"* autonomo del trattamento nella misura in cui raccoglie i dati personali dell'utente (profilo utente, indirizzo IP, ubicazione, lingua del sistema operativo) per i propri scopi.
Il fornitore di reti pubblicitarie è da considerarsi, a sua volta, un *"titolare*" del trattamento nella misura in cui determina le finalità (seguire gli utenti sui vari siti web) o gli strumenti essenziali dell'elaborazione dei dati.

Può considerarsi, al riguardo, al servizio di erogazione dei *banner* pubblicitari offerto da talune società ai propri clienti su diversi siti o anche il servizio di rendicontazione delle *impression* e dei *click* effettuati, posto che le *impression* corrispondono al numero di volte che un annuncio pubblicitario appare ad un visitatore *web* mentre i *click* sono le risposte del cliente internauta ai *banner*.

[96] P. PACILEO, *Profilazione e diritto di opposizione,* in S. SICA – V. D'ANNTONIO – G.M. RICCIO, *La Nuova Disciplina Europea della Privacy*, 177-196
[97] F. PIZZETTI, *Protezione dei dati personali in Italia tra GDPR e codice novellato*, Torino, 2021.

2. Profilazione: pratiche di tracciamento e di mappatura.

Si pensi alle applicazioni che vengono "*scaricate*" sui dispositivi, gratuite solo in apparenza poiché vengono ampiamente ripagate allorquando viene consentito alla società che offre il servizio l'accesso al profilo personale, al fine di inviare all'utente pubblicità mirata, basata sugli interessi, in quanto ogni azienda, in tal guisa, è in grado di offrire un prodotto su misura, perché conosce le abitudini, i gusti, le preferenze dei clienti a cu invia il banner pubblicitario.

Per l'identificazione del soggetto, secondo il Gruppo dei Garanti Europei, vanno considerati gli indirizzi IP, dichiarando che "*i fornitori di accesso Internet e i gestori delle reti LAN possono, utilizzando mezzi ragionevoli, identificare gli utenti Internet cui essi hanno attribuito indirizzi IP, poiché normalmente, essi "registrano" in un apposito file la data, l'ora, la durata e l'indirizzo IP dinamico assegnato all'utente Internet*".

Del resto, anche la giurisprudenza della CGUE, sez. II, con sentenza del 19.10.2016 (C-582/14), è pervenuta a ritenere che "*il fornitore di servizi di media online disponga di mezzi che possono essere ragionevolmente utilizzati per identificare, con l'aiuto di altri soggetti, ossia l'autorità competente e il fornitore di accesso ad internet, la persona interessata sulla base degli indirizzi IP conservati (...),*
l'art. 2 lett. a) dir. 95/46 deve essere interpretato nel senso che un indirizzo IP dinamico registrato da un fornitore di servizi di media online in occasione della consultazione, da parte di una persona, di un sito internet che tale fornitore rende accessibile al pubblico costituisce, nei confronti di tale fornitore, un dato personale ai sensi di detta disposizione, qualora detto fornitore disponga di mezzi giuridici che gli consentano di far identificare la persona interessata grazie alle informazioni aggiuntive di cui il fornitore di accesso a Internet di detta persona dispone".

In talune circostanze, tuttavia, alcuni indirizzi IP non consentono l'immediata identificazione dell'utente, come nel caso degli indirizzi IP attribuiti ad un computer di un *internet café*, ove non è richiesta l'identificazione dei clienti[98].

In Italia, il primo caso di mappatura dei numeri IP risale al 2007 quando una società di servizi svizzera (*Logistep* che lavorava per conto della casa discografica *Peppermint Jam Records Gmbh* e per la *Techland*) ha registrato 3636 utenti che avrebbero messo in condivisione file musicali protetti da diritto d'autore.

[98] N. BERNARDI, M. PEREGO, M. POLACCHINI, M. SOFFIENTINI, *Privacy Officer. La figura chiave della data protection europea,* IPSOA, 2013

In ispecie, il Garante, richiamando anche la decisione dell'omologa Autorità svizzera, ha ritenuto illecita l'attività svolta dalle società, ricordando che *"la direttiva europea sulle comunicazioni elettroniche vieta ai privati di poter effettuare monitoraggi, ossia trattamenti di dati massivi, capillari e prolungati nei riguardi di un numero elevato di soggetti. È stato poi violato il principio di finalità: le reti P2P (peer to peer) sono finalizzate allo scambio tra utenti di dati e file per scopi personali. L'utilizzo dei dati dell'utente può avvenire, dunque, soltanto per queste finalità e non per scopi ulteriori quali quelli perseguiti dalle società Peppermint e Techland (cioè il monitoraggio e la ricerca di dati per la richiesta di un risarcimento del danno*)[99]".

La pratica che sembra essere tra le più preoccupanti è quella del *web listening* con la quale aziende vendono un servizio di "*ascolto di informazioni*", contando quante volte viene nominata una data parola o marca in una conversazione pubblica, quindi, su Twitter, Facebook, Groupon etc, con il risultato per il quale, se si avverte che un determinato concetto viene ripetuto costantemente, i pubblicitari hanno facilitato il compito di capire cosa vuole l'utenza in quel determinato momento.

Le complicazioni connesse al suddetto processo di profilazione risiedono nella circostanza per la quale il suddetto risulti del tutto invisibile agli interessati, in quanto vengono acquisiti dati personali senza che vengano forniti dagli interessati[100].

L'importante *leading case* che può essere quivi citato è rappresentato dal *DoubleClick, Inc, v. Privacy Litigation*[101], nel quale la società *DoubleClic*k fu chiamata in giudizio in quanto, secondo gli attori, il suo servizio di banner pubblicitario violava il *Wiretap Act* e lo *Stored Communications* Act.

Il punto nodale della questione risiedeva nell'utilizzo da parte della predetta società, di *cookie*[102] mediante i quali riusciva a tracciare un profilo dell'utente così da indirizzare al meglio le tipologie di annunci pubblicitari da inviare diversificandole a seconda del soggetto.

---

[99] Cfr. *Internet: illecito "spiare" gli utenti che scambiano file musicali e giochi,* 13.03.2008, *www.garanteprivacy.it.*

[100] Già nel 2006, La *Federal Trade Commission* (FTC) condusse uno studio dal quale emerse che il 92,8% dei siti web raccoglievano almeno una tipologia di dato personale (nominativo, indirizzo IP, indirizzo di posta elettronica), W. CHUNG - J. PAYNTER, *Privacy issues on the internet, Proceedings of the 35th International Conference on System Sciences*, Hawaii, 2002.

[101] Cfr. 154, F. Supp. 2d 497 (S.D.N.Y. 2001).

[102] Cfr. Trattasi di stringhe di testo di piccole dimensioni che i siti visitati dall'utente inviano al suo terminale (solitamente al browser) dove vengono memorizzati per essere poi ritrasmessi agli stessi siti alla successiva visita del medesimo utente. Secondo il W.G. art. 29, *Tutela della vita privata su Internet – un approccio integrato dell'EU alla protezione dei dati on-line* -, "*i cookie sono pezzi di dati creati da un web server, che possono essere memorizzati come file di testo e depositati sul disco dell'utente,*

Secondo la prospettazione attorea, si violava il *Wiretap Act*, in quanto il *cookie* catturava i dati in transito, sia lo *Stored Communication Act*, in quanto il *cookie* si installava nell'hard disk del navigatore Internet al fine di essere richiamato ogni qualvolta che fosse necessario, accedendo così in maniera non autorizzata alle memorie di massa del computer dell'utente.

La difesa della società argomentò sostenendo che il rapporto originario – da considerare al fine di valutare l'eventuale responsabilità – non era quello tra *DoubleClick* e gli utenti, bensì tra *DoubleClick* e i siti *partner* che avevano accettato di ospitare i suoi *banner* pubblicitari, per cui l'accesso alla comunicazione tra gli utenti e i siti web era stato dato non dagli utenti singolarmente, ma dai siti affiliati a *DoubleClick* con i quali gli utenti avevano comunicato.

La Suprema Corte accettò tale interpretazione, non riscontrando alcun reato, in quanto era presente l'autorizzazione da parte dei siti partner, integrando così l'esimente di responsabilità del consenso di una delle parti coinvolte nella comunicazione[103].

Altro esempio è rappresentato dall'esperienza del 2006 di AOL, motore di ricerca britannico allora più utilizzato, che aveva divulgato i dati relativi alle ricerche effettuate da oltre 650.000 utenti in tre mesi, permettendo di ricostruire la quotidianità di ogni singolo utente, contraddistinto da un numero, attraverso le domande rivolte al motore stesso.

Con riferimento agli USA, ove è situata la sede legale di Facebook, Google, Youtube, si ricordi che vige una legislazione ispirata ai principi di *common law*, la quale attribuisce valore legale "*forte*" alla scelta dell'utente, mediante click, su una pagina web; per fare un esempio, quando l'utente spunta la casella "*accetta*", posta come espressione della volontà dell'utente, per la legislazione USA, tale atto ha valore legale equiparato a quello di una firma apposta su di un documento.

Se si cita il caso di Facebook, infatti, l'utente, durante la registrazione al sito, cliccando sulla casella *"accetto*", acconsente a Facebook di appropriarsi di quello che

mentre una copia può essere conservata dal sito web. Essi rappresentano una parte standard del traffico http e, in quanto tali, possono essere trasportati senza ostacoli, con il traffico IP. Un cookie può contenere un numero esclusivo (GUI, Global Unique Identifier), che permette una migliore personalizzazione rispetto agli indirizzi IP dinamici. I cookie permettono al sito web di tenere traccia dei modelli e preferenze dell'utente" (Y. POULLET. *Riservatezza e sicurezza delle reti*, in Atti del convegno "*Internet e privacy: quali regole*?", n. 1 a Garante, in *Bollettino*, 5, p. 33.

[103] Cfr. P. PERRI, *Protezione dei Dati e Nuove Tecnologie, Aspetti nazionali, europei e statunitensi*, Milano, 2007, p. 52.

viene pubblicato dall'iscritto: musica, scritti, foto, banche dati, software e, in aggiunta, sarà responsabilità dell'utente verificare che il materiale che egli pubblica non sia coperto, a sua volta, dal diritto d'autore.

Ai fini sanzionatori, le numerose istanze avanzate per reprimere le suddette condotte hanno, talvolta, incontrato un atteggiamento della giurisprudenza alquanto restrittivo, potendosi richiamare una famosa pronuncia statunitense del 2008 (*Viacom Int.'l, Inc. v. YouTube, Inc* – 676 F.3d 19 (2d CIr. 2012), che obbligava Google a trasmettere alla società Viacom (proprietaria di MTV e Paramount Pictures) l'archivio con i dati di login di tutti gli utenti di Youtube, gli indirizzi IP dei loro computer e i parametri dei video che hanno guardati, al dichiarato fine di valutare l'attrattività dei video che violano i diritti d'autore presenti su Youtube.

Il richiamo a Facebook o alle altre piattaforme risalenti a società statunitensi pone l'ulteriore quesito circa la conservazione dei dati personali da parte dei suddetti server con sede all'estero.

A tal proposito, dunque, si rammenti che la gran parte, se non totalità, dei siti web con sede negli Stati Uniti dichiara di aderire al programma *Safe Harbor*, che scaturisce dall'intesa raggiunta tra USA ed Europa per quanto riguarda la sicurezza del trattamento dei dati personali da parte dei siti con sede negli USA, nato dalla decisione del 26.07.2000 n. 2000/520/CE, trasformata in legge n. 115 del 25.04.2001, e recepito in Italia con la Deliberazione del Garante n. 36 del 10.10.2001 denominata "*Autorizzazione al trasferimento verso gli Stati Uniti d'America*" che recita: "*Sulla base dei principi fissati dalla Commissione europea, il Garante, preso atto della dichiarazione comunitaria di adeguatezza del livello di protezione garantito dalle organizzazioni aventi sede negli Stati Uniti d'America ed aderenti al cd. accordo del Safe Harbor, ha autorizzato il trasferimento dei dati personali dall'Italia verso gli USA; il Garante si è riservato di svolgere i necessari controlli su trasferimenti di dati e su connesse operazioni di trattamento, nonché di adottare eventuali provvedimenti di blocco o di divieto di trasferimento*"[104] .

Vi è, infatti, un elenco redatto dal Dipartimento del Commercio statunitense in cui ogni anno vengono riportati i siti che aderiscono al citato patto e che vengono reputati attendibili, poiché offrono un livello adeguato di protezione dei dati personali.

[104] Cfr. *http://www.garanteprivacy.it/garante/doc.jsp?ID=30939*.

L'Italia ha vissuto un'esperienza similare, ricordando che, tra il 2001 e 2008, le tre grandi compagnie di telecomunicazione e fornitori di accesso ad internet (Telecom, Vodafone, H3g) hanno monitorato tutto il traffico da mobile o, più recentemente, il caso di *Google Street View* con i dati captati *"involontariamente".*

In detto caso, Google si è servita di apposite vetture, dotate di apparecchiature particolari, per fotografare a 360' migliaia di città, per offrire un servizio di mappe online.

Durante i "*viaggi*", Google ha ammesso di aver "i*nvolontariamente*" captato e raccolto migliaia di informazioni provenienti da reti wireless non protette[105].

A titolo di rimedio, a tal proposito, interviene l'art. 12 del GDPR che, al par. 1, prevede che il titolare del trattamento debba fornire un'informativa "*concisa", "trasparente", "intellegibile" e "facilmente accessibile".*

Per soddisfare tale criterio, dunque, sono necessarie: a) l'attività del titolare del trattamento deve risultare da un'indicazione ben visibile ed adeguatamente distinguibile nel testo dell'informativa; b) la possibilità, per l'interessato, di esprimere il proprio consenso (o di rifiutare il trattamento automatizzato dei dati)[106].

Se l'informativa consente all'interessato di essere perfettamente al corrente delle attività di trattamento dei dati, egli sarà in grado di esprimere un consenso consapevole. Questo è il motivo per cui il consenso (separato dall'informativa) deve essere indipendente rispetto agli altri possibili tipi di consenso espresso (come quello ad essere destinatario delle comunicazioni commerciali e promozionali).

L'interessato deve poter non sottostare inconsapevolmente al trattamento dei dati mediante profilazione (ed in generale tutti i processi automatici) e ciò è confermato dallo stesso Regolamento, all'art. 22 GDPR.

Secondo la norma, quando il processo decisionale è automatizzato, l'interessato ha il diritto di non essere sottoposto ad una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona.

L'art. 22 del GDPR riprende lo schema dell'art. 15 della Direttiva 95/46, ripresa successivamente dalla Direttiva e-Privacy (2002/58/CE), includendo la "*profi-*

[105] Cfr. E. EBASSOLI (a cura di), *Come difendersi dalla Violazione dei Dati su Internet, Diritti e Responsabilità*, Maggioli Ed. 2012, p. 136-137.
[106] Cfr. G.M. RICCIO – G. SCORZA – E. BELISARIO (a cura di), *Comm. GDPR e Normativa Privacy*, I ed. IPSOA 2018, art. 4.

lazione" tra le operazioni di trattamento che comportano un processo decisionale totalmente automatizzato al quale l'interessato ha diritto a non essere assoggettato se esso è in grado di produrre un effetto giuridico o avere effetti significativi analoghi nei suoi confronti.

La disposizione *de qua*, infatti, non sancirebbe solo il diritto dell'interessato a non essere oggetto di una decisione interamente automatizzata che possa avere effetti significativi ma conterrebbe un vero e proprio divieto rispetto al quale vengono poi previste talune eccezioni come il consenso esplicito[107].

Tale interpretazione, tuttavia, è stata ritenuta eccessivamente rigida e non aderente alla lettera del GDPR che non formulerebbe il principio alla stregua di un divieto bensì come garanzia/diritto per l'individuo.

3. L'attività di profilazione alla luce del GDPR e gli adempimenti del titolare del trattamento. Gli adempimenti aggiuntivi di *Privacy-by-design* e *Privacy-by-default*

L'art. 22 del GDPR, dunque, sembrerebbe ammettere la possibilità di assoggettare l'individuo a decisioni automatizzate; nel caso in cui esse possano avere un impatto significativo, allora l'individuo ha diritto a non essere assoggettato a tale decisione automatizzata.

A questo proposito, il GDPR introduce il consenso dell'interessato come nuova base giuridica (o eccezione) per giustificare tale trattamento e, atteso l'alto livello di rischio, impone il consenso *"esplicito",* che, in mancanza di una specifica definizione, è da ricollegare ad una dichiarazione affermativa attiva e specifica dell'interessato di fronte alla proposta di accettare o rifiutare un particolare trattamento[108].

In definitiva, la profilazione e i trattamenti decisionali automatizzati sopra descritti sono posti sul medesimo livello del trattamento delle categorie di dati particolari ex art. 9 GDPR, per cui è richiesto parimenti il consenso esplicito.

Secondo il Parere 2/2010 sulla pubblicità comportamentale online, adottato dal Gruppo di lavoro art. 29 per la protezione dei dati il 22.06.2010, il considerando 66 della dir. 2008/136/CE, che modifica la direttiva *e-privacy*, precisa che "*il consenso*

[107] Cfr. *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679.* Bruxelles, 17/EN, WP 251, p.9.
[108] Cfr. Working Party art. 29, *Opinion 15/2011 on the definition of consent*. Bruxelles, 01197/11/EN WP187, 0. 25.

dell'utente al trattamento può essere espresso mediante l'uso delle opportune impostazioni di un motore di ricerca (browser) o di un'altra applicazione "qualora ciò si riveli tecnicamente fattibile ed efficace, conformemente alle pertinenti disposizioni della direttiva 95/46/CE". Tale disposizione, più che costituire una deroga all'articolo 5, paragrafo 3, ricorda piuttosto che in questo ambiente tecnologico il consenso può essere espresso in modalità diverse, qualora ciò si riveli tecnicamente fattibile ed efficace e sia conforme agli altri requisiti pertinenti per un valido consenso. In questo contesto, è importante determinare le condizioni alle quali le impostazioni del browser soddisfano i requisiti di cui alla direttiva 95/46/CE e costituiscono pertanto un valido consenso "conformemente alla direttiva 95/46/CE".

Pertanto, sempre secondo il WP29, affinchè i browser o qualsiasi altra applicazione siano idonei a "*trasmettere*" un consenso valido è necessario considerare che *"a) i browser o le altre applicazioni respingono i cookie di terzi e che impongono all'interessato di compiere un'azione positiva per accettare l'impostazione e la continua trasmissione di informazioni contenute nei cookie da parte di determinati siti web sono idonei a trasmettere un consenso valido ed efficace. Per contro, se il browser è stato precedentemente impostato in modo tale da accettare tutti i cookie, il consenso non sarà conforme all'articolo 5, paragrafo 3, in quanto, in generale, esso non può costituire una vera manifestazione di volontà dell'interessato. Tale consenso non sarebbe né specifico né preliminare (al trattamento). Pur ammettendo che l'interessato possa aver deciso di mantenere le impostazioni di accettazione di tutti i cookie di terzi, i fornitori di reti pubblicitarie non possono realisticamente ritenere che la maggior parte degli interessati i cui browser sono impostati in modo da accettare i cookie abbia effettivamente esercitato questa scelta; b) i browser, assieme o combinati con altri strumenti di informazione, compresa la collaborazione tra fornitori di reti pubblicitarie ed editori, dovrebbero trasmettere informazioni chiare, complete e interamente visibili per garantire che il consenso sia pienamente informato. Al fine di soddisfare i requisiti di cui alla direttiva 95/46/CE, i browser dovrebbero trasmettere, a nome del fornitore di rete pubblicitaria, informazioni pertinenti circa le finalità dei cookie e l'ulteriore trattamento. Pertanto, avvisi generici senza espliciti riferimenti alla rete pubblicitaria responsabile del collocamento del cookie non sono soddisfacenti*".

Alla luce di tanto, gli adempimenti *privacy* da osservare per il trattamento di dati per finalità di marketing, si osservi, dapprima, che il titolare del trattamento deve

fornire ai destinatari delle comunicazioni promozionali un'informazione chiara e completa relativamente al trattamento dei dati.

Il titolare del trattamento deve, dunque, a) riportare chiaramente se intende utilizzare i dati per l'invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato e di comunicazione commerciale (attività che, secondo l'Autorità garante per la privacy, sono funzionali a perseguire un'unica finalità - *latu sensu* – di marketing e possono pertanto essere svolte a fronte di un unico consenso)[109]; b) indicare le modalità scelte per il trattamento dei dati, precisando se voler utilizzare telefonate automatizzate e modalità assimilate, previste dall'art. 130, co. I e II, d.lgs. 196/2003 (quali fax, e-mail, sms, mms e messaggi di altro tipo), oltre a quelle tradizionali (posta cartacea, telefonate con operatore); c) segnalare che il consenso prestato per l'invio di comunicazioni commerciali e promozionali, sulla base dell'art. 130 d.lgs. 196/2003, co. I e II, implica la ricezione di tali comunicazioni, non solo attraverso modalità automatizzate di contatto, ma anche attraverso quelle tradizionali, come posta cartacea e telefonate con operatore; d) riportare i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza (riferendosi sia a chi opera all'interno della struttura e abbia ricevuto apposita nomina a incaricato o a responsabile, sia ai soggetti esterni di cui il titolare si può avvalere – agenti, consulenti di marketing, società fornitrici di piattaforme per l'invio di email – che, in base al rapporto instaurato e al livello di autonomia riconosciuto in ordine al trattamento dei dati trasmessi, possono operare come responsabili o come autonomi titolari); e) segnalare se voler trasmettere i dati a partner commerciali, società del gruppo o soggetti esterni per consentire l'invio di loro comunicazioni promozionali (profilo che, oltre a rilevare in ordine all'indicazione delle finalità e dell'ambito di comunicazione, incide anche in termini di gestione del consenso); f) richiamare i diritti previsti dall'art. 7 del D.lgs. 196/2003 (Cod. privacy) e precisare che l'interessato può opporsi al trattamento effettuato per finalità di marketing esercitando tale diritto effettuato per finalità di marketing esercitando tale diritto; g) indicare che il diritto di opposizione dell'interessato al trattamento dei propri dati personali per finalità di marke-

[109] Linee guida in materia di attività promozionale e contrasto allo spam del 04.07.2013, *www.garante-privacy.it*

ting diretto, attraverso modalità automatizzate di contatto, si estende a quelle tradizionali e che resta salva la possibilità di esercitare tale diritto in parte, così come previsto ex art. 7 co. IV del cod. privacy[110].

Soffermandosi ancora sull'articolato del Regolamento, l'art. 25[111] introduce, altresì, il principio di *privacy by design* e *privacy by default*, che impone alle aziende di prevedere, già al momento inziale di un progetto di marketing, gli strumenti e le corrette impostazioni a tutela dei dati personali.

Sebbene l'elencazione offerta dalla disposizione circa le regole gravanti sul titolare del trattamento, per le finalità di responsabilizzazione, non sia da ritenersi esaustiva, si ricava, in ogni caso, un quadro coerente e nitido per orientare il titolare nelle scelte relative al trattamento, assicurandone la conformità alla legge e garantendo tutele.

Al titolare, infatti, spetterà di interessarsi dello stato dell'arte, dei costi di attuazione, della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nella prospettiva dei rischi connessi che siano idonei ad incidere sui diritti e le libertà delle persone cui i dati si riferiscono.

Analogamente, al titolare è richiesto, altresì, di agire con ponderazione e flessibilità, oltre che in modo dinamico e costante nel tempo.

Si consideri, al contempo, che tali obblighi risultano ad integrazione della previsione del precedente art. 24 in materia di "*responsabilità del titolare del trattamento*" e l'azione cui qui si fa riferimento è specifica, in quanto consiste, seguendo il tenore del testo, nell'adozione di misure tecniche ed organizzative adeguate proprio al conseguimento dello scopo, come si è appena identificato.

---

[110] R. RAPICAVOLI, *Privacy e Diritto nel web. Le Regole*, Dario Flaccovio Ed., 2017, pp. 127-128.

[111] "*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. 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".*

L'art. 25, poi, individua anche il momento temporale dell'adempimento gravante in capo al titolare, da ricondursi sia ad una fase preliminare del trattamento, durante la quale al titolare competono scelte ed oneri organizzativi e decisionali quali la predisposizione dei mezzi dei quali avvalersi, sia ad una fase operativa, consistente nella concreta effettuazione delle operazioni nelle quali si esplica il trattamento medesimo, sottintendendo che l'obbligo della consapevole adozione delle misure che, sotto il profilo tanto tecnico quanto organizzativo, tutelino con la maggiore efficacia possibile i principi di protezione dei dati è avvertito di importanza tale da imporne il rispetto, in sostanza, in ogni fase del trattamento, sin dal momento della progettazione (*privacy by design*) fino a quello della sua esecuzione.

Tra i promotori di tale approccio circa la progettazione iniziale dei sistemi di trattamento (*privacy by design*), Ann Cavoukian, *Information and Privacy Commissioner* dell'Ontario, già nel 1990, ne elaborò i concetti base, attraverso sette principi fondamentali e negli stessi anni, considerato l'impatto delle nuove tecnologie di carattere informatico e nel settore delle comunicazioni, si cominciò a diffondere il ricorso alle cd. *PETs* o *Privacy Enhancing Technologies*, ovverosia tecnologie "*aggiuntive",* idonee a mitigare gli effetti lesivi per gli interessati dei trattamenti dei dati che li riguardano[112].

Orbene, i concetti di *privacy by design* sono stati oggetto di discussione, altresì, in seno alla 32esima Conferenza mondiale dei Garanti per la protezione dei dati personali di Gerusalemme del 27-29.10.2010 (*ICDPPC International Conference of Data Protection and Privacy Commissioners*) all'esito della quale è stata adottata la *Resolution on Privacy by design*[113], da cui emergevano i sette principi fondamentali sottesi alla *privacy by design*: a) agire in modo proattivo e non reattivo, prevenendo anziché correggendo; b) la privacy come impostazione di default; c) la privacy incorporata nella progettazione; d) massima funzionalità: valore positivo, non valore zero; e) tutela fino alla fine dei processi, protezione piena per l'intero ciclo vitale; f) visibilità e trasparenza; g) rispetto della privacy dell'utente e dunque centralità del ruolo dell'interessato.

---

[112] ENISA, *The European Union Agency for Network and Information Security*, in un Rapporto del 2015, "*Readiness Analysis for the Adoption and Evolution of Privacy Enhancing Technologies – Methodology, Pilot Assessment and Continuity Plan" ha definite le PETs come "all kinds of technologies that support privacy or data protection features (e.g. technologies that make use of privacy design strategies or consider protection goals for privacy engineering*".
[113] www.gpdp.it, doc, web 1807346.

Tra le prime definizioni offerte per connotare la *privacy by design* si registra quella che ne definisce le principali caratteristiche e i primari obiettivi come "*the realization of values, in this case the principles of privacy and corresponding rules/regulations, via the physical design, technical specifications, architecture and/or computer code of the device, system or technology concerned, where applicable*"

Scopo della *privacy by design* è quello di progettare e sviluppare un sistema o un dispositivo, quali un software o un sistema hardware, in modo tale da supportare e concretare quei principi, valori e regole di protezione tramutandoli in obiettivi e funzioni, sì da rendere quel sistema o quel dispositivo *privacy-aware* o *privacy-friendly*. In definitiva, la *privacy by design* può intendersi come l'insieme di *"practical measures, in the form of technological and/or design-based solutions, aimed at bolstering privacy/data protection laws, better ensuring or almost guaranteeing compliance, and minimizing the privacy-intrusive capabilities of the technologies*"[114].

La base giuridica del cd. *Trattamento aggiuntivo* si rinviene nel regolamento stesso, non trovando esplicita legittimazione né nel consenso dell'interessato né in alcuno degli altri presupposti di cui all'art. 6 par. 1 lett. a) a f) (sulla liceità del trattamento), se si eccettua il richiamo alla condizione prevista alla lett. c che riconosce la liceità del trattamento "necessario per adempiere un obbligo legale al quale è soggetto il titolare".

L'obbligo legale in discorso, imposto dal Regolamento, sarà, dunque, assolto se il trattamento comprensivo delle attività ulteriori necessarie per una configurazione di *privacy by design* sarà condotto alla luce di tutti i principi disciplinati dall'art. 5 RPDP e trattasi dei principi di liceità, correttezza, trasparenza, limitazione della finalità, minimizzazione, esattezza, limitazione della conservazione, integrità e riservatezza, cioè sicurezza.

Un ulteriore principio meritevole di menzione è rappresentato, poi, dall'a*ccountability*, o responsabilizzazione del titolare sul quale grava l'onere di comprovare la conformità del proprio agire ai principi di cui sopra.

Senza soffermarsi sul contenuto dell'art. 5 che offre la disamina analitica dei suddetti principi, si osservi, tuttavia, che il rispetto del prefato principio di "*minimizzazione*", già enunciato nell'art. 5, viene espressamente richiamato dal qui vagliato art. 25 che, alla luce della *privacy by design*, è riferito sia ad una dimensione quantitativa

[114] K. DEMETRIUS, *Privacy-invading technologies: safeguarding privacy, liberty & security in the 21st century*, Leiden University Repository, 2014.

dei dati, imponendone il trattamento esclusivamente nella misura indispensabile al conseguimento dello scopo, sia ad una dimensione qualitativa, che consenta di assicurare il duplice obiettivo della conformità alla legge e della tutela degli interessati, attivamente privando le informazioni personali, il più possibile, del loro potere identificativo.

Ai sensi del richiamato art, 5, par. 1, lett. c), dunque, un'informazione personale ridondante, cioè non strettamente necessaria rispetto al fine perseguito dal trattamento, non potrà certamente essere utilizzata, ma i dati che, invece, risulteranno funzionali al trattamento dovranno essere impiegati in tutte le diverse operazioni che il trattamento prevede, secondo modalità meno identificative possibili, con minore impatto possibile.

Con l'impostazione predefinita sancita dall'art. 25, comprensiva della massiva proliferazione di dati ed informazioni, si è dato spazio alla mitigazione offerta dall'art. 5, con la sua finalità di responsabilizzare il trattamento de quo, con attenzione sia alla dimensione quantitativa dei trattamenti dei dati sia alla sua dimensione qualitativa.

E tanto si è riverberato, altresì, in altre disposizioni del Regolamento, rammentandosi gli artt. 34, secondo il quale il titolare può essere esonerato dalla comunicazione all'interessato di un *data breach* se "*ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione*"; o ancora l'art. 83, par. 2 lett. d) per il quale la determinazione delle sanzioni applicabili per il caso di violazioni dovrà tenere conto, tra l'altro, del "*grado di responsabilità del titolare del trattamento o del responsabile del trattamento tenendo conto delle misure tecniche e organizzative da essi messe in atto*" ai sensi dell'art. 25; l'art. 6, par. 4 lett. e) che richiede si consideri, tra l'altro, "*l'esistenza di garanzie adeguate, che possono comprendere la cifratura o la pseudonomizzazione"*[115].

[115] L'art. 4 del GDPR definisce la pseudonomizzazione nei termini seguenti: "*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 alali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche o organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile".* Il processo di pseudonomizzazione dei dati personali significa che tali attributi sono sostituiti da uno pseudonimo. *"(...) contrariamente ai dati anonimizzati, i dati pseudonimizzati rimangono dati personali e sono quindi soggetti alla legislazione in materia di portezione dei dati. Anche se la pseudonimizzazione può ridurre i rischi per gli interessati sul piano della sicurezza, essa non si sottrae all'ambito di applicazione del RGDP (...). Un modo per pseudonimizzae i dati è attraverso la crittografia degli stessi. Una volta che i dati sono pseudonimizzati, il collegamento ad un'identità esiste sotto forma di pseudonimo associato alla chiave di decifratura. Senza tale chiave, identificare i dati pseudonimizzati è difficile*". Cfr. *Manuale*

Analoghe considerazioni valgono anche per la previsione del par. 1 dell'art. 32 per il quale, "*tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, 9che comprendono tra le altre, se del caso: a) la pseudonimizzazione e la cifratura dei dati personali*.

Infine, può citarsi l'art. 37 che, per la valutazione preliminare di impatto, prevede la figura del *Data Protection Officer (DPO)* che va designato se: a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali; b) le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala, di categorie particolari di dati personali ex art. 9 o di dati relativi a condanne penali e a reati ex art. 10.

Il DPO ha, dunque, il precipuo compito di informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal Regolamento nonché dalle altre disposizioni UE relative alla protezione dei dati; di sorvegliare l'osservanza del Regolamento, delle altre disposizioni dell'Unione Europea o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo; di fornire, laddove richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati e di sorvegliarne lo svolgimento ai sensi dell'art. 35; di cooperare con l'autorità di controllo per le questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'art. 36.

Correlativamente alla *privacy by design*, l'art. 25 par. 2 esplicita il principio di *privacy by default,* che appare riproduttivo del principio già rammentato di minimizzazione di cui all'art. 5, con l'unico discrimine rappresentato dalla specificazione per

sul diritto europeo in materia di protezione dei dati, 2018, pubblicazione istituzionale del Consiglio d'Europa.

la quale le misure di minimizzazione prescelte dal titolare devono essere predisposte in modo da garantire che la selezione dei soli dati da trattare per il conseguimento delle finalità stabilite sia l'esito di una impostazione predefinita.
Il titolare, dunque, dovrà garantire che, per impostazione predefinita, siano trattati solo i dati personali necessari in relazione a ciascuna finalità specifica del trattamento e che la quantità dei dati raccolti e la durata della loro conservazione non eccedano il minimo necessario per le finalità perseguite.

Ancora una volta è il principio della misura, della minimizzazione, a costituire una modalità di trattamento, idonea ad impostare ex ante la massima protezione dei dati attraverso il loro minimo trattamento, sia nella fase iniziale di raccolta sia nelle fasi successive.

L'utilizzo di informazioni per l'accesso ad un servizio o ad un prodotto dovrà, pertanto, essere inizialmente limitato al minimo indispensabile per consentirne la fruizione, di modo che sia rimesso interamente all'interessato un effettivo, concreto potere di scelta in ordine alla possibilità di consentire o meno un utilizzo eventualmente più ampio dei suoi dati.

Secondo la posizione dell'orami famoso WP29, con la citata disposizione si realizza uno tra i principali obiettivi posti dal GDPR, quello della responsabilizzazione del titolare, "*per l'attuazione efficace dei principi di protezione dei dati*", perno di una possibile architettura giuridica generale dei sistemi[116].

[116] Cfr. parere 3/2010 – WP173 sul principio di responsabilità, 13.07.2010.

"PREVENIRE È MEGLIO CHE CURARE": IL COMPITO DELL'AVVOCATO IN CASO DI DATA BREACH

Di Livia Smoraldi e Marta Strazzullo

SOMMARIO. 1. Aumento dei rischi degli attacchi Hacker: telelavoro – 2. L'avvocato come responsabile del trattamento dati – 3. Adozione di buone prassi per la sicurezza dei dati – 4. Obblighi e doveri del professionista forense in caso di violazione dei dati.

The aim of this article is to identify the proper behavior of the lawyer as responsible of the treatment of his clients personal data. After identifying the current historical context in which personal data breaches have increased, the article identifies the duties that the lawyer must fulfill to prevent data breaches and the obligations to which he is bound after the violation.

1. Aumento dei rischi degli attacchi Hacker: telelavoro.

L'epidemia da Covid-19 ha senza dubbio stravolto le nostre abitudini. Telelavoro, *smart-working*, lavoro a distanza, qualunque sia il nome che si vuole attribuire a tale fenomeno, è innegabile che un nuovo modo di svolgere le quotidiane attività ci ha travolto.

Lo stesso non può negarsi per i professionisti forensi: una classe che, particolarmente ancorata alle tradizioni, ai codici ed ai faldoni, si è trovata ormai ad affrontare un repentino cambiamento che ha visto un accesso per nulla indiscreto della tecnologia nell'esercizio della professione. Chi avrebbe utilizzato tanto Microsoft team se non ci fosse stato il Covid? Probabilmente alcuni non avrebbero neanche avuto conoscenza di tale strumento se non fosse intervenuta una pandemia.

Ma qual è uno degli effetti più pericolosi di questa improvvisa *"digitalizzazione"*? Probabilmente quella che fa maggiormente tremare ogni azienda o professionista: l'aumento esponenziale di attacchi informatici.

Nel corso nel corso del convegno "*L'hacker nel faldone*"[117], organizzato dal Consiglio dell'ordine degli avvocati di Roma, a tal proposito, sono stati riportati dati particolarmente preoccupanti, idonei ad attestare come, ad oggi, gli studi legali siano nel mirino degli *Hacker*.

Oren Elimelech, consulente del Governo israeliano per la *cybersecurity*, ha, nel corso del succitato convegno, fornito un riepilogo del 2020 sottolineando che nel corso dell'anno della pandemia, in Italia, ci sono stati circa 2332 attacchi *hacker*, e quindi un attacco ogni quattro ore. Un dato che diventa ancor più preoccupante se si considera che nel 2019 si sono contati circa 600 attacchi informatici in meno. I mesi in cui è stata registrata una maggiore criticità sono stati ottobre e dicembre 2020. Più segnatamente, lo scorso dicembre ci sono state 227 invasioni informatiche a fronte delle 157 segnalate nello stesso mese nel 2019. Il dato è invece più che raddoppiato rispetto a quello registrato nel dicembre 2018, in cui gli attacchi denunciati furono "solo" 106. Il perché di tali attacchi risiede nella richiesta di denaro.

Per quanto attiene, invece, alla natura di tali attacchi, Oren Elimelech ha fornito delucidazioni anche in tal senso: il 40% degli attacchi proviene dai malware[118], mente il 9% degli attacchi può definirsi "mirato" ovvero è avvenuto nei confronti di soggetti individuati in precedenza[119].

Lo scenario che si è palesato in Italia ha determinato senza dubbio grade preoccupazione e fa emergere ancor di più la necessità, per aziende e professionisti, di adottare, per le proprie attività, tutte le fondamentali precauzioni volte a garantire un'idonea *cybersecurity*.

Si aggiunga che gli odierni attacchi informatici sono molto più sofisticati rispetto al passato, ciò significa che gli *hacker* hanno acquisito una tale dimestichezza che gli consente di eludere anche gli strumenti di sicurezza eventualmente apposti, perché i *"pirati informatici"* sono sempre più capaci di sfruttare le eventuali vulnerabilità delle vittime.

---

[117] "*L'hacker nel faldone*" convegno patrocinato dall'Ordine degli Avvocati di Roma. È possibile consultare il convegno al seguente link: *https://www.youtube.com/watch?app=desktop&v=japGYf8qefA&feature=youtu.be*

[118] Malware è un termine utilizzato per indicare un programma idoneo ad arrecare danno ed a mettere a rischio un sistema. I malware invadono computer, sistemi, reti, tablet e assumono il controllo delle operazioni del dispositivo, interferendo, in tal modo, con il loro normale funzionamento. Sebbene i malware non possano danneggiare gli hardware fisici o le attrezzature di rete sono ugualmente capaci di rubare, criptare o eliminare i dati, alterare o compromettere le funzioni del dispositivo e controllare le attività con esso svolta dagli utenti assolutamente ignari del tutto.

[119] Sul punto: M. DAMIANI, *Nel 2020 un attacco hacker ogni quattro ore",* in *italiaoggi.it*, 023, 2021, *https://www.italiaoggi.it/news/nel-2020-un-attacco-hacker-ogni-quattro-ore-2505740*

Con particolare riferimento alla professione forense, come considerato dal Consiglio Nazionale Forense, nelle linee guida fornite, i dati ai quali il professionista, esercitando le proprie attività quotidiane, accede sono, per loro natura, dati estremamente sensibili: salute, orientamento religioso, politico o sessuale, dati giudiziari, situazione familiare, dati di minori etc[120].

L'avvocato si serve della categoria di dati più delicata il cui trattamento deve quindi rispettare una logica ben precisa e strettamente legata al rapporto di fiducia che intercorre tra avvocato e cliente nonché al rispetto delle regole deontologiche, tra le quali spicca l'obbligo di garantire il segreto professionale.

Un attacco informatico presso uno studio legale potrebbe determinare la diffusione di dati sensibili degli interessati ed avere effetti tali da ledere i diritti e la libertà dei clienti coinvolti, sicché è indispensabile per il professionista forense adottare tutte le prassi fondamentali per garantire la massima sicurezza dei dati trattati.

Per tali ragioni, gli studi legali, indipendentemente dalle proprie dimensioni, sono stati chiamati a conformare la propria attività alle previsioni del Regolamento UE 2016/679 relativo alla protezione dei dati personali.

Più segnatamente, gli avvocati, al fine di scongiurare i pericoli connessi al trattamento dei dati da loro sviluppato dovranno:

- definire le finalità del trattamento nonché le modalità di trasmissione dei dati trattati;
- attuare precise misure di sicurezza;
- informare e preparare adeguatamente tutto lo staff legale che si trova a trattare i dati dei clienti.

Il professionista forense, inoltre, è tenuto al rispetto di dettagliate procedure in caso di *data breach* al fine di evitare che un attacco informatico abbia gravi e spiacevoli conseguenze.

L'elaborato che segue mira a definire obblighi e doveri posti in capo al professionista forense, nonché a delineare un chiaro quadro delle misure da adottare in caso di "attacco informatico".

[120] CNF, *Il GDPR e l'avvocato,* consultabile sul sito *https://bit.ly/3u8F7Vy.*

2. L'avvocato come responsabile del trattamento dati.

In via preliminare, è doveroso sottolineare che lo studio legale è senza dubbio una struttura complessa che si compone spesso di più professionisti ai quali si affiancano diversi collaboratori: praticante, segretario, commercialista sono solo alcuni dei soggetti che interagiscono con lo studio.

Pertanto, è doveroso comprendere il ruolo rivestito da ciascuno di essi nel contesto in cui operano.

A tal fine è importante definire quali siano, in via generale, gli utenti dei dati personali, ovvero i titolari del trattamento e i responsabili del trattamento[121].

Le funzioni di *titolare* e *responsabile del trattamento* comportano in capo ai soggetti che rivestono tali qualifiche la responsabilità giuridica derivante dal rispetto degli obblighi previsti dal diritto in materia di protezione dei dati. Nel settore privato questa responsabilità grava, di solito, su una persona fisica o giuridica, mentre nel settore pubblico spetta, generalmente, ad un'autorità.

La differenza tra questi soggetti si radica nel fatto che il titolare del trattamento è la persona fisica o giuridica che determina le finalità e i mezzi del trattamento mentre il responsabile del trattamento è la persona fisica o giuridica che tratta i dati per conto del titolare del trattamento, nel rispetto delle istruzioni da quest'ultimo impartite.

"*In linea di principio, il titolare del trattamento esercita il controllo sul trattamento e su chi ne ha la responsabilità, compresa la responsabilità legale*"[122].

Con riferimento al dato normativo, ai sensi dell'art. 4 comma 7 del Regolamento europeo per la protezione dei dati personali, per **titolare del trattamento** si intende *"la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri".*

[121] M. ALLEGRI, in *Ubi social, Ibi ius. Fondamenti costituzionali dei social network e profili giuridici della responsabilità dei provider,* Milano, 2018, considera come la distinzione fra "titolare" e "responsabile" del trattamento dei dati non era presente nella disciplina antecedente: la direttiva europea parlava solo di data controller, tradotto come "responsabile" del trattamento. Invece, il Regolamento introduce una differenza fra il soggetto che determina le modalità e i mezzi del trattamento (il titolare) e quello che effettua il trattamento per conto del titolare (il responsabile).
[122] Cfr. *Manuale sul diritto europeo in materia di protezione dei dati*, Lussemburgo, Ufficio delle pubblicazioni dell'Unione europea, 2018, p. 115.

Il medesimo Regolamento prevede altresì la figura dei **contitolari del trattamento** stabilendo, all'art. 26 che *"allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento. Essi determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal presente regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14, a meno che e nella misura in cui le rispettive responsabilità siano determinate dal diritto dell'Unione o dello Stato membro cui i titolari del trattamento sono soggetti. Tale accordo può designare un punto di contatto per gli interessati".*

Dunque, focalizzando la nostra attenzione sull'attività svolta all'interno di uno studio legale è indubbio che l'Avvocato, titolare dello studio stesso, rivesta la funzione di titolare del trattamento.

Laddove, invece, questi collabori con altri colleghi, per la sussistenza di un mandato comune, tutti dovranno, in comune accordo, determinare le finalità e le modalità del trattamento. In tal caso, gli avvocati saranno contitolari del trattamento e, pertanto, ai sensi dell'art. 24, 2 co., GDPR, saranno tenuti alla stesura di un accordo con cui definire *"i rispettivi ruoli e i rapporti dei contitolari con gli interessati"*.

Al contrario, laddove ogni professionista abbia autonomo mandato per precise attività, seppure inerenti alla medesima controversia, non verrà ad integrarsi una collaborazione e, quindi, ognuno sarà un autonomo titolare e tratterà i dati con le modalità da esso stabilite.

Dunque, la contitolarità deve essere considerata e valutata caso per caso, sulla base dell'effettivo apporto professionale e strategico decisionale di ciascun avvocato. Si ponga, ad esempio, il caso in cui Tizio agisca per diffamazione, sia in sede penale che in sede civile al fine di ottenere una tutela risarcitoria. In tal caso, il legale di Tizio in sede penale sarà Sempronio, mentre il legale in sede civile sarà Caio. Avendo entrambi gli avvocati incarichi specifici in ambiti diversi e autonomi non si parlerà di contitolari ma ognuno tratterà i dati personalmente.

Diverso è il caso in cui gli avvocati siano membri di uno studio associato. In tal caso titolare del trattamento è l'ente giuridico, in persona del legale rappresentante[123].

[123] Gruppo di lavoro articolo 29 (2010), parere 1/2010 sui concetti di «responsabile del trattamento» e «incaricato del trattamento», WP 169, Bruxelles, 16 febbraio 2010: "*sarebbe preferibile considerare*

Nonostante ciò, il mandato conferito dall'assistito all'avvocato fa sì che titolare del trattamento sia l'avvocato che riceve il mandato, dato il rapporto di fiducia si instaura con il conferimento della procura.

Come anticipato, diversa, rispetto a quella di titolare, è la figura del **responsabile del trattamento**.

Ai sensi dell'art. 4 paragrafo 8 del GDPR per responsabile del trattamento si intende: *"la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento".*

Pertanto, può intendersi responsabile del trattamento l'avvocato domiciliatario che, tratta i dati del cliente, non per conto proprio ma per conto del *dominus* che, quindi, avrà le vesti di titolare del trattamento.

Ancora, è responsabile del trattamento il commercialista che collabora con lo studio legale per gestirne la contabilità.

È compito dell'avvocato, titolare del trattamento, scegliere i responsabili del trattamento prestando particolare attenzione alle capacità degli stessi e valutando la sussistenza di tutti gli strumenti necessari per garantire un trattamento conforme alle previsioni del Regolamento UE al fine di assicurare la tutela dei diritti dell'interessato, come previsto all'art. 28 del regolamento stesso.

Più segnatamente, il comma 3 dell'art. 28 prevede che i trattamenti effettuati dal responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri.

Il contratto o altro atto giuridico prevede, in particolare, che il responsabile del trattamento: *"a) tratti i dati personali soltanto su istruzione documentata del titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento; in tal caso, il responsabile del trattamento informa il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;*

b) garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;

c) adotti tutte le misure richieste ai sensi dell'articolo 32;

---

come titolare del trattamento la società o l'organismo in quanto tali piuttosto che una specifica persona al loro interno".

d) rispetti le condizioni di cui ai paragrafi 2 e 4 per ricorrere a un altro responsabile del trattamento;
e) tenendo conto della natura del trattamento, assista il titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III;
f) assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli 32 a 36, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;
g) su scelta del titolare del trattamento, cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati;
h) metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato".

Infine, il responsabile del trattamento ha la facoltà di nominare a sua volta un **sub-responsabile** ma tale nomina è subordinata al consenso del titolare del trattamento.

Negli studi legali, inoltre, interagiscono altri soggetti, nel rispetto delle direttive impartite dal titolare o dal responsabile del trattamento: si pensi, ad esempio, ai dipendenti, segretari, stagisti, praticanti ecc. Tali soggetti saranno pertanto **autorizzati al trattamento**, ai sensi dell'art. 4 comma 10 GDPR. Anche in tal caso l'avvocato dovrà indicare per iscritto il soggetto autorizzato e dovrà dare precise indicazioni circa l'attività di trattamento.

Dunque, in conclusione si riporta quanto specificato dal Garante per la protezione dei dati personali, già con il chiarimento del 3 giugno 2004 n. protocollo 22457, inviato al Consiglio Nazionale Forense:
- *"il titolare del trattamento è il soggetto cui competono le decisioni di fondo in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza";*

- "quando l'attività professionale è prestata individualmente, il titolare del trattamento è la persona fisica dell'avvocato esercente. Ad analoga conclusione deve giungersi nel caso di attività svolta congiuntamente da due professionisti, i quali assumono in questa ipotesi la qualità di contitolari del medesimo trattamento";
- "quando, invece, l'attività è svolta in forma societaria o da un'associazione professionale o da una società tra avvocati, il titolare è l'entità nel suo complesso. In questo caso, gli adempimenti previsti dal Codice vanno pertanto attuati in termini unitari, evitando la loro frammentazione o ripetizione a cura dei singoli professionisti.
- Il responsabile esegue i compiti specificati analiticamente per iscritto dal titolare del trattamento, il quale deve vigilare sulla puntuale osservanza delle disposizioni in materia di trattamento. Può trattarsi anche di un soggetto esterno -persona fisica o giuridica- che svolga prestazioni strumentali e subordinate alle scelte del titolare del trattamento. Per esigenze organizzative possono essere designati responsabili anche più soggetti, mediante eventuale suddivisione di compiti.
- Tutte le persone fisiche che hanno accesso ai dati a vario titolo (avvocati, praticanti, collaboratori e personale amministrativo) devono essere designate per iscritto quali incaricati del trattamento. L'atto di designazione, da parte del titolare o dell'eventuale responsabile, deve individuare l'ambito del trattamento consentito agli incaricati, i quali devono attenersi alle istruzioni impartite[124]".

Con riferimento, invece, alla tipologia di dati trattati dal professionista forense nell'ambito del suo rapporto con il cliente, è indubbio che tra questi rientrino tutti i dati di volta in volta considerati indispensabili per la corretta gestione dell'attività giudiziaria.

Gli avvocati, generalmente, hanno un ambito di competenza particolarmente ampio sicché i dati da essi trattati potrebbero spaziare particolarmente: possono essere relativi alla vita privata del cliente nonché rivelarne l'origine razziale, le opinioni etniche, politiche, le credenze religiose o filosofiche, l'appartenenza sindacale. Ancora, il professionista forense potrebbe trattare dati genetici, dati biometrici, dati sanitari.

[124] Cfr. Garante per la protezione dei dati personali, *Chiarimenti sui principali adempimenti in materia di protezione di dati personali nello svolgimento dell'attività forense,* Prot n. 2245, Roma, 3 giugno 2004. Il documento è consultabile al seguente link: *https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1007280*

Alcuni di tali dati rientrano nella c.d. categoria di **dati sensibili** il cui trattamento è, in linea generale, limitato dall' articolo 9, comma 1 del GDPR. [125]

Ciononostante, il citato dato normativo contempla al comma 2.f) una deroga al limite di tale trattamento, potendosi effettuare lo stesso per *"accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionale".*

Dunque, è indubbio che gli avvocati possano trattare dati particolari nell'esercizio della propria professione purché necessari a garantire la miglior difesa del proprio cliente.

L'avvocato potrebbe, inoltre, trovarsi a trattare dati giudiziari. In tal caso, l'articolo 10 del GDPR prevede espressamente che tale trattamento possa essere effettuato solo sotto il controllo dell'autorità pubblica, o regolamentato da disposizioni specifiche previste dalla legge nazionale.

3. Adozione di buone prassi per la sicurezza dei dati.

Come già anticipato, nell'esercizio delle proprie funzioni difensive, l'avvocato ha accesso a dati di diversa natura. Tra questi, ritroviamo sicuramente i dati che riguardano gli aspetti più intimi della vita personale del cliente.

Proprio in relazione alla tutela di tali dati, l'interrogativo da porsi in questa sede è se l'avvocato, in ottemperanza all'obbligo dapprima normativo e, successivamente, morale del segreto professionale, debba o meno adottare degli accorgimenti utili a prevenire l'eventuale diffusione illecita non solo dei dati personali del cliente trattati in via digitale ma anche di quelli tenuti dallo stesso analogicamente.

Sicuramente, per i dati analogici l'avvocato avrà la possibilità di agire in via preventiva mettendo in sicurezza i documenti e gli atti che li contengono. Proprio per la sicurezza di tali documenti e fascicoli, oltre al debito buon senso proprio di ogni professionista, la Commissione del Consiglio Nazionale Forense in materia di privacy ha individuato le necessarie e doverose misure di sicurezza da predisporre fisicamente nel proprio studio legale.

[125] È bene rammentare che, proprio in relazione a tali categorie di dati, l'articolo 9 del GDPR, rubricato "*Trattamento di categorie particolari di dati personali*" stabilisce al primo comma il principio secondo cui "*È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona*".

Tra queste, ritroviamo, ad esempio, la limitazione dell'accesso di terzi all'ufficio, il non archiviare fascicoli o documenti contenenti dati personali in locali dello studio accessibili a tutti nonché l'installazione allarmi nei locali dello studio.

Tuttavia, pur scongiurando il pericolo di una diffusione illecita di dati contenuti nei fascicoli analogici mediante la messa in sicurezza dello studio professionale e dei fascicoli stessi, la minaccia più grande resta ancorata ai documenti ed ai fascicoli gestiti dal professionista digitalmente.

In tal senso, viene, ancora una volta, in aiuto il GDPR che accanto alla predisposizione dei generici principi relativi al trattamento dei dati personali idonei a limitare gli effetti nefasti di diffusioni "non consentite" quali la *finalità del trattamento*[126] - ossia il limite all'utilizzo degli stessi ai soli obiettivi di tutela, consulenza e difesa perseguiti con specifico mandato dell'avvocato-, la *necessità e proporzionalità*[127] - vale a dire il principio secondo il quale il trattamento deve essere adeguato, pertinente e necessario allo scopo-, la *durata limitata* - cioè la limitazione del trattamento al tempo necessario all'espletamento degli incarichi-, la *sicurezza e riservatezza*[128] ed il *rispetto del diritto delle persone,* introduce ulteriori principi e doveri cui l'avvocato è tenuto ad uniformarsi in via preventiva per evitare "*incidenti nella sicurezza*"[129].

Primo fra questi ultimi è sicuramente il principio di *responsabilizzazione* (o cd. *accountability*), statuito all'art. 5 comma 2 del GDPR secondo il quale *"Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo («responsabilizzazione»)".*

Tale principio richiede un profondo cambiamento nel trattamento delle informazioni di cui viene in possesso l'avvocato in virtù del proprio mandato, ed impone allo stesso - nella qualità di titolare del trattamento dei dati del proprio cliente - un

[126] Di cui all'art. 5 GDPR rubricato "*Principi applicabili al trattamento di dati personali*" secondo il quale "*i dati personali sono … b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità"*.

[127] Il GDPR, a differenza del precedente codice della Privacy italiano che imponeva espressamente all'art. 3 il rispetto del principio di necessità nel trattamento dei dati, non fa esplicito riferimento al principio di necessità, ma fa riferimento alla "*minimizzazione del trattamento*", che ne costituisce una sottocategoria, e che richiede che i dati personali debbano sempre essere "*c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati*".

[128] Sempre l'art. 5, comma 1, lett. f), stabilisce che i dati personali devono essere "*trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali*". L'intero trattamento dovrà quindi essere sicuro e non solo i dati come prodotto finale.

[129] Secondo la Nortonlifelock – azienda statunitense che produce software per la sicurezza e antivirus leader del settore per PC, Mac e dispositivi mobili – infatti, "*A data breach is a security incident in which information is accessed without authorization*".

comportamento proattivo e concreto poiché, considerato quale unico responsabile del trattamento dati, avrà l'obbligo giuridico di adottare misure tecniche ed organizzative adeguate a garantire che il trattamento dei dati sia conforme al Regolamento Europeo e dunque, dovrà sempre essere in grado di dimostrare la pedissequa osservanza dei "*principi applicabili al trattamento dati*" disciplinati dall'art. 5 GDPR.[130]

Su tale ultimo compito, che potremmo definire "*obbligo processuale*" dell'avvocato, l'articolo 24 GDPR stabilisce che "*Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario*".

Pertanto, il principio di "*responsabilizzazione*", pur non essendo in sé e per sé una vera e propria misura di sicurezza, è il principio attorno al quale l'avvocato dovrà costruire qualsiasi politica di sicurezza dei dati e, nella pratica, il rispetto di quest'ultimo, si risolve non solo nell'adozione misure adeguate alla struttura del singolo trattamento ma anche nell'elaborazione caso per caso di misure volte a garantire, di fatto, il pieno rispetto delle norme del GDPR.

L'avvocato non potrà dunque più limitarsi all'adozione delle cd. *misure minime*[131].

Pertanto, la responsabilizzazione, se da un lato dà maggiore discrezionalità all'avvocato nel decidere attraverso quali misure tutelare i dati personali del proprio cliente, dall'altro, lega questa maggiore libertà ad una grossa responsabilità: quella di dimostrare come e per quali motivazioni si è arrivati a determinate decisioni, con tanto di documentazione delle scelte fatte.

Al fine di agevolare la documentazione delle misure predisposte dall'avvocato, l'art. 30 del GDPR impone ad "*ogni titolare del trattamento e, ove applicabile,* al *suo rappresentante* di tenere *un registro delle attività di trattamento svolte sotto la propria responsabilità*"[132].

---

[130] Tali principi sono, nello specifico: lett. a) «liceità, correttezza e trasparenza»; lett. b) «limitazione della finalità»; lett. c) «minimizzazione dei dati»; lett. d) «esattezza»; lett. e) «limitazione della conservazione»; lett. f) «integrità e riservatezza».

[131] Dopo l'abrogazione dell'"*allegato B*" del Codice della Privacy viene meno quel sistema di tutele predisposto dalle cd. *misure minime* che, individuando in anticipo specificamente tutti i necessari oneri che il titolare del trattamento doveva porre in essere, gli assicurava il rispetto dello standard minimo legislativamente previsto deresponsabilizzandolo.

[132] In realtà, l'art. 30 comma 5 del GDPR statuisce altresì che "*Gli obblighi di cui ai paragrafi 1 e 2 non si applicano alle imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo*

Il registro - che deve essere predisposto in forma scritta, anche elettronica (es. foglio *excel*) - costituisce uno degli strumenti preliminari di cui l'avvocato dovrà dotarsi per ottemperare al principio di "*responsabilizzazione*", in quanto, essendo strumento idoneo a fornire un quadro aggiornato dei trattamenti posti in essere all'interno della propria organizzazione sarà indispensabile per ogni attività di valutazione o analisi del rischio e dunque preliminare rispetto alle stesse[133].

Tale strumento aiuterà l'avvocato a "tracciare" i dati in base al loro rischio e dunque a renderlo maggiormente consapevole della natura dei dati raccolti per l'esercizio della propria attività.

Non solo, tale strumento permetterà all'avvocato di tener sempre conto della loro conservazione, della loro finalità, della loro conformità al regolamento, del loro stato di conservazione nonché delle misure di sicurezza adottate e della loro eventuale perdita accidentale.

Accanto al principio dell'"*accountability*" che fa da perno alla politica di sicurezza adottata da ogni responsabile di trattamento, sempre nell'ottica preventiva, fondamentale risulta l'introduzione della cd. *valutazione d'impatto* cui il titolare del trattamento è tenuto ad eseguire non solo nei casi tassativamente individuati dall'art. 35 del GDPR ma anche ogni qualvolta sia probabile che un tipo di trattamento possa creare un elevato rischio per i diritti e le libertà delle persone fisiche.

Tale rischio sarà, ad esempio, maggiore nei casi in cui ci troviamo di fronte al monitoraggio sistematico e globale dei comportamenti del cliente, oppure difronte al gran numero dei soggetti interessati di cui sono magari trattati dati sensibili, o anche innanzi una combinazione di questi e altri fattori (persone vulnerabili, dati personali su larga scala, uso innovativo).[134]

Innanzi a tali situazioni, il GDPR impone ai titolari del trattamento – l'avvocato nel nostro caso - di svolgere una valutazione di impatto prima di dare inizio al trattamento, imponendogli, altresì, di consultare l'Autorità di controllo nel caso in cui le misure tecniche e organizzative da loro stessi predisposte per mitigare l'impatto del

1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10", nonostante il limite posto alle imprese ed organizzazioni con meno di 250, l'obbligo di tenere un registro di trattamento pare applicabile all'avvocato data la non occasionalità del trattamento dei dati personali del suo cliente e le loro particolari caratteristiche.

[133] Regolamento UE. Le istruzioni del Garante privacy sul registro dei trattamenti: FAQ sul Registro delle attività di trattamento.

[134] Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679.

trattamento non siano ritenute sufficienti - e cioè, quando il rischio residuale per i diritti e le libertà degli interessati resti comunque elevato-.[135]

Pertanto, l'avvocato, al fine di prevenire i rischi legati al trattamento dei dati sensibili e dato il suo costante contatto con i fattori di rischio indicati dalle linee-guida WP29, dovrà interpretare l'obbligo di valutazione d'impatto più che come un adempimento *una tantum*, come un vero e proprio processo soggetto a revisione continua.
Inoltre, sempre in chiave preventiva, il professionista forense, dopo aver selezionato con premura i soli dati necessari al raggiungimento dello scopo (cd. *principio di minimizzazione*), dovrà definire una rigida politica di durata e di conservazione dei dati nel suo ufficio. [136]

I dati dovranno dunque essere conservati solo per il tempo necessario al completamento del fine perseguito durante la loro raccolta, e potranno essere tenuti lungo tutta la durata del mandato professionale.

Solo in via eccezionale - sia al fine di conseguire il diritto al compenso, sia per resistere ad eventuali azioni di responsabilità - l'avvocato, prima della loro definitiva cancellazione, potrà prolungare la raccolta dati lungo tutto il periodo di prescrizione ordinaria.

In via meno teorica e più pratica, la Commissione CNF in materia di privacy individua nelle linee guida pubblicate nel 2018 altre buone prassi cui l'avvocato è tenuto a seguire per garantire la sicurezza dei dati personali dei propri clienti.

Tra queste, ritroviamo sicuramente la definizione di idonee misure di identificazione dell'utilizzatore/utente mediante la predisposizione di password minime di otto caratteri contenenti lettere maiuscole, minuscole, numeri e caratteri speciali e, soprattutto in presenza di un *teamwork,* le stesse linee guida consigliano al professionista forense di non condividere le stesse - o quantomeno di non scriverle su fogli -, di evitarne la preregistrazione, provvedendo talvolta a cambiarla regolarmente.

---

[135] L'art. 35 comma 2 GDPR impone altresì al *titolare del trattamento* di consultarsi *con il responsabile della protezione dei dati, qualora ne sia designato* uno.

[136] In tal senso, il comma 1 dell'art. 2 del Regolamento n. 512/2009 (Regole deontologiche relative ai trattamenti di dati personali effettuati per svolgere investigazioni difensive o per fare valere o difendere un diritto in sede giudiziaria) statuisce che "*L'avvocato organizza il trattamento anche non automatizzato dei dati personali secondo le modalita' che risultino piu' adeguate, caso per caso, a favorire in concreto l'effettivo rispetto dei diritti, delle liberta' e della dignita' degli interessati, applicando i principi di finalita', proporzionalita' e minimizzazione dei dati sulla base di un'attenta valutazione sostanziale e non formalistica delle garanzie previste, nonche' di un'analisi della quantita' e qualita' delle informazioni che utilizza e dei possibili rischi*".

Ove invece risulti assolutamente necessario condividerle con i propri colleghi o assistenti, la Commissione del CNF suggerisce all'avvocato titolare del trattamento di istruire gli stessi sull'eventuale utilizzo.

Anzi, proprio in presenza di questi ultimi, il Consiglio raccomanda all'avvocato di fornire al collaboratore un supporto costante mediante la predisposizione di uno specifico regolamento di utilizzo del computer da inserire al regolamento interno d'ufficio.

L'avvocato potrà poi provvedere alla difesa della propria navigazione rimuovendo le autorizzazioni di accesso obsolete.

Ancora, sempre nell'ottica di un efficiente e sicuro "*mobile computing*", l'avvocato dovrà fornire mezzi di crittografia sia per computer portatili sia per i dispositivi di archiviazione rimovibili e dovrà altresì conservare tali supporti in luoghi sicuri.

Non solo: se da un lato dovrà evitare di memorizzare i dati personali sensibili del cliente, dall'altro dovrà incrementare l'esecuzione dei backup.

Tuttavia, pur essendo sicuramente applicabile anche all'ambito della sicurezza digitale il motto "*prevenire è meglio che curare*", l'adozione di tutte le buone prassi per la sicurezza dei dati potrebbe non essere sufficiente a contrastare una diffusione illecita di questi ultimi.

4. Obblighi e doveri del professionista forense in caso di violazione dei dati

L'art. 4 del GDPR definisce la violazione dei dati personali (cd. *data breach*) come "*la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati*".

Stando a tale definizione, la violazione dei dati personali ossia il c.d. *data breach*, non è solo frutto di un evento doloso come un attacco informatico, ma può essere qualsiasi violazione accidentale come, ad esempio, un eccesso abusivo, un incidente (es. incendio dello studio e dei fascicoli o calamità naturale), la sottrazione illecita di documenti (es. furto della valigia contenente i documenti), e così via.[137]

In presenza di *data breach*, in virtù degli artt. 33 e 34 del GDPR, l'avvocato – quale responsabile del trattamento – dovrà documentare ed eventualmente esibire su

[137] Un *data breach* è dunque una violazione della sicurezza che comporta – in maniera accidentale o illecita – la distruzione, la perdita, l'alterazione, la divulgazione o l'accesso non autorizzato di dati di natura personale trasmessi, conservati o altrimenti elaborati.

richiesta del Garante, ogni avvenuta violazione unitamente alle circostanze che l'hanno causata, alle sue conseguenze e ai provvedimenti adottati per porvi rimedio[138].

L'avvocato, dunque, a norma dell'art. 33 del GDPR, sarà tenuto ad una duplice comunicazione disciplinata rispettivamente dal comma 1 – all'autorità di controllo competente - e dal comma 2 – al titolare del trattamento -.

Il comma 1 dell'art. 33 GDPR prevede che "*In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo".*

Dunque, in applicazione al principio generale di *accountability*, sarà sempre rimessa alla discrezionalità dell'avvocato titolare del trattamento la valutazione del rischio che lo specifico *data breach* possa rappresentare per i diritti e le libertà degli assistiti e degli interessati, seppur, in presenza di una valutazione affermativa circa la sussistenza del rischio, la sua discrezionalità viene meno essendo l'avvocato, entro e non oltre le 72 ore dalla presa di coscienza, vincolato a notificare al Garante della protezione dei dati personali l'avvenuta violazione[139,140].

Inoltre, la Commissione del CNF in materia di Privacy - all'interno delle summenzionate "linee guida - raccomanda all'avvocato, una volta preso coscienza del rischio e notificato la violazione al Garante di mettere in atto ulteriori misure utili ad analizzare i rischi del trattamento istituito per i diritti e le libertà delle persone fisiche.

---

[138] Nel caso in cui lo studio legale si sia avvalso di un responsabile del trattamento, quest'ultimo ha l'obbligo di notificare al titolare, senza ingiustificato ritardo dal momento in cui ne viene a conoscenza, qualsiasi violazione dei dati personali.

[139] A norma del 3 comma dell'art. 33 del GDPR, l'avvocato sarà vincolato anche nel contenuto della notifica all'autorità di controllo competente che dovrà necessariamente:
"*a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;*
b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
c) descrivere le probabili conseguenze della violazione dei dati personali;
d) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi".

[140] Il modulo per la notifica della violazione dei dati personali è a disposizione del titolare sul sito del Garante al seguente link *https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9128501*

Tra queste ritroviamo il compito di assicurarsi che le violazioni siano state notificate entro 72 ore, ed in caso contrario spiegare accuratamente le motivazioni del ritardo all'autorità garante; il compito di indicare nella notifica i fatti della violazione, la natura della violazione, i suoi effetti e le misure adottate per porvi rimedio nonché l'ulteriore sforzo di documentare il più possibile qualsiasi violazione per consentire all'autorità di vigilanza di verificare la conformità ai requisiti imposti dal GDPR.

Per ciò che riguarda invece la comunicazione al titolare del trattamento, l'art. 33 GDPR al comma 2 statuisce "*Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione*".

Laddove, dunque, il titolare valuti che sia probabile che la violazione sia suscettibile di presentare un elevato rischio per i diritti e le libertà di una persona fisica, sarà necessario comunicare anche all'interessato il *data breach*.[141]

Tuttavia, la comunicazione all'interessato può considerarsi non necessaria ove le misure tecniche e organizzative preventivamente predisposte dal titolare abbiano hanno reso i dati incomprensibili per qualsiasi persona (es. laddove i dati siano stati cifrati o crittografati), oppure, allorquando siano state adottate misure per garantire che il rischio sia scongiurato e non possa più verificarsi: in questi casi, il rischio di violazione è minimizzato al punto tale di rendere superflua l'eventuale comunicazione. [142]

Ove invece la comunicazione richieda "*sforzi sproporzionati*" ma comunque il rischio di violazione non sia stato totalmente eliminato, l'avvocato avrà la possibilità di eseguire una comunicazione "*pubblica*" sempreché la stessa possa raggiungere ed informare gli interessati con analoga efficacia della comunicazione diretta.[143]

---

[141] L'*European Data Protection Board* (ex WP29), ora EDPB, ha fissato dei parametri per la valutazione dei fattori che determinano il rischio per le libertà e i diritti degli interessati e, tra questi rientrano: il tipo di "breach", ossia il tipo di violazione (es. la violazione dei dati personali di tutti i clienti è ben diversa dalla perdita dei dati personale di un singolo cliente); la natura, numero e grado di sensibilità dei dati personali violati (es. l'accesso al nome e all'indirizzo dei genitori di un figlio rappresenta un rischio diverso rispetto all'accesso da parte dei genitori naturali del nome e dell'indirizzo dei genitori adottivi); la facilità di associare i dati violati ad una persona fisica; la gravità delle conseguenze per gli interessati; il numero di interessati esposti al rischio; le caratteristiche del titolare del trattamento.

[142] Tale comunicazione sarà difforme rispetto a quella adottata per il Garante in quanto dovrà contenere: le informazioni del nome e dei dati di contatto del DPO (ove applicabile) o di altro punto di contatto presso cui ottenere maggiori informazioni; la descrizione - con un linguaggio semplice e chiaro - della natura della violazione dei dati personali e delle probabili conseguenze, le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione e anche, se del caso, per attenuarne i possibili effetti negativi.

[143] La comunicazione gli interessati potrà in ogni caso essere richiesta dall'Autorità garante ove quest'ultima reputi, dopo aver esaminato la notificazione, che vi sia un alto rischio per gli interessati derivante dal *data breach*.

In conclusione, si rende indispensabile sottolineare che l'avvocato - quale responsabile del trattamento dei dati dei propri cliente - può essere, in caso di mancato rispetto delle disposizioni di cui al GDPR, soggetto a sanzioni amministrative significative.

Il regolamento prevede infatti che l'autorità Garante per la protezione dei dati personali possa rivolgere all'avvocato specifici avvertimenti, ammonirlo, limitare temporaneamente o permanentemente un trattamento, sospendere i flussi di dati, ordinare allo stesso di soddisfare richieste per l'esercizio dei diritti delle persone, nonché - ancora - ordinare la rettifica, limitazione o cancellazione dei dati.

È inoltre previsto che il Garante possa ritirare la certificazione di conformità concessa all'avvocato – o allo studio legale-, ovvero ordinarne il ritiro all'autorità di certificazione.

In ultimo, il GDPR contempla la possibilità di comminare una sanzione amministrativa di importo compreso tra i 10 ed i 20 milioni di euro, ovvero, in caso di grandi studi internazionali di importo compreso tra il 2% ed il 4% del fatturato mondiale.

IL TRATTAMENTO DEI DATI PERSONALI IN AMBITO SCOLASTICO

di Gaetano Guarino

SOMMARIO: 1. Introduzione; 2. Le peculiarità dell'istituzione scolastica; 3. Il trattamento dei dati personali e categorie particolari di dati; 4. I soggetti garanti della riservatezza scolastica; 5 La tutela dei dati nel rapporto scuola personale; 6 La tutela dei dati nel rapporto scuola studenti; 7 L'intervento del Consiglio d'Europa; 7 Osservazioni conclusive.

Abstract: This article will explain the applicable regulations in the field of privacy relating to education sector. It begins demonstrating the typical elements of schools as a subject of rights, with the main rules about personal data protection and special categories of personal data. In particular, it explores the relationships between schools/employeers and schools/students. In addition, it is outlined the role of the data controllers and processors and the point of view of the Council of Europe. It finishs with some closing remarks.

1. Introduzione

Si è in presenza di un'istituzione scolastica quando vi è un insieme di studenti e docenti finalizzato alla condivisione e trasmissione di conoscenze, esperienze ed abilità. A questi si aggiunge la presenza del personale dirigenziale, amministrativo, direttivo e collaborativo che gestisce le pratiche burocratiche e finanziarie nonché le ulteriori attività volte al buon andamento dell'istituzione scolastica.

2. Le peculiarità dell'istituzione scolastica

La scuola dal punto di vista giuridico è una pubblica amministrazione, quindi un soggetto di diritto pubblico.

Tra le norme che disciplinano l'istituzione scolastica possiamo annoverare anche quelle in materia di riservatezza: il Dlgs. 196/2003[144] ed il Regolamento europeo

[144] così come modificato dal Dlgs. 101/2018.

769/2016/UE[145], a cui vanno aggiunti il contributo del Garante italiano per la protezione dei dati personali con apposite misure di garanzia[146] ed un vademecum. Concludono il quadro le linee guida del Consiglio d'Europa.

Preme evidenziare che la scuola ha come destinatari dei suoi atti e fatti giuridici sia soggetti minorenni (gli studenti), che maggiorenni (genitori, docenti, personale amministrativo ed ausiliario), nonché persone giuridiche spesso incaricate di eseguire opere o prestare servizi connessi allo svolgimento delle attività scolastiche (si pensi alle opere di tinteggiatura dell'edificio).

Al contempo vi sono due elementi di segno opposto, da un lato la presenza sia di dati personali sia di dati sensibili che vengono gestiti nel rispetto di tutte le garanzie, per limitarne la conoscenza indiscriminata e consentirne solo un uso conforme alle norme di legge; dall'altro vi sono obblighi di trasparenza e pubblicità legale che ogni scuola, in quanto pubblica amministrazione, è tenuta a porre in essere tramite pubblicazione nelle apposite bacheche negli spazi scolastici, ovvero sul sito istituzionale, nonché sul registro elettronico.

Quindi grande è la preoccupazione che per errore i dati personali vengano divulgati poiché ogni giorno nella scuola confluiscono e vengono gestiti un significante numero di dati. Si pensi al flusso di informazioni che arrivano via posta elettronica, o a quelli riguardanti la presenza di studenti e professori. A queste si sommano situazioni particolari come la redazione delle graduatorie di istituto e le comunicazioni con soggetti istituzionali come il Comune.

3. Il trattamento dei dati personali e di categorie particolari di dati.

Le due nozioni fondamentali per poter cominciare ad analizzare questo fenomeno sono quelle riguardanti i dati personali e le categorie particolari di dati, detti anche dati sensibili.

Il Reg. 769/2016/UE definisce all'art.4 i dati personali come: *"qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»)";* precisando altresì che si considera identificabile: *"la persona fisica che può essere*

[145] Di seguito denominato Reg.
[146] In particolare il provvedimento del Garante: "*che individua le prescrizione contenute nelle Autorizzazioni generali n.1/2016,3/2016,6/2016,8/2016 e 9/2016 che risultano compatibili con il Regolamento e con il D.lgs n. 101/08 di adeguamento del codice*" – 13 dicembre 2018 [9068972]

identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale";

In altre parole, si tratta di un dato che può assumere differenti denominazioni e derivare da diversi ambiti settoriali e che consente un collegamento univoco tra una persona ed una sua personale caratteristica, ad esempio la residenza.

Lo stesso testo normativo identifica[147] come categorie particolari di dati quei dati personali che: *"Rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale; i dati genetici, quelli biometrici intesi a identificare in modo univoco una persona fisica, infine quelli relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona".*

Si tratta di dati che dimostrano caratteristiche specifiche e strettamente personali della persona, non visibili dall'esterno e non pubblici normalmente. Tuttavia, essi sono in grado di rendere distinguibile una persona dalla massa indeterminata di altri soggetti.

Sono informazioni per cui spesso vi sono stati episodi discriminatori o violenti.

Per evitare sul nascere questo tipo di situazioni, è espressamente vietato trattare questi dati[148], in linea con il divieto di discriminazioni espresso sia dalle convezioni europee a tutela dei diritti fondamentali[149], sia dalla costituzione italiana all'art.3 ovvero con il principio di uguaglianza[150].

Il Reg. prevede una serie di eccezioni al divieto di trattamento dei dati sensibili[151]: quando l'interessato ha prestato il consenso al trattamento; quando il trattamento è necessario per obblighi in materia di diritto del lavoro, sicurezza sociale, protezione sociale o per tutelare un interesse vitale dell'interessato o di un'altra persona fisica e l'interessato è incapace di prestare il proprio consenso; per finalità riguardanti l'appartenenza ad un'associazione; si tratta di dati resi pubblici dall' interessato; sono dati trattati dall'autorità giudiziarie durante lo svolgimento di indagini; in materia di

[147] Ex art.9 Reg.
[148] Ex. Art. 9 com.1 Ibidem.
[149]Ex. Art. 21 carta dei diritti fondamentali dell'Unione Europea, ex. Art. 14 della convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali ed ex art. 1 protocollo n.12 della stessa convenzione.
[150] Ex. Art. 20 carta dei diritti fondamentali dell'Unione Europea.
[151] Ex. Art.9 com. 2 Reg.

medicina preventiva o del lavoro; per motivi di interesse pubblico nella sanità pubblica; infine, per finalità statistica o storica.

Quindi come conseguenza è possibile dedurre che in via di principio, salvo le sopra citate eccezioni, i dati sensibili di tutti i soggetti che entrano in contatto con la scuola non devono essere trattati ma possono essere trattati solo i dati personali.

Il codice privacy ha stabilito un peculiare elemento distintivo tra queste due tipologie di dati, quando ha introdotto le nozioni di comunicazione e diffusione[152].

La prima è definita come: *"Il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dell'Unione Europea, dal responsabile o dal suo rappresentante nel territorio dell'Unione Europea, dalle persone autorizzate**[153]**, al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione".*

La seconda come: ***"****Il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione".*

In altre parole, la comunicazione è la trasmissione a soggetti diversi dall'interessato e a lui non collegati dei suoi dati; la diffusione è trasmissione generica dei dati a soggetti non determinati e con qualunque mezzo e forma.

Ebbene il codice ha stabilito che la comunicazione dei dati personali è ammessa, tra soggetti titolari del trattamento dei dati che effettuato trattamenti **per l'esecuzione di un compito di interesse pubblico, o connesso all'esercizio di pubblici poteri,** solo se è prevista da una norma di legge, in qualità di base giuridica[154].

In mancanza di tale norma, la comunicazione è ammessa solo se è obbligatoria per l'esecuzione di compiti di pubblico interesse e di funzioni istituzionali, decorsi 45 giorni da un'apposita comunicazione al Garante, senza che questi si sia pronunciato sulle misure di garanzia da adottarsi[155]**.**

[152] Ex. Art. 2 ter com.4 ibidem. Questa distinzione si basa sull'art. 6 com. 2 del Reg.
[153]Ex art. 2-quaterdecies ibidem.
[154] Ex. Art. 2 ter. com. 2 ibidem.
[155] Ex. Art. 2 ter. com. 2 ibidem.

Inoltre, sempre e solo in presenza di una base giuridica è possibile diffondere e comunicare dati, a soggetti che sebbene operino nello svolgimento dei medesimi compiti e la loro azione sia connessa a quei medesimi poteri pubblici già citati intendono trattarli per altre finalità[156].

Per quanto riguarda i dati sensibili la normativa è più dettagliata e stringente.

Essa prevede che il trattamento di tali dati, essendo necessario per motivi di interesse pubblico rilevante, è ammesso se previsto da una norma di legge, anche regolamentare, che indichi il tipo di dati oggetto del trattamento, le operazioni possibili e il motivo di interesse pubblico rilevante, nonché le misure volte a garantire l'interessato[157].

Il codice stabilisce[158] che va considerato rilevante l'interesse pubblico dei trattamenti effettuati da soggetti che svolgono compiti di interesse pubblico, o connessi all'esercizio di poteri pubblici, in differenti materie, tra cui quella di istruzione e formazione in ambito scolastico.

Allo stesso tempo l'art. 2 *septies* del codice stabilisce che il trattamento di alcune categorie particolari di dati, quelli genetici, biometrici e relativi alla salute, deve avvenire nel rispetto di apposite misure di garanzie del garante, ma pone l'espresso divieto di diffusione di questa tipologia di dati.

A questo punto bisogna chiarire la definizione di trattamento dei dati personali, secondo il Reg.[159]: *"Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione".*

In altri termini, si considera trattamento qualsiasi operazione che abbia ad oggetto dati personali e la loro gestione, tra cui spiccano la consultazione, la registrazione e la comunicazione.

[156] Ex. Art. 2 ter. com. 3 ibidem.
[157] Ex. Art. 2 sexies com.1 ibidem.
[158] Ex. Art. 2 sexies com. 2 ibidem.
[159] Ex. Art.4 Reg.

Quindi secondo la normativa, in ambito scolastico un trattamento può essere effettuato solo in presenza di una base giuridica[160] quale ad esempio la creazione del fascicolo personale dell'allievo, che prevede il trattamento dei suoi dati. Tale trattamento è possibile perché previsto dalla Circolare Ministeriale 16 novembre 1992, n. 339 annessa al D.M. del 16.11.1992, in attuazione di una norma di legge[161].

Da un'ulteriore analisi del Regolamento, si osserva che la necessarietà di una norma legislativa, come base giuridica del trattamento, soddisfa anche il principio di liceità del trattamento[162], secondo il quale il trattamento può essere effettuato solo in modo lecito e tra i casi di liceità vi identifica anche quello in cui il trattamento sia *ex lege*[163].

Vi sono altri principi che guidano la gestione dei dati[164]. Quelli di correttezza e trasparenza, il principio di limitazione che stabilisce che i dati devono essere raccolti per finalità determinate, esplicite e legittime e trattati con una modalità che non sia incompatibile con tali finalità. Poi il principio di minimizzazione secondo il quale i dati devono essere adeguati, pertinenti e limitati a quanto necessario rispetto ai fini per i quali sono trattati.

In aggiunta a questi, vi è il principio di esattezza per cui i dati devono essere esatti ed aggiornati, nonché cancellati o rettificati. Inoltre, il principio di limitazione della conservazione precisa che i dati devono essere conservati in modo che venga consentita l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità.

Bisogna poi garantire un'adeguata sicurezza e protezione dei dati ai sensi del principio di integrità e riservatezza. Infine, vi è il principio di responsabilizzazione, detto anche *accountability*, secondo il quale il titolare del trattamento è il responsabile del rispetto dei principi del Reg. ed è colui che deve attivarsi per garantirne l'efficacia e su cui grava il relativo onere della prova in caso di contestazioni. Una conseguenza della necessarietà della base giuridica in ambito scolastico è l'assenza della richiesta del consenso all'interessato. Questo perché l'art.6 del Reg. valuta lecito un trattamento

[160] Ex. Art. 2 ter, Dlgs. 196/2003.
[161] Ex Art. 2 della legge 5 giugno 1990, n. 148.
[162] Ex art.5 com.1. let.a) Reg.
[163]Ex Art. 6 com.1 let.c) Reg.:"Il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento".
[164] Indicati dall'art.5 del Reg.

se basato sul consenso, o su una norma di legge, considerando le due ipotesi alternative tra loro.

Tuttavia, l'assenza del consenso non determina il venir meno degli obblighi informativi[165] che il titolare del trattamento deve comunicare al momento della prima comunicazione utile. Si tratta di quell'insieme di elementi contenuti nella c.d. informativa *privacy*[166] che spesso viene fornita all'atto di compilare moduli, o formulari e ne viene richiesta la firma.

In ambito scolastico tale comunicazione può concretizzarsi all'atto di iscrizione di un allievo, ovvero all'atto di presentazione di una domanda formale, in modo cartaceo, o digitale.

Nello specifico devono essere comunicate le seguenti informazioni[167]: l'identità ed i contatti del titolare del trattamento e/o del suo rappresentante; nonché quelli del responsabile del trattamento dei dati personali; la finalità del trattamento; la base giuridica ed i relativi destinatari; la volontà o meno di trasferire i dati e la durata della loro conservazione[168].

Allo stesso tempo devono essere indicati i diritti dell'interessato: l'accesso ai dati personali; la loro rettifica; cancellazione; limitazione; opposizione e portabilità; il diritto di reclamo.

Infine, dovrà essere comunicato se sarà svolto su quei dati un processo automatizzato, come la profilazione, la sua logica e le sue conseguenze, nonché la fonte dei dati e la sua eventuale accessibilità al pubblico.

4. I soggetti garanti della riservatezza scolastica

Insieme agli obblighi informativi vi sono altri compiti che l'istituzione scolastica deve attuare preventivamente: gli obblighi di sicurezza.

Essi gravano su due specifici soggetti denominati titolari del trattamento e responsabile del trattamento. Il primo viene definito come: *"La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali"*[169]. Il secondo

[165] Ex art. 12 ibidem.
[166] Il Reg. precisa che quest'informativa va scritta in forma concisa, trasparente, intellegibile e facilmente accessibile, con un linguaggio semplice e chiaro Ex art.12 ibidem.
[167] Ex art. 14 ibidem.
[168] o i criteri per determinarla
[169] Ex. Art. 4 n. 7 Reg.

è identificato nella: *"Persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento"*[170].

In ambito scolastico il titolare del trattamento è proprio la scuola, perché ogni volta che uno studente, un dipendente della scuola, o un soggetto terzo, si relaziona con l'ente scolastico è con quest'ultimo che si istituisce un rapporto giuridicamente rilevante, sebbene sia mediato dal personale scolastico.

Si verte in una delle ipotesi di rappresentanza organica in cui il personale agisce in nome e per conto della PA, ma è proprio l'ente, in quanto persona giuridica, titolare di diritti e doveri nei confronti dei soggetti con cui crea rapporti giuridici. Al contempo la responsabilità giuridica è allocata nei confronti dei soggetti che di volta in volta svolgono i singoli atti e che firmano proprio in qualità di responsabile del provvedimento il singolo provvedimento. A riprova di quest'interpretazione si osservi che la norma europea cita proprio l'ipotesi di "autorità pubblica" e in questo caso codesta l'autorità è la scuola.

A chiusura di questa ricostruzione interpretativa si può individuare il soggetto che agisce in nome e per conto della scuola, avendone la rappresentanza: il dirigente scolastico[171]. Egli è la persona fisica tenuta a adempiere agli obblighi di garanzia che il Reg. impone al titolare del trattamento.

Il secondo, il responsabile del trattamento, è colui che effettua il trattamento di volta in volta, così come il responsabile del provvedimento, con l'unica differenza che il primo, nella sua azione giuridicamente rilevante, si occupa di dati personali. Nel contesto della scuola, questi può essere un soggetto del personale amministrativo addetto alle pratiche amministrative concernenti le persone fisiche, come ad esempio la gestione delle risorse umane.

Ebbene il Reg. pone obblighi specifichi in capo al titolare e al responsabile.

Riguardo il titolare egli deve realizzare tutte le misure tecniche ed organizzative al fine di garantire e dimostrare il rispetto delle relative norme in tema di riservatezza[172]. La norma precisa che codeste operazioni, tra le quali vi rientrano l'adozione di politiche adeguate, devono essere aggiornate e riesaminate nel corso del tempo[173].

[170] Ex art. 4 n.8 ibidem.:
[171] o un suo delegato.
[172] Ex art. 24 e 25 Reg.
[173] Ex. Art. 24 ibidem.

Detto diversamente è previsto l'obbligo del titolare di attivarsi in maniera costante e continuativa per far sì che la sua attività, nel caso di specie un'istituzione scolastica, agisca nel rispetto della normativa di settore.

Tale onere è temperato da due elementi. Da un lato il fatto che queste misure sono da valutarsi in base alla natura, all'ambito d'applicazione, al contesto alla finalità ed ai rischi connessi. Dall'altro dall'applicazione di codici di condotta e meccanismi di certificazione[174].

Dal punto di vista tecnico, il titolare è tenuto a prendere tutte le misure tecniche ed organizzative per proteggere i dati e garantire gli interessati (tra cui la pseudominizzazione) sia quando stabilisce i mezzi del trattamento, sia al momento del trattamento stesso[175]. In particolare, esse devono essere preventivamente impostate di modo che si riferiscano ai soli dati necessari per svolgere il trattamento e garantire che gli stessi non siano accessibili ad un numero indefinito di persone, senza l'ausilio di una persona fisica.

Andando in dettaglio si evidenzia che siamo dinanzi ad un obbligo di carattere tecnico e particolarmente incisivo sulle modalità d'azione del titolare, che si spinge sino alla limitazione dell'accesso ai dati e quindi alla loro custodia. Infatti, tramite un meccanismo impostato a priori vanno gestite solo le informazioni necessarie al trattamento ed escluse quelle superflue, nonché devono essere rese non identificabili e celate all'altrui visualizzazione[176]. Si tratta di un'applicazione del principio di minimizzazione[177].

Calando queste norme nell'ambito educativo, che qui si analizza, si può dedurre che il dirigente scolastico deve adoperarsi per garantire i mezzi adeguati ad un trattamento dei dati rispettoso della riservatezza e dotato delle caratteristiche tecniche sopra citate. Nel dettaglio ciò si concretizza nella fornitura di software e programmi informatici adeguati nei computer utilizzati dal personale, per soddisfare proprio quelle caratteristiche tecniche sopra citate.

Per quanto riguarda il responsabile del trattamento, principalmente egli deve dimostrare di possedere garanzie idonee ad attuare le misure tecniche ed organizzative

[174] Ex. Art. 24 ibidem.
[175] Per approfondire: E. ERRICCHIELLO, *Privacy by design e privacy by default: origini, prospettive e criticità, in Data Protection Law n. 1/2018.*
[176] G. GUARINO, *Gli obblighi privacy nei contratti online, in Data Protection Law n. 2/2020.*
[177] Tale norma deve essere interpretata alla luce del contesto, dei rischi, dello stato dell'arte, della natura e delle finalità del trattamento e dalla presenza o meno di meccanismi di certificazioni di tali misure.

predisposte[178]. Egli non può ricorrere ad un altro responsabile senza previa autorizzazione scritta del titolare[179], fatto salvo il suo diritto di opporsi. Infatti, alla base di ogni trattamento vi deve essere sempre un atto[180] con il quale il titolare autorizza e disciplina il trattamento da parte del responsabile. Il testo normativo parla di un contratto o altro atto simile, che indichi le caratteristiche specifiche del trattamento: durata, natura, finalità, tipologia dati, categorie di interessati, obblighi e diritti titolare. Oltre a ciò, lo stesso deve prevedere che sul soggetto autorizzato al trattamento vi sia un obbligo di riservatezza, in via negoziale, o legale[181].

Non deve essere sottovalutato tale atto perché è' espressamente stabilito dall'art. 29 del Reg. che il responsabile del trattamento, o chiunque agisca per suo conto, ovvero sotto la sua autorità, non li può trattare se non ha ricevuto autorizzazione dal titolare[182]. Detto altrimenti non vi può essere alcun trattamento senza autorizzazione.

In ambito scolastico questa questione può essere leggermente ridimensionata, perché è sempre una norma di legge che individua quegli atti e fatti che incidono sui dati personali generando un trattamento e chi, a livello generale ed astratto, all'interno della scuola deve realizzarli. Al livello concreto saranno il mansionario e/o lo stato di servizio ad individuare chi è addetto a quella specifica pratica burocratica e di conseguenza responsabile del trattamento dei dati ivi raccolti. Pertanto, nel momento in cui il dirigente indirizzerà un soggetto del suo personale verso determinate mansioni dovrà valutare la sua idoneità al rispetto delle norme in materia di riservatezza.

Infine, sul responsabile gravano anche alcuni obblighi tecnici[183]. Questi a seconda della richiesta del titolare, deve cancellare, o restituire i dati dopo il trattamento, comprese eventuali copie, salvo l'obbligo conservazione. Inoltre, è tenuto a mettere a disposizione tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di legge, contribuendo ad attività di revisione e ispezione ed è tenuto ad informare il titolare se un'istruzione viola regolamento.

---

[178] Ex. Art. 28 com. 1 Reg., l'adesione ad un codice di condotta o il possesso di una certificazione sono prova sufficiente.
[179] Ex. Art. 28 com 2 ibidem.
[180] Il responsabile tratta dati solo previa istruzione documentata del titolare, salvo la presenza di un obbligo giuridico di cui informa titolare, ovvero che non vi sia un divieto di effettuare tale informazione ex. Art. 28 Reg. com.3 let. a.
[181] Questo vale anche nel caso in cui il responsabile voglia farsi assistere da un altro responsabile. In caso di omissione del secondo responsabile il primo ne risponde ex. Art. 28 com. 4 Reg.
[182] salvo che lo richieda la legislazione di uno stato membro o dell'diritto dell'Unione Europea.
[183] G. GUARINO, *Gli obblighi privacy nei contratti online, in Data Protection Law n. 2/2020.*

Su titolare e responsabile l'art. 32 del Reg. pone l'obbligo di realizzare tutte le misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio c.d. misure di sicurezza. Queste devono concretizzarsi alla luce di diversi criteri: lo stato dell'arte, i costi, la natura, l'oggetto, il contesto e le finalità del trattamento, come anche le probabilità di rischio per i diritti e le libertà delle persone[184].

In altre parole, il titolare ed il responsabile hanno il dovere di realizzare tutte le misure tecniche per salvaguardare i diritti e le libertà delle persone di cui gestiscono i dati[185]. Tali meccanismi devono adattarsi in base a diversi elementi tra i quali spicca il contesto in cui si concretizza il trattamento, in questo caso quello scolastico.

Si noti che consapevole delle difficoltà applicative la normativa europea non ha imposto un obbligo fisso, ma flessibile, in base a specifici fattori, che orienteranno l'interprete nella valutazione del requisito di adeguatezza[186].

In aggiunta a questa delimitazione delle responsabilità e dei compiti la stessa disposizione normativa pone delle specifiche di carattere tecnico. Infatti, essa prevede l'obbligo di pseudominizzazione e cifratura dei dati, di misure per garantire la riservatezza, l'integrità, la disponibilità e la resilienza di sistemi e servizi. Poi deve essere garantita la possibilità di ripristino e di accesso in caso di incidente, nonché una procedura per verificare l'efficacia delle misure, considerando i rischi per la perdita, la distruzione, la modifica, e la divulgazione delle informazioni[187].

Un ulteriore onere che grava su titolare e responsabile, in modo diverso, è quella della tenuta dei due registri di trattamento dei dati, denominati registri delle attività di trattamento[188].

Il primo ha ad oggetto le attività di trattamento svolte sotto la responsabilità del titolare del trattamento e dal suo rappresentante. Esso deve contenere gli estremi del titolare, del responsabile e di eventuali rappresentanti o contitolari, la finalità, le categorie dei soggetti interessati, dei dati e dei destinatari, l'indicazione del loro eventuale trasferimento, il termine per ottenerne la cancellazione e le relative misure di sicurezza[189].

---

184 G. GUARINO, *Gli obblighi privacy nei contratti online,ibidem.*
185 G. GUARINO, *Gli obblighi privacy nei contratti online,ibidem.*
186 G. GUARINO, *Gli obblighi privacy nei contratti online,ibidem.*
187 In questo contesto secondo il Reg. l'adesione del titolare a codici di condotta, o a meccanismi di certificazione degli obblighi di riservatezza e delle misure di sicurezza, è prova del corretto adempimento di queste norme di sicurezza.
188 Ex art.30 Reg. ibidem.
189 G. GUARINO, *Gli obblighi privacy nei contratti online,ibidem.*

Il secondo comprende tutte le categorie di attività relative al trattamento svolte per conto di un titolare del trattamento. Esso contiene le qualifiche, i dati anagrafici ed i contatti dei diversi soggetti coinvolti nella cura dei dati personali: il titolare, il responsabile (o i responsabili) del trattamento che agisce per suo conto, nonché dei lori eventuali rappresentanti ed infine il responsabile della protezione dei dati. Inoltre, al suo interno devono essere raccolte le categorie dei trattamenti svolti, i trasferimenti effettuati e le relative misure di sicurezza adottate.[190]

Tali registri sono tenuti in forma scritta anche elettronica e devono essere tenuti a diposizione dell'autorità di controllo[191].

La distinzione tra i due registri si nota nel fatto che mentre il primo registro è tenuto alla conservazione delle attività di trattamento effettuate nel tempo, il secondo riguarda tutte quelle diverse attività che denotano un utilizzo dei dati successivo alla loro fornitura. Quindi in un insieme si conservano i dati acquisiti, nell'altro si tiene traccia di quelle attività, che si sono svolte con quei dati successivamente[192].

Infatti, il regolamento distingue le operazioni riferendosi espressamente ad attività di trattamento e a tutte le categorie di attività di trattamento. Ne deriva che mentre il primo ricorda un elenco cronologico dei trattamenti, il secondo appare di tipo più tecnico, finalizzato a poter garantire un controllo esterno per conoscere quali sono le operazioni svolte con quei dati e per quale scopo. Ulteriore differenza è che mentre il primo registro è custodito dal titolare il secondo è tenuto dal responsabile[193].

Ne emerge che il contenuto di entrambi queste raccolte sarà abbastanza articolato e complesso. Esso registrerà ogni preciso trattamento svolto nel tempo, da parte di chi, riguardante quali informazioni, sotto la responsabilità di chi, a nome di chi, per quale motivazione e poi dovrà essere ordinato in una precisa categoria nel secondo registro[194].

La tenuta di questi registri nel contesto scolastico è obbligatoria, perché gli istituti trattano anche categorie particolare di dati c.d. dati sensibili. Sulla loro compila-

190 G. GUARINO, *Gli obblighi privacy nei contratti online,ibidem.*
191 G. GUARINO, *Gli obblighi privacy nei contratti online,ibidem.*
192 G. GUARINO, *Gli obblighi privacy nei contratti online,ibidem.*
193 G. GUARINO, *Gli obblighi privacy nei contratti online,ibidem.*
194 G. GUARINO, *Gli obblighi privacy nei contratti online,ibidem.*

zione è intervenuto il ministero dell'istruzione con nota n. 877 del 03/08/2018, inviando alle scuole un modello di registro, un esempio di compilazione ed una guida per la sua compilazione.

Quest'ultima illustra una metodologia per individuare i trattamenti suddivisa in tre passaggi: descrizione del processo con i suoi elementi e soggetti coinvolti, analisi delle caratteristiche dei dati e indicazione delle attività di trattamento da svolgersi in base ai dati raccolti. Vengono così individuati tre macro-processi: l'iscrizione degli alunni, suddivisa nel trattamento di iscrizione ed in quello di acquisizione di documenti aggiunti, quello della gestione della carriera scolastica in cui si individuano due trattamenti quello di gestione dei dati dell'allievo e del suo inserimento nell'anagrafe nazionale degli studenti[195], infine quello della gestione del personale.

Codesto documento specifica che se l'istituto utilizza il portale SIDI il responsabile esterno del trattamento è il ministero, se invece è in uso un software prodotto da un altro fornitore sarà quest'ultimo il responsabile, nell'ipotesi in cui il procedimento sia cartaceo titolare è la scuola e non è presente il responsabile.

Nell'ultimo caso di processo la guida individua tre ipotesi: la gestione dei contratti a tempo indeterminato, quella di quelli a tempo determinati e quella relative alle supplenze brevi e saltuarie. Nei primi due casi vi è una contitolarità del trattamento del Miur e dell'istituzione scolastica, nel terzo titolare è la scuola, mentre responsabile è il ministero.

Riguardo il modello di registro, lo stesso si concretizza su 3 fogli di lavoro Excel. Due contengono i dati del titolare e del responsabile, il terzo contiene la suddivisione in colonne tutti gli elementi di un trattamento: attività di trattamento, descrizione dell'attività di trattamento, modalità di trattamento, finalità etc.

Tuttavia, emergono alcune criticità. La prima è la presenza di un solo registro, in contrasto con l'art.30 del Reg., espressamente denominato registri delle attività di trattamento. Da un'attenta osservazione sembra che il ministero predisponendo la sezione categoria dei dati, abbia inteso fondere i due registri in uno solo, offrendo uno spazio in tabella per quello che dovrebbe essere un registro autonomo.

In aggiunta manca la previsione dell'indicazione degli estremi cronologici del trattamento. Vi è il rischio di generare confusione nell'operatore, perché non essendo

[195] al fine di adempiere agli obblighi previsti dal D.M. 692/2017.

previsto l'indicazione degli estremi cronologici, né di suddividerli per categoria i trattamenti dovrebbero essere indicati uno sotto l'altro senza un ordine prestabilito. Poi si utilizza l'etichetta dati comuni invece di dati personali. Sarebbe stato sufficiente prevedere un foglio di lavoro Excel a parte per il registro delle categorie dei dati per permettere un maggior ordine ed un utilizzo più agevole ed intuitivo. Ciò anche alla luce del fatto che sono migliaia i dati personali trattati in una scuola e che di conseguenza queste colonne sono ricolme di informazioni.

Ulteriore obbligo di carattere preventivo vigente in capo al titolare è quello di nomina del responsabile per la protezione dei dati personali. Infatti, l'art. 37 del reg. stabilisce i casi tassativi in cui deve essere effettuata questa nomina, tra cui vi rientrano le pubbliche amministrazioni. Ne consegue che la scuola in quanto appartenente a questa tipologia di persona giuridica è tenuta a soddisfare quest'adempimento.

L'attività di vigilanza del RPD verte su queste attività: quella informativa, quella relativa alla custodia dei registri e quella riguardante gli obblighi di sicurezza[196].

Alla luce dell'insieme di norme che gravano sulle istituzioni scolastiche in tema di riservatezza, il RPD è espressamente tenuto a sensibilizzare tutti soggetti che vi lavorano, in particolare coloro che effettuano i trattamenti dei dati e sono tenuti alla loro custodia[197].

Oltre a ciò, egli è il punto di contatto tra l'ente e l'autorità di vigilanza per la protezione dei dati personali, alla quale la sua nomina deve essere comunicata[198]. Infine, egli è tenuto a fornire un parere in merito alla valutazione di impatto, si tratta di un piano riguardante l'adozione nell'ente di nuove tecnologie[199] che possono mettere a rischio i dati personali.

In sostanza l'RPD ha il compito di far porre in essere tutte le misure previste dal Reg. che altrimenti rischierebbero di rimanere lettera morta. Tant'è vero che egli deve essere adeguatamente coinvolto in tutte le questioni in tema di riservatezza[200].

Nei suoi confronti il titolare ed il responsabile del trattamento devono garantire il suo regolare operato[201]. Pertanto, il Reg. prevede che gli stessi sono tenuti a fornire al RPD le risorse necessarie per assolvere tali compiti e a garantire l'accesso ai dati e

[196] G. GUARINO, *La mancata nomina del responsabile della protezione dei dati per i soggetti privati, in Data Protection Law n. 1/2021*
[197] Ex. Art. 39 par. 1 Lett. (a. Reg.
[198]Ex. Art. 37 par. 8 ibidem.
[199] Ex. Art 35 ibidem.
[200] Ex. Art. 38 com. 1 ibidem.
[201] Ex. Art. 38 ibidem.

ai trattamenti per mantenere la sua conoscenza specialistica. Inoltre, non devono ostacolarlo, né fornirgli istruzioni riguardo l'esecuzione dei suoi compiti, né sanzionarlo in alcun modo per l'adempimento dei suoi doveri.

D'altro canto, l'RPD è tenuto a riferire solo ai vertici del titolare dell'ente, o del responsabile del trattamento e a serbare il segreto e/o la riservatezza sul suo operato[202].

La sua posizione di terzietà è salvaguardata anche dal fatto che nel caso in cui egli svolga anche altri compiti nell'ente, il titolare e il responsabile devono garantire che non vi siano conflitti di interesse[203].

5. La tutela dei dati nel rapporto scuola personale

Il Garante ha emanato uno specifico provvedimento relativo al trattamento dei dati sensibili nei rapporti di lavoro sia pubblici che privati[204], effettuati dai soggetti c.d. responsabili delle risorse umane[205], nello svolgimento delle relative pratiche burocratiche (ad es.: la gestione di graduatorie e convocazioni).

Nella fase preliminare delle assunzioni, il Garante ha specificato che si possono trattare i dati idonei a rivelare lo stato di salute e l'origine razziale ed etnica dei candidati, solo se la loro raccolta sia giustificata da scopi determinati e legittimi e sia necessaria per instaurare tale rapporto. Quest'operazione deve specificamente riguardare, nei limiti del divieto di indagini su opinioni personali e trattamenti discriminatori[206], le sole informazioni strettamente pertinenti e limitate a quanto necessario alle finalità per cui sono trattati, anche considerando le particolari mansioni e/o le specificità dei profili professionali richiesti[207]. Si tratta nient'altro che di un'applicazione dei principi di liceità e necessarietà.

In aggiunta se sono presenti dati non pertinenti rispetto all'assunzione, i datori di lavoro devono astenersi dal trattarli, così come i dati genetici, anche per la valutazione dell'idoneità professionale[208].

---

[202] Ex. Art. 38 com. 5 ibidem.
[203] Ex. Art. 38 com. 6 ibidem.
[204]Ex art.1 com.1 allegato 1 Prescrizioni relative al trattamento di categorie particolari di dati nei rapporti di lavoro (aut. gen. n. 1/2016): *provvedimento che individua le prescrizioni contenute nella autorizzazione generali […] che risultano compatibili con il regolamento […] del 13 dicembre 2018 [9068972]*.
[205] Ex art.1 com.1.1. ibidem.
[206]Ex art. 8 legge 20 maggio 1970, n.300 ed ex art. 10 Dlgs. 10 settembre 2003, n. 276.
[207]Ex. 1.4 1 *provvedimento del garante*, op. cit.
[208] Ex. 1.4 1 let c) e d). ed Ex. 1.4.2 ibidem.

Il Garante ha anche previsto altre ipotesi di trattamento dei dati sensibili. Quei dati che rivelano le convinzioni religiose o filosofiche ovvero l'adesione ad associazioni od organizzazioni a carattere religioso o filosofico, possono essere gestiti solo in caso di fruizione di permessi, per l'erogazione di servizi mensa, o nei casi di obiezione di coscienza. Inoltre, se l'interessato è un rappresentante di lista non è possibile effettuare un trattamento dati che riveli le sue opinioni politiche.

Infine, secondo l'autorità di vigilanza la raccolta di questi dati deve avvenire presso l'interessato ed essere oggetto di comunicazioni in forma elettroniche individuali, o in forma cartacea in plico chiuso, fatta salva la prova della ricezione dell'atto[209].

6. La tutela dei dati nel rapporto scuola studenti

Per quanto concerne il trattamento dei dati degli studenti punto di partenza di quest'analisi è l'art. 2 co. 2 del DPR 249/98 che dichiara: *"La comunità scolastica […] tutela il diritto dello studente alla riservatezza".* Ne consegue che l'istituzione scolastica tutta è tenuta nella sua azione a tutelare i dati personali dei suoi allievi e a prevenire lesioni di questo diritto.

Data la delicatezza della materia il garante è intervenuto pubblicando un apposito vademecum nel 2016[210], chiamato la scuola a prova di privacy, chiarendo alcune questioni al riguardo.

Da uno sguardo d'insieme del documento è possibile dedurre che si tratta di uno strumento che aiuta a diffondere le norme sopra citate delineando alcune ipotesi del contesto scolastico, con un linguaggio semplice e chiaro.

Si riporta alcune delle ipotesi più salienti.

Ad esempio, si ribadisce che il limite al trattamento in base alla finalità *ex lege* determina il venir meno del consenso, ma non dell'informativa; ovvero si specifica che è possibile trattare dati riguardanti le convinzioni religiose degli studenti, ma solo per tutelarne la libertà religiosa e finalizzata a garantire, o a esentare dall'insegnamento della religione cattolica. Così come è possibile trattare i dati relativi allo stato di salute degli allievi con disabilità, o disturbi dell'apprendimento, per predisporre interventi di sostegno.

[209] Ex. Art.1. 5 ibidem.
[210] Reperibile sul sito del garante: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/5602002

Al contempo si chiarisce che è possibile richiedere i dati personali al momento dell'iscrizione, ma non quelli eccedenti a soddisfare quest' obbligo di legge, come ad esempio le informazioni riguardo l'attività lavorativa dei genitori.

Riguardo i temi in classe è possibile assegnarne alcuni riguardanti il contesto personale o familiare dell'allievo, ma la loro eventuale lettura in classe deve basarsi su un equilibrio tra le esigenze didattiche e la tutela della riservatezza, fatta salvi gli obblighi di conservazione ed il segreto professionale.

Nello stesso documento si specifica che i voti degli scrutini e dell'esame di stato sono pubblici perché soggetti ad uno specifico regime di conoscibilità, ma non è possibile comunicare in via diretta in quest'occasione dati relativi allo stato di salute degli alunni disabili o con dsa.

Anche le altre comunicazioni scolastiche non devono contenere dettagli che possono identificare o rendere identificabile uno studente.

Inoltre, previa informativa e consenso degli studenti è possibile trattare i dati degli stessi di modo da essere comunicate ad aziende ed enti per l'inserimento professionale o lavorativo[211].

Per quanto concerne il servizio mensa possono essere trattati dati sensibili degli studenti per soddisfare specifiche richieste dei genitori. Tuttavia, viene precisato che i bollettini di pagamento devono essere inviati in busta chiusa ai genitori, eventuali buoni pasto devono avere colori uguali ed eventuali comunicazioni riguardo a ritardi di pagamento online devono avere carattere generico e non contenere i nominativi di singoli studenti, o dei loro genitori per evitare l'identificazione degli allievi appartenenti a famiglie economicamente più svantaggiate.

Nelle graduatorie di istituto è possibile pubblicare i nominativi dei soggetti coinvolti, ma non gli indirizzi ed i numeri di telefono al fine di prevenire stalking e furto di identità.

Infine, si precisa che la comunicazione di dati e fatti senza consenso ed informativa, tramite smartphone o altri apparecchi digitali, anche da parte degli studenti, se genera comunicazioni a catena di dati integra una violazione della normativa sulla riservatezza e nei casi più gravi fattispecie di reato.

[211] Ex. Art. 96 Dlgs. 96/2003

7. L'intervento del Consiglio d'Europa

In materia vi è da registrare anche l'intervento del Consiglio D'Europa con l'emanazione di apposite linee guida riguardanti la protezione dei dati dei minori in ambiente educativo. Questo documento si inserisce nella scia della convenzione n. 108 detta anche Convenzione di Strasburgo del 1981, che aveva il dichiarato scopo di tutelare i diritti delle persone fisiche, in particolare la loro vita privata e familiare[212] in relazione all'elaborazione automatica dei loro dati personali. Infatti, prevedeva che il trattamento doveva avvenire in modo leale e legale, rispettando principi di garanzia, che sono congruenti con quelli sopra citati del GDPR.

Queste linee guida cercano di tutelare in maniera ancora più forte e stringente il minore ed i suoi dati personali dalle nuove tecnologie. Lo scopo perseguito dal Consiglio, tramite le linee guida, è quello, espresso, di **supportare le organizzazioni e gli individui, educando al rispetto, alla protezione ed alla realizzazione dei diritti di protezione dei minori** all'interno dell'ambiente digitale[213].

Si ribadiscono anche in questa sede i principi GDPR e i diritti da esso derivanti con l'aggiunta dei principi del miglior interesse per il minore[214] da cui deriva il bilanciamento tra il diritto alla riservatezza del minore ed ad altri diritti fondamentali, del principio della protezione dei diritti del minore inteso quale soggetto dinamico[215] il diritto ad essere ascoltato[216], il diritto a non essere discriminato[217].

In dettaglio le linee cercano di limitare il raggio d'azione dei soggetti che trattano i dati personali prevedendo tre apposite raccomandazioni per i legislatori[218]: garantire la minimizzazione dei dati e la soddisfazione delle aspettative del minore, limitare gli scopi per i quali è consentito il trattamento dei dati nell'ambiente scolastico, limitare i tempi di conservazione dei dati. Per tutelare maggiormente i minori dovrebbe essere richiesto un innalzamento degli standard di sicurezza ai fornitori di prodotti e servizi

[212] Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale Strasburgo, 28 gennaio 1981
[213] M. R. CARBONE, *Privacy a scuola, ecco le linee guida del Consiglio d'Europa sul trattamento dati dei minori*, https://www.cybersecurity360.it/legal/privacy-dati-personali/privacy-a-scuola-ecco-le-linee-guida-del-consiglio-deuropa-sul-trattamento-dati-dei-minori/
[214] Ex. Art. 5.1 convenzione di Strasburgo op cit.
[215]Ex. Art. 5.2. linee guida del comitato consultivo della convenzione sulla protezione delle persone rispetto al trattamento automatizzato dei dati personali, del 20 novembre 2020.
[216]Ex art. 5.3, linee guida cit.
[217] Ex art. 5.4, linee guida cit.
[218] Ex art. 6, linee guida cit.

a scopo didattico, dotando l'autorità di controllo di risorse sufficienti, intervenendo sulla formazione del personale scolastico, sui contratti pubblici ed infine adottando misure appropriate per "***prevenire, monitorare e indagare sulle violazioni da parte delle imprese nel contesto educativo e nell'ambiente digitale***"[219].

In aggiunta le linee guida richiedono che nel momento in cui vengono utilizzati piattaforme, programmi e simili strumenti digitali ci sia una chiara identificazione dei soggetti coinvolti ed i loro ruoli, perché gli anche loro devono garantire il rispetto dei principi in materia, nonché le misure di sicurezza e garanzia[220]. In particolare, si evidenzia che la loro azione deve svolgersi nel rispetto del principio di legalità, da cui consegue l'impossibilità di trattare dati previo consenso del minore e di comunicare i dati a soggetti terzi, o l'utilizzo a fini analitici e commerciali. Inoltre, viene stabilito il rispetto del principio di valutazione del rischio, tramite l'obbligatorietà della valutazione preventiva dei rischi.

La convezione si conclude con delle raccomandazioni all'industria di settore[221], invitandole a garantire standard adeguati in materia di riservatezza, di modo che tutte le funzionalità dei prodotti siano chiare e trasparenti, per evitare che i prodotti possano spingere i minori a fornire dati non necessari, o a limitare i loro diritti.

8. Osservazioni conclusive

Da uno sguardo complessivo sulle norme riguardanti la tutela della riservatezza in ambito scolastico, si comprende che si tratta di un grave onere che grava sugli operatori scolastici, che si concretizza in una molteplicità di obblighi.

Punto centrale di tutta la disciplina è la norma di legge, perché essa è alla base di ogni trattamento e di ogni garanzia prevista. Tuttavia, il codice privacy ammette la possibilità che vi possa essere un regolamento alla base di un trattamento dei dati sensibili. Da qui la preoccupazione che un regolamento, non emanato nel rispetto della stessa disciplina della norma di legge, possa prevedere dei trattamenti di dati sensibili, particolarmente incisivi e rischiosi per gli interessati. In particolare, per quanto riguarda la gestione del dato, una volta acquisito e la sua comunicazione a soggetti terzi.

Il tutto con il possibile contrasto con il principio di necessarietà e liceità del trattamento, espressi dal Reg., che però consente che la base giuridica sia prevista dal

[219] EX. ART. 6.3.3, LINEE GUIDA CIT.
[220] EX. Art. 7, linee guida cit.
[221] Ex Art. 8, linee guida cit.

"*diritto dello stato membro cui è soggetto il titolare del trattamento"*[222] e quindi lascia aperta la porta anche ad una base di tipo non espressamente legislativo. Tuttavia, una norma contenuta in un regolamento, magari non emanata dal parlamento nazionale o regionale, ma da un ente pubblico, potrebbe portare ad una sottovalutazione delle problematiche connesse al trattamento da parte della PA, con conseguenti fughe di dati accidentali.

Altra criticità è l'assenza di interventi di sensibilizzazione e formazione adeguati al personale scolastico. Questo potrebbe comportare che il trattamento dei dati diventi una delle tante pratiche burocratiche scolastiche, dimenticando che la riservatezza è un diritto fondamentale.

In aggiunta non è stata prevista una disciplina dell'archiviazione dei dati e della loro successiva consultazione, prassi frequente considerando che un ciclo scolastico dura al massimo cinque anni, così come frequente è il ricambio del personale, spesso a tempo determinato.

Un aspetto positivo è l'aver insistito sulla necessarietà della legge, della base giuridica, di modo che ogni volta che un responsabile del trattamento avesse un dubbio, o una qualche incertezza, può trovare un punto di riferimento certo in una norma.

[222] Ex. Art. 6 com. 3 let. b).1 Reg.

GLI OBBLIGHI DI NOTIFICA AL GARANTE E COMUNICAZIONE AGLI INTERESSATI: PECULIARITÀ E CRITICITÀ NELLA GESTIONE *EX POST* DELLA *DATA BREACH* IN ITALIA

di Lorenzo Baudino Bessone

SOMMARIO: 1. Introduzione in materia di *data breach* – 2. L'obbligo di notifica ai sensi dell'art. 33 del GDPR e applicazioni pratiche – 3. L'obbligo di comunicazione agli interessati ai sensi dell'art. 34 del GDPR: modalità e casistica – 4. Le notifiche di *data breach* in Italia: un confronto con i dati europei.

This paper aims to highlight the peculiarities and some critical issues of the regulation provided by the GDPR on the notification to the Supervisory Authority and on the communication to the data subject in the event of a date breach.

The analysis flows over legal topics and focuses on the need to implement the Italian culture around "data protection" and the cooperation beetwen the Italian Data Protection Authority and the controller, with the increasing risk of violations of natural persons' freedom and rights.

1. Introduzione in materia di *data breach*

Le disposizioni sulla violazione di dati personali (cd. data breach) contenute nel Capo IV del Regolamento UE 2016/679 ("*General Data Protection Regulation*" o "GDPR") rappresentano, sotto diversi aspetti, la prospettiva innovativa che il Legislatore europeo ha adottato in materia di protezione dei dati personali.

Gli art. 33 e 34 GDPR, ai quali verrà dato ampio spazio nei prossimi paragrafi, sono, infatti, espressione del nuovo principio di *accountability* ("responsabilizzazione") e dell'approccio cd. "risk based" (gestione del rischio) introdotti dal

Regolamento europeo anche al fine di fronteggiare i più frequenti casi di violazione dei dati personali (cd. *data breach*).[223]

È bene ricordare che, sulla base del disposto dell'art. 4, n. 12, del GDPR, il *data breach* (violazione dei dati personali) può essere definito come una "*violazione di sicurezza che comporta, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati*".

Il suddetto Capo IV del Regolamento troverà, quindi, applicazione, soltanto in caso di violazione dei dati personali, e unicamente nel (non raro) caso in cui, a seguito di tale incidente di sicurezza il titolare del trattamento non sia più in grado di garantire l'osservanza dei principi relativi al trattamento dei dati personali di cui all'art. 5 del GDPR.[224]

Sul punto, il Gruppo di Lavoro Articolo 29 (cd. WP29, poi sostituito dal Comitato Europeo per la protezione dei Dati personali – EDPB) nel Parere 03/2014 sulla notifica delle violazioni di dati personali, ripreso della Linee Guida dell'EDBP del 2021, ha precisato che le violazioni possono essere classificate in base ai tre criteri classici in materia di sicurezza delle informazioni:

1. "*violazione della riservatezza*", in caso di divulgazione o accesso non autorizzati, ai dati personali;
2. "*violazione dell'integrità*", in caso di modifica non autorizzata o accidentale dei dati personali;
3. "*violazione della disponibilità*", in caso di perdita o distruzione, accidentali o illecite di dati personali.[225]

In tale contesto, e fermo restando l'obbligo preventivo di adottare tutte le misure necessarie e adeguate a limitare eventuali pregiudizi conseguenti al *data breach*,[226] il Regolamento prevede in capo al titolare del trattamento due obblighi

[223] G. Finocchiaro, *Introduzione al Regolamento europeo sulla protezione dei dati*, in *Nuove leggi civ. comm.*, 2017, I, 1 ss. e EAD., *Privacy e protezione dei dati personali*, cit., 289 ss.
[224] Tale aspetto mette in evidenza la differenza tra un incidente di sicurezza e una violazione dei dati personali: mentre tutte le violazioni dei dati personali sono incidenti di sicurezza, non tutti gli incidenti di sicurezza sono necessariamente violazioni dei dati personali. In tal senso, Cfr. le recenti Guidelines 01/2021 on Examples regarding Data Breach Notification,14 gennaio 2021, consultabile sul sito *www.edpb.europa.eu*, in cui i Garanti *privacy* europei hanno evidenziato le diverse forme in cui si può manifestare una violazione dei dati personali.
[225] Gruppo Di Lavoro Articolo 29 Per La Protezione Dei Dati, 693/14/IT, WP 213, Parere 03/2014 sulla notifica delle violazioni dei dati personali, 25 marzo 2014, consultabile sul sito *www.ec.europa.eu*.
[226] Vedi art. 32 del GDPR: "*1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:*

di notifica, uno nei confronti dell'Autorità di controllo e l'altro nei confronti degli interessati.

Tali obblighi discendono, rispettivamente, dagli artt. 33 (rubricato: "Notifica di una violazione dei dati personali all'autorità di controllo") e 34 (rubricato: "Comunicazione di una violazione dei dati personali all'interessato") del GDPR che contengono alcune disposizioni in materia di *risk management* per la gestione, *ex post*, di un evento pregiudizievole per i diritti e le libertà degli interessati, come, ad esempio, una violazione di un sistema informatico che comporti la sottrazione dei dati personali ivi raccolti da parte di *hacker* ignoti.

2. L'obbligo di notifica ai sensi dell'art. 33 del GDPR e applicazioni pratiche

La previsione di particolari forme di responsabilità in seguito a gravi violazioni di dati personali è stata introdotta dalla Direttiva 2009/136/CE che, modificando l'art. 4 della Direttiva 2002/58/CE, ha stabilito l'obbligo, per il fornitore di servizi di comunicazione elettronica accessibili al pubblico, di notificare senza indebiti ritardi l'accaduto alle Autorità nazionali di controllo e, in alcuni casi, anche all'interessato.[227]

a) la pseudonimizzazione e la cifratura dei dati personali;
b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.
2. Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.
3. L'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo.
4. Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri"

[227] Art. 4 della Direttiva del 12/07/2002, n. 58, in *Gazzetta Uff. 31/07/2002 n. 201*: "*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, se necessario congiuntamente con il fornitore della rete pubblica di comunicazione per quanto riguarda la sicurezza della rete Tenuto conto delle attuali conoscenze in materia e dei loro costi di realizzazione, dette misure assicurano un livello di sicurezza adeguato al rischio esistente". Fatta salva la direttiva 95/46/CE, le misure di cui al paragrafo 1 quanto meno: - garantiscono che i dati personali siano accessibili soltanto al personale*

Pertanto, rispetto alla precedente Direttiva in materia di protezione dei dati personali, il Regolamento 2016/679 ha ampliato la casistica considerata, estendendola ad ogni tipologia di trattamento di dati personali.

Il disposto contenuto all'art. 33 del GDPR, infatti, riprende la disciplina appena citata e prevede, dunque, in capo al titolare del trattamento, l'obbligo di notificare la violazione di dati personali all'Autorità di controllo competente ai sensi dell'art. 55 GDPR, ossia quella del Paese ove ha avuto luogo la violazione.

In particolare, secondo la disposizione considerata, la notifica dev'essere effettuata dal titolare del trattamento "*senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui è venuto a conoscenza, a meno che sia che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche*".

Il rispetto del termine di 72 ore per la notifica rappresenta sicuramente per i titolari del trattamento uno degli oneri di più difficile adempimento, e ciò non solo per la brevità del termine, ma anche per l'individuazione del relativo termine di decorrenza che la norma individua nella "venuta a conoscenza", da parte del titolare del trattamento, della violazione dei dati personali.

---

autorizzato per fini legalmente autorizzati, - tutelano i dati personali archiviati o trasmessi dalla distruzione accidentale o illecita, da perdita o alterazione accidentale e da archiviazione, trattamento, accesso o divulgazione non autorizzati o illeciti, e - garantiscono l'attuazione di una politica di sicurezza in ordine al trattamento dei dati personali. Le autorità nazionali competenti sono legittimate a verificare le misure adottate dai fornitori di servizi di comunicazione elettronica accessibili al pubblico e a emanare raccomandazioni sulle migliori prassi in materia di sicurezza che tali misure dovrebbero conseguire. Nel caso in cui esista un particolare rischio di violazione della sicurezza della rete, il fornitore di un servizio di comunicazione elettronica accessibile al pubblico ha l'obbligo di informarne gli abbonati indicando, qualora il rischio sia al di fuori del campo di applicazione delle misure che devono essere prese dal fornitore di servizio, tutti i possibili rimedi, compresi i relativi costi presumibili. In caso di violazione di dati personali, il fornitore di servizi di comunicazione elettronica accessibili al pubblico comunica senza indebiti ritardi detta violazione all'autorità nazionale competente. Quando la violazione di dati personali rischia di pregiudicare i dati personali o la vita privata di un abbonato o di altra persona, il fornitore comunica l'avvenuta violazione anche all'abbonato o ad altra persona interessata. Non è richiesta la notifica di una violazione dei dati personali a un abbonato o a una persona interessata se il fornitore ha dimostrato in modo convincente all'autorità competente di aver utilizzato le opportune misure tecnologiche di protezione e che tali misure erano state applicate ai dati interessati dalla violazione della sicurezza. Tali misure tecnologiche di protezione rendono i dati incomprensibili a chiunque non sia autorizzato ad accedervi. Fatto salvo l'obbligo per i fornitori di informare gli abbonati e altri interessati, se il fornitore di servizi non ha provveduto a notificare all'abbonato o all'interessato la violazione dei dati personali, l'autorità nazionale competente, considerate le presumibili ripercussioni negative della violazione, può obbligare il fornitore in questione a farlo. La comunicazione all'abbonato o ad altra persona contiene almeno una descrizione della natura della violazione di dati personali e i punti di contatto presso cui si possono ottenere maggiori informazioni ed elenca le misure raccomandate per attenuare i possibili effetti pregiudizievoli della violazione di dati personali. La comunicazione all'autorità nazionale competente descrive, inoltre, le conseguenze della violazione di dati personali e le misure proposte o adottate dal fornitore per porvi rimedio […]".

Sulla determinazione del momento di "venuta a conoscenza" non sembra, infatti, di grande aiuto per l'interprete neanche l'intervento del Gruppo di Lavoro Art. 29, il quale ha suggerito di far riferimento al momento in cui il titolare del trattamento abbia avuto un "*ragionevole grado di certezza che l'incidente di sicurezza si sia verificato*".[228]

Ad ogni modo, secondo l'interpretazione fornita dal Considerando 87 del Regolamento EU 2016/679, è compito del titolare del trattamento predisporre adeguate misure di sicurezza, tecnologiche e organizzative, al fine di poter tempestivamente valutare il rischio di una violazione dei dati personali.[229]

Il termine stringente di cui sopra è, tuttavia, allentato da una serie di condizioni che possono permettere al titolare del trattamento di notificare la violazione dei dati personali all'Autorità competente anche in un lasso di tempo superiore alle 72 ore.

Da una parte, l'art. 33 riconosce che il titolare del trattamento potrebbe non essere sempre in grado di notificare una violazione entro tale termine e che una notifica tardiva può essere consentita, sempre se giustificata dai motivi che hanno determinato tale ritardo. Dall'altra, unitamente notifica tardiva "giustificata", il titolare del trattamento può procedere alla "notifica per fasi", qualora la natura della violazione subita richieda di effettuare ulteriori accertamenti per esaminare tutti i fatti pertinenti e le conseguenze relativi all'incidente.[230]

---

[228] Guidelines on Personal data breach notification under Regulation 2016/679, 18/EN, WP250rev.01, 3 ottobre 2017, pag. 11 ss., consultabile sul sito *www.ec.europa.eu*: "*the GDPR requires that, in the case of a breach, the controller shall notify the breach without undue delay and, where feasible, not later than 72 hours after having become aware of it. This may raise the question of when a controller can be considered to have become "aware" of a breach. WP29 considers that a controller should be regarded as having become "aware" when that controller has a reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised*"

[229] Considerando 87: "*È opportuno verificare se siano state messe in atto tutte le misure tecnologiche e organizzative adeguate di protezione per stabilire immediatamente se c'è stata violazione dei dati personali e informare tempestivamente l'autorità di controllo e l'interessato. È opportuno stabilire il fatto che la notifica sia stata trasmessa senza ingiustificato ritardo, tenendo conto in particolare della natura e della gravità della violazione dei dati personali e delle sue conseguenze e effetti negativi per l'interessato. Siffatta notifica può dar luogo a un intervento dell'autorità di controllo nell'ambito dei suoi compiti e poteri previsti dal presente regolamento*".

[230] La notifica non è richiesta ai sensi dell'art. 33 quando sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Cfr. M. Mandico, "Data breach", in M. Mandico, *Privacy e GDPR: manuale applicativo con esempi e casistiche settoriali*, Maggioli Editore, Santarcangelo di Romagna, 2019, pp. 167-173. L'esempio consueto è dato dal caso dei dati personali già disponibili pubblicamente, la cui divulgazione non costituirebbe un rischio probabile per la persona fisica sebbene, come osservato *supra*, tale ipotesi non si applica ai fornitori di servizi di comunicazione elettronica accessibili al pubblico di cui alla direttiva 2009/136/CE, che stabilisce che tutte le violazioni rilevanti devono essere notificate all'Autorità competente.

L'impostazione "per fasi" risulta, peraltro, coerente con l'ulteriore adempimento demandato al titolare del trattamento in ordine al contenuto della notifica in oggetto. Il titolare del trattamento deve, infatti, inoltrare all'Autorità Garante una comunicazione che descriva, ai sensi del già richiamato art. 33 del GDPR, da un lato, la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione, nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione, e, dall'altro, le probabili conseguenze della violazione per i diritti e le libertà degli interessati coinvolti, nonché le misure adottate o di cui il titolare si propone l'adozione per porre rimedio alla violazione dei dati personali e, se del caso, per attenuarne i possibili effetti negativi.

Il Garante *privacy* italiano, conscio delle difficoltà incontrate dal titolare del trattamento nel dover diligentemente adempiere ai gravosi obblighi imposti dal GDPR, al fine di supportare i titolari del trattamento, ha creato sul proprio sito istituzionale un "servizio telematico dedicato al *data breach"* che include una scheda informativa sul *data breach,* un modello compilabile di notifica di *data breach* e una procedura di auto-valutazione ("*self assessment*") che supporta il titolare nell'individuazione delle azioni da intraprendere a seguito di una violazione di dati personali , facilitando l'assolvimento degli obblighi in materia di notifica di una violazione dei dati personali all'autorità di controllo e di comunicazione di una violazione dei dati personali all'interessato.[231]

3. L'obbligo di comunicazione agli interessati ai sensi dell'art. 34 del GDPR: il caso di Ho. mobile

Oltre all'obbligo di notifica di cui si è appena detto, ai sensi dell'art. 34 del GDPR, il titolare del trattamento è tenuto, in alcuni casi, a comunicare la violazione dei dati personali alle persone fisiche interessate.

La norma circoscrive tale adempimento ai casi in cui la violazione dei dati personali possa produrre "*un rischio elevato per i diritti e le libertà delle persone*

[231] Il portale è accessibile sul sito: *https://servizi.gpdp.it/databreach/s/*.

fisiche". Analogamente alla notifica all'Autorità, anche la comunicazione, ove necessaria, dev'essere effettuata "*senza ingiustificato ritardo*".[232] Tale locuzione, e con essa l'individuazione del termine congruo a garantirne il rispetto, incontra le stesse difficoltà interpretative già descritte al paragrafo precedente. Ancora una volta, infatti, il GDPR, nel Considerando 86, non sembra venire in soccorso all'interprete nel prevedere che: "*il titolare del trattamento dovrebbe comunicare all'interessato la violazione dei dati personali senza indebito ritardo, qualora questa violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà della persona fisica, al fine di consentirgli di prendere le precauzioni necessarie* […]. *Tali comunicazioni agli interessati dovrebbero essere effettuate non appena ragionevolmente possibile* […]. *Ad esempio, la necessità di attenuare un rischio immediato di danno richiederebbe che la comunicazione agli interessati fosse tempestiva, ma la necessità di attuare opportune misure per contrastare violazioni di dati personali ripetute o analoghe potrebbe giustificare tempi più lunghi per la comunicazione*".

Quanto, poi, al contenuto minimo della comunicazione, che dovrà essere fornita in *"linguaggio semplice e chiaro*", l'art. 34, al paragrafo 2, richiama i medesimi contenuti previsti per la notifica all'Autorità di controllo.

Nella sezione del sito istituzionale relativa ai *data breach*, il Garante per la Protezione dei dati personali richiama, quindi, le disposizioni sopra indicate, ribadendo che la violazione deve essere comunicata a tutti gli interessati, utilizzando i canali più idonei e confermando che "*il titolare dovrebbe fornire consulenza specifica alle persone fisiche sul modo in cui proteggersi dalle possibili conseguenze negative di una violazione dei dati ad esempio reimpostando le password in caso di compromissione delle credenziali di accesso*".[233]

Le pronunce dell'Autorità di controllo italiana sul tema delle forme e dei contenuti della comunicazione agli interessati sono diverse[234] ed inoltre utili insegnamenti sulla corretta gestione dei rapporti con gli interessati possono essere tratti,

[232] Fermo restando che anche in tale caso l'obbligo di comunicazione viene meno quando sia improbabile, a maggior ragione rispetto all'obbligo di notifica, che dalla violazione possano derivare rischi per i diritti e le libertà delle persone fisiche, cfr. M. Mandico, "Data breach", cit., pag. 173.
[233] Manuale RPD – Linee guida destinate ai Responsabili della protezione dei dati nei settori pubblici e parapubblici per il rispetto del Regolamento generale sulla protezione dei dati dell'Unione Europea (Regolamento (UE) 2016/679), luglio 2019, pag. 247, consultabile sul sito *www.garanteprivacy.it*.
[234] Provvedimento n. 499 su *data breach* del 13 dicembre 2018 e provvedimento n. 106 su *data breach* del 30 aprile 2019, consultabili *Ibid.*

altresì, dall'osservazione diretta della gestione delle violazioni dei dati personali da parte delle Aziende coinvolte in casi eclatanti e noti al pubblico, pur allorquando agli stessi non consegue un intervento sanzionatorio da parte dell'Autorità competente. Ne è un esempio il caso di *data breach* che ha coinvolto Ho. Mobile, un operatore di telefonia mobile italiano, e che ha portato alla sottrazione di dati personali (dati anagrafici e dati tecnici della SIM) degli utenti da parte di alcuni *hackers*. Venuto a conoscenza della violazione di sicurezza subita, l'operatore telefonico, in qualità di titolare del trattamento, si è attivato notificando (pur con ritardo) al Garante la violazione dei dati personali, innalzando le proprie difese informatiche e fornendo agli interessati una comunicazione chiara e dettagliata, perfettamente in linea con il quadro normativo di riferimento sin qui delineato.

Ed infatti, il titolare del trattamento in questione ha ritenuto che dalla violazione dei dati personali subita poteva scaturire un rischio elevato per i diritti e le libertà delle persone fisiche [si pensi alle insidiose truffe di tipo "*sim swap*" che sarebbero state facilitate con la conoscenza dei dati anagrafici e dei dati delle Sim degli utenti] ed ha conseguentemente:

- informato gli interessati coinvolti con comunicazione via *sms*;
- predisposto una pagina *web* informativa in forma di *Faq* che ha permesso agli interessati di informarsi sui rischi e sulle modalità di prevenzione del rischio;[235]
- arginato il rischio, modificando il numero seriale delle Sim di tutti gli utenti coinvolti dalla violazione.

Ed infine, la comunicazione così predisposta da Ho. mobile risulta soddisfare anche i requisiti richiesti dal paragrafo 3 dell'art. 34 GDPR che permette al titolare del trattamento, nel caso in cui la *data breach* abbia coinvolto un numero significativo di interessati, di procedere ad una comunicazione pubblica che permetta di informare gli interessati con efficacia analoga alla comunicazione diretta.[236]

[235] Vedi la pagina: *www.ho-mobile.it/comunicazione/data-breach-faq/*.
[236] L'art. 34, par. 3 del GDPR elenca, più in generale, i casi in cui la comunicazione diretta agli interessati non è necessaria, ossia quando "*il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura; il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui al paragrafo 1*".

4. Le notifiche di *data breach* in Italia: un confronto con i dati europei

Alla luce di tutte le considerazioni operate nei precedenti paragrafi, il motivo dell'urgenza di arginare il fenomeno della *data breach*, implementando le previsioni in materia di *risk management* introdotte dal GDPR è presto spiegabile. Il costante ripetersi di furti di dati e l'incremento della frequenza e/o entità di tali eventi, dimostrano come, stante il crescente valore delle informazioni personali, la prevenzione di tali rischi, attraverso l'adozione da parte del titolare del trattamento di strumenti adeguati e controlli periodici degli stessi, non sempre si dimostri efficiente e sufficiente a scongiurare il verificarsi di violazioni dei dati personali.[237]

Secondo uno studio recente, in Europa, nel periodo compreso tra il 28 gennaio 2020 e il 27 gennaio 2021 sono state effettuate, in media, 331 notifiche di violazione dei dati personali al giorno, con un aumento del 19% rispetto al media di notifiche al giorno dell'anno precedente confermando la tendenza attuale di una crescita a doppia cifra di anno in anno.[238] Ciononostante in Italia, nello stesso periodo, è stato calcolato un totale di circa 3460 notifiche di violazione dei dati personali: un valore minimo se relazionato quello calcolato in Germania, sempre nel medesimo periodo, e pari a 77.747 notifiche di *data breach*.

Tale dato lascia presumere che in Italia vi sia un'elevata percentuale di società che, anche a causa di una scarsa sensibilità per la materia della *data protection*, troppo spesso vista soltanto come un mero e oneroso costo per l'Azienda, non hanno portato a termine con successo il processo di adeguamento al GDPR e che non sono ancora strutturalmente capaci di rispettare tutti gli obblighi imposti dalla nuova normativa. Ciò, soprattutto, con riferimento a quegli adempimenti – come la notifica di *data breach* – che, rispetto ad altri (ad esempio, il rilascio dell'informativa *privacy* agli interessati e/o la richiesta del consenso al trattamento dei loro

[237] A. Mantelero, "Il nuovo approccio della valutazione del rischio nella sicurezza dei dati", in G. Finocchiario, *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Zanichelli Editore, Bologna, 2017, 287-326.

[238] DLA Piper, *GDPR fines and data breach survey: January 2021*: *a report by DLA Piper's cybersecurity and data protection team*. Secondo tale studio, l'Autorità Garante italiana si è classificata prima in Europa per valore totale delle sanzioni comminate a seguito di *data breach* (€ 69,328,716) e al terzo posto per valore delle sanzioni individuali con una multa ad un operatore di telecomunicazioni di € 27,8 milioni a gennaio 2020 per una serie di violazioni del GDPR, fra le quali: violazioni relative agli obblighi di trasparenza, non avendo una sufficiente base giuridica per il trattamento dei dati personali, e inadeguata misure tecniche e organizzative e violazione del principio della *privacy by design* (violazione degli artt. 5, 6, 17, 21 e 32 GDPR).

dati personali), risultano di più difficile interpretazione e gestione per i titolari del trattamento.[239]

Proprio tali circostanze inducono, con elevata probabilità, molte Aziende a non notificare le violazioni subite nel timore che l'effettuazione di una notifica possa tradursi nel rischio di subire verifiche e ispezioni da parte del Garante *privacy*, finalizzate ad acquisire maggiori elementi di valutazione in ordine alla portata, alle cause ed alle conseguenze della violazione stessa e dunque destinate ad evidenziare tutte le mancanze del Titolare nella predisposizione ed attuazione del proprio Modello organizzativo *data protection*.

[239] Garante Privacy, *Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali*, consultabile sul sito *www.garanteprivacy.it*. Come spiegato dal Garante in tale guida, la notifica di una violazione trova le proprie radici in un preliminare processo di valutazione del rischio che compete esclusivamente al titolare del trattamento – in forza del più generale principio di "*accountability*" o responsabilizzazione su cui si fonda l'intero impianto normativo del GDPR – e che, per essere condotto in maniera efficiente, deve necessariamente basarsi su una radicata conoscenza della materia.

Coordinamento editoriale:

Gruppo di lavoro *Data Protection Law*

This work is published under a Creative Commons Attribution-NonCommercial-No-Derivatives 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.