DIPARTIMENTO DI ECONOMIA, SOCIETÀ E POLITICA

CORSO DI DOTTORATO DI RICERCA IN ECONOMIA, SOCIETÀ E DIRITTO

Curriculum: Diritto – Sviluppo, diritti dell'uomo, diritti sociali fondamentali e formazioni sociali

CICLO XXXI°

RESPONSABILITÀ PENALE DEL DATA PROTECTION OFFICER E TUTELA TRANSNAZIONALE DELLA PRIVACY DOPO IL REGOLAMENTO (UE) 2016/679.

S.S.D: Diritto Penale (IUS/17)

RELATORE
Chiar.mo Prof. Lucio Monaco

DOTTORANDO
Dott. Gian Marco Pellos

Anno Accademico 2017/2018

RESPONSABILITÀ PENALE DEL DATA PROTECTION OFFICER E TUTELA TRANSNAZIONALE DELLA PRIVACY DOPO IL REGOLAMENTO (UE) 2016/679.

"La preoccupazione dell'uomo e del suo destino devono sempre costituire l'interesse principale di tutti gli sforzi tecnici. Non dimenticatelo mai in mezzo a tutti i vostri diagrammi ed alle vostre equazioni".

(Albert Einstein)

A.M.D.G.

INDICE

INTRODUZIONE

Se qualche anno fa si fosse detto all'autore di questa tesi che avrebbe approfondito la tematica della privacy, questi sarebbe apparso alquanto perplesso.

Gli sforzi dei delicati anni post-lauream infatti, erano stati fino a quel momento rivolti ad altri obiettivi ma, come spesso capita nella vita, i percorsi si aprono senza aver fatto nulla di particolare per imbattervisi e così una serie di coincidenze e incontri inaspettati hanno messo lo scrivente di fronte a quella che all'epoca era la bozza del regolamento europeo di riforma della tutela dei dati personali nell'Unione Europea, l'odierno Regolamento (UE) 2016/679.

In quel momento, in cui ancora termini come G.D.P.R. e D.P.O. erano pressoché sconosciuti all'opinione pubblica e risuonavano solo in poche sedi specializzate, la possibilità di presentare un progetto di dottorato sul tema rappresentava al contempo una sfida affascinante e un salto nel buio; vi era la consapevolezza di mettere le mani su qualcosa che avrebbe rappresentato, in un prossimo futuro, un cambiamento importante dal punto di vista giuridico e, nello stesso momento, l'incertezza su quali sarebbero stati i punti salienti su cui sarebbe stato opportuno concentrare l'attenzione.

Dall'inizio del percorso dottorale nel 2015, quindi, gli sforzi sono stati rivolti a seguire il dibattito che prendeva progressivamente piede non più solo nell'ambito delle istituzioni europee ma anche fra docenti, giuristi, professionisti di vari settori, imprenditori, politici, fino a divenire di dominio pubblico dal mese di maggio del 2018.

Questo ha consentito di apprezzare i tanti risvolti legali, sociali ed economici di un tema a volte viene avvertito come chiuso in un tecnicismo giuridico fine a sé stesso e che invece rappresenta a pieno titolo una frontiera del diritto, nella quale sono in gioco aspetti decisivi per la tutela della dignità umana.

Una frontiera, tra l'altro, che è destinata a rimanere per lungo tempo al centro di qualsiasi dibattito in materia di diritti umani che voglia avere una rilevanza concreta nella società dell'*Internet of Things.*

In questa opera di osservazione e confronto, l'oggetto della ricerca si è andato man mano definendo.

Si è così deciso di approfondire la figura del Data Protection Officer (il Responsabile della protezione dei dati), che rappresenta una delle novità sulle quali più si è concentrata l'attenzione degli osservatori.

Infatti con l'introduzione di questa nuova figura, il regolamento ha fatto un deciso salto di qualità nell'ottica di garantire l'apporto di una competenza specialistica nella tutela dei dati personali.

È questa d'altronde una diretta e concreta conseguenza del principio di *accountability* che costituisce la vera spina dorsale dell'innovazione portata dal G.D.P.R., perché chiede di passare dall'idea di un "elenco delle cose a fare" a quella di dover confezionare "un abito su misura", ossia garantire la difesa dei dati in concreto, in relazione alle specificità della struttura e alle caratteristiche dei trattamenti.

Da questo punto di vista, il D.P.O. può essere visto come il presidio che assicura, grazie alla sua preparazione, lo sviluppo di questo approccio nelle aziende e nelle amministrazioni.

Come spesso accade quando vi è una novità legislativa di questo genere, nei mesi che hanno seguito l'entrata in vigore del Regolamento (UE) 2016/679 in molti hanno visto in questa nuova figura un'opportunità professionale da cogliere, pur rimanendo ancora diversi aspetti non del tutto chiari circa i requisiti, i compiti e soprattutto il regime di responsabilità connessi a questo ruolo.

Si è quindi pensato nella ricerca di lavorare proprio sugli aspetti penalistici legati ad esso, non certo per fornire risposte definitive che, si ritiene potranno venire solo dalla giurisprudenza, bensì per contribuire alla riflessione e alla formazione di una consapevolezza adeguata rispetto a una professione che certamente è di grande interesse e di sicuro sviluppo ma che è anche estremamente delicata e non può in alcun modo essere presa alla leggera.

La posizione del D.P.O. è strategica ai fini di una corretta gestione dei dati e della prevenzione dei fattori di rischio legati alla privacy; alla luce dello sviluppo tecnologico degli ultimi decenni questo tipo di analisi non può prescindere dalla dimensione internazionale, su cui pure si è posta l'attenzione, in primo luogo descrivendo le modalità attraverso cui mettere in atto una corretta circolazione internazionale dei dati,

in modo da garantirne la sicurezza, oltre che la tutela dei diritti degli interessati e in secondo luogo andando a descrivere quale sia lo stato dell'arte relativo agli aspetti criminalistici che coinvolgono la privacy. Sono state passate in rassegna le fattispecie penali di riferimento e si è posto l'accento sugli aspetti che ineriscono la dimensione internazionale del problema, rispetto ai quali il contributo del D.P.O. può venire in rilievo sia in termini di prevenzione degli illeciti sia in termini di responsabilità.

Nel corso della trattazione, si è preferito fare uso per lo più dei termini e degli acronimi in lingua inglese, pur dando atto della traduzione in lingua italiana.

Lo si è fatto non già per sterile esterofilia ma perché si è pur sempre davanti a un regolamento europeo, destinato ad essere riconosciuto, nei suoi elementi caratteristici, da giuristi e operatori di tutto il mondo, i quali fanno usualmente ricorso alle definizioni in inglese. D'altronde chi intenda cimentarsi, sia per studio che a livello professionale, con la materia della privacy, dovrà necessariamente entrare in un'ottica internazionale, avendo certamente a che fare con istituzioni europee e, molto probabilmente, con soggetti stranieri.

Va infine opportunamente segnalato che i temi di ricerca, approfonditi nel corso di questi anni, hanno formato oggetto di pubblicazioni, alcune delle quali sono state in parte riportate come capitoli della tesi, come indicato in nota (cap. II e IV).

CAPITOLO I

L'EVOLUZIONE DEL DIRITTO ALLA PRIVACY E LE INCOGNITE DELLA SOCIETÀ DEI DATI

1. L'origine del diritto alla privacy. - 2. Le implicazioni sociali, culturali e politiche del diritto alla privacy. - 2.1. I monopoli dei dati e i timori dei cittadini. - 3. Evoluzione del diritto alla privacy. - 3.1 Le premesse in Europa: la tutela del domicilio domestico. - 3.2. L'affermazione della privacy nel sistema dei diritti umani in Europa e in Italia. - 3.3. Dalla riservatezza alla data protection. - 3.3.1. La Convenzione di Strasburgo e la Direttiva 95/46/CE. - 3.4. La Carta di Nizza e la scissione fra riservatezza e protezione dei dati. - 4. Dati in pericolo, persone in pericolo - 5. La riforma europea sulla protezione dei dati. - 5.1. I Principi fondamentali del Regolamento (UE) 2016/679 - 5.2. L'accountability come chiave di lettura della nuova privacy.

1. L'origine del diritto alla privacy

Agli albori del secolo scorso lo scrittore portoghese Fernando Pessoa, scriveva di quanto sarebbe stato semplice, dopo la sua morte, scrivere una biografia su di lui; due sole date erano rilevanti: quella della nascita e quella della morte, perché i giorni intercorsi fra l'una e l'altra appartenevano a lui soltanto.[1].

Non sappiamo quali riflessioni si celassero dietro questo pensiero del maestro dell'eteronomia; ciò che però appare chiaramente è la ferma volontà di operare una cesura netta fra la propria persona e il mondo.

Pur se sarebbe di indubbio interesse, non è questa la sede per svolgere una riflessione sul significato dei versi dell'autore portoghese e d'altronde non sapremo mai se in queste

[1] Cfr. Pessoa F., *Se depois de eu morrer* (1913-1915), in *Poemas Inconjuntos*, il testo in lingua originale è disponibile in "Arquivo Pessoa" (http://arquivopessoa.net/textos/996), ultima cons. 30.10.2018.

poche righe egli volesse in qualche modo reclamare non solo una distanza ideologica dal mondo a sé vicino ma anche una tutela della propria riservatezza.

Ciò che però fa amaramente sorridere è il pensare che questa aspettativa di Pessoa, se già sarebbe stata difficile da soddisfare da parte di una persona vissuta a cavallo fra il XIX° e il XX° secolo, sarebbe praticamente irrealizzabile nel contesto odierno, in cui in pochi secondi è possibile sapere di ciascuno di noi ben più che i dati anagrafici, con buona pace dei desideri del poeta, del quale infatti sono facilmente rinvenibili in rete decine di dettagliate biografie.

Ad ogni buon conto, la volontà di rimanere estranei al mondo, a cavallo fra '800 e '900 non connota solo il mondo letterario.

Qualche anno prima infatti, un'aspettativa di questo genere aveva animato le penne, forse non altrettanto poetiche ma sicuramente efficaci, di due giovani e lungimiranti giuristi di Boston: Samuel Warren e Louis Brandeis.

Poiché Warren aveva difficoltà con i giornali locali, che avevano iniziato a riportare le gesta mondane di sua moglie in una misura che egli considerava inaccettabile, scrisse insieme al collega Brandeis il famoso articolo *The Right to Privacy*[2]. In tale articolo, una volta riconosciuti e delineati magistralmente i confini del diritto di cronaca e di informazione, stabiliva il loro limite nel contrapposto *right to be let alone*, il diritto a essere lasciati soli e a non vedere invasa senza motivo la propria sfera di intimità personale e di relazione.

Nel fare ciò, essi fecero leva sui sentimenti che devono albergare nel moderno uomo civilizzato, i quali devono fungere da barriera contro l'assalto delle curiosità morbose e degli strumenti invadenti di cui si servono[3].

---

[2] Warren S., Brandeis L., *The Right to Privacy*, in "Harvard Law Review", Vol. IV, December 15, 1890, n. 5.

[3] In particolare, in un passaggio del citato articolo si legge: "Owing to the nature of the instruments by which privacy is invaded, the injury inflicted bears a superficial resemblance to the wrongs dealt with by the law of slander and of libel, while a legal remedy for such injury seems to involve the treatment of mere wounded feelings, as a substantive cause of action"; è emblematico il riferimento alla natura degli strumenti cui si fa riferimento, invasivi della privacy.

Non stupisce, in verità, che proprio in quel momento storico si sia sentita l'esigenza di difendere gli spazi di intimità dalle intromissioni di una tecnologia che diveniva sempre più pervasiva e capillarmente diffusa, a beneficio di una società che la utilizzava in modi non sempre edificanti.

Tutto è cambiato da allora e, allo stesso tempo, niente è cambiato.

Sicuramente negli ultimi cento anni, e in particolar modo negli ultimi trenta, l'impatto della tecnologia e i cambiamenti della società hanno portato a nuove elaborazioni del concetto di privacy, facendo affiorare problemi del tutto inediti e impensabili per le generazioni precedenti; non si è persa però la necessità di tutelare gli aspetti più intimi e privati della propria esistenza e della propria persona, esigenza che si trova a dover essere declinata in un contesto decisamente più complesso e contraddittorio.

In un certo senso, si può ben dire che l'esigenza di difendere una dimensione "privata" sia sempre stata presente nel mondo occidentale, tanto che già nella Grecia antica si separava l'ambito della *oikòs* da quello della *pòlis*, poiché la prima era la dimora della relazionalità e la seconda il luogo dove l'individuo diveniva parte di un superiore e più complesso meccanismo politico[4].

Tuttavia, a partire dal *paper* di Warren e Brandeis, il concetto di privacy ha iniziato uno sviluppo che pare ben lungi dall'essersi concluso e che ha recepito le diverse istanze della società e del rapport o fra le persone e la tecnologia.

2. Le implicazioni sociali, culturali e politiche del diritto alla privacy

Già verso la fine del secolo scorso il Prof. Rodotà, che per primo guidò l'Autorità garante per la protezione dei dati personali, ebbe a constatare come non avesse più senso declinare il concetto di privacy secondo la tradizionale accezione di diritto alla riservatezza il quale, beninteso, manteneva intatta la sua importanza; tuttavia negli

[4] Cfr. Cangiotti M., *Dalla sfera privata alla sfera del diritto alla privacy. Evoluzione o distorsione dello spazio pubblico?*, in Congiunti L., Ndreca A., Formica G. (a cura di), *Oltre l'individualismo: Relazioni e relazionalità per ripensare l'identità*, pp. 115-126, Urbaniana University Press, Città del Vaticano 2017; nel suo contributo l'autore svolge un'approfondita analisi delle problematiche affrontate in questo paragrafo. Cfr. anche: Niger S., *Le nuove dimensioni della privacy, dal diritto alla riservatezza alla protezione dei dati personali*, in *Contratto e Impresa*, serie diretta da Francesco Galgano, Cedam, 2006, capitoli I e II.

ultimi decenni del XX° secolo si era già fatta largo una nuova lettura del concetto tradizionale di privacy, secondo la quale il cuore della tutela risiedeva nel diritto a mantenere il controllo delle informazioni riguardanti la propria persona e, di conseguenza, lo sviluppo normativo avrebbe dovuto assecondare questa esigenza[5].

Secondo questa logica, quindi, riferendosi alla privacy del terzo millennio, ci si riferisce soprattutto al "diritto di mantenere il controllo sulle proprie informazioni"[6] e la sfera privata si realizza in "quell'insieme di azioni, comportamenti, opinioni, preferenze, informazioni personali su cui l'interessato intende mantenere un controllo esclusivo non solo per garantirne la riservatezza, ma per assicurarsi una piena libertà di scelte"[7]

Il tempo ha saputo dimostrare la correttezza dell'analisi del Professore, perché il solco che si è venuto a creare fra la dimensione della semplice riservatezza e quella, figlia della rivoluzione informatica, della protezione dei dati, ha portato alla necessità di stabilire norme sempre più specifiche e tecniche, che siano sostegno efficace a quei diritti e a quella capacità di controllo che i cittadini, utenti del mondo digitale, chiedono a gran voce di vedere riconosciuti non solo formalmente ma effettivamente.

D'altronde, parlare di privacy oggi significa parlare non solo di diritto ma anche di una certa posizione culturale, o meglio di un aspetto del diritto che è incastonato nella cultura odierna, quale premessa logico-giuridica necessaria del principio di autodeterminazione.

Questi aspetti venivano già acutamente sottolineati alcuni anni dalla Prof.ssa Marta Cartabia, secondo la quale proprio a partire dall'elaborazione teorica del diritto alla privacy si è fatta strada tanto negli Stati Uniti che in Europa una cultura che fa perno su di esso per giustificare ogni sorta di rivendicazione individuale in campo giuridico[8]:

---

[5] Cfr. Rodotà S., *Repertorio di fine secolo*, Laterza, Roma-Bari, 1992, pp. 189-190.

[6] Ibidem

[7] Ibidem

[8] Cfr. Cartabia M., *I nuovi diritti*, in "Stato, Chiese e pluralismo confessionale" - Rivista telematica, febbraio 2011, pp. 11-14 (https://www.statoechiese.it/images/uploads/articoli_pdf/cartabia_i_nuovi.pdf?pdf=i-nuovi-diritti), ultima cons. 26.10.2018.

> "Oggi in tutto il mondo occidentale tutto ciò che ha a che fare con questioni «morali» o «eticamente controverse» tende ad essere dominato dal principio di autodeterminazione, il quale a sua volta genera tutta una serie di nuovi diritti individuali: dal diritto di sposarsi e di divorziare, alla libertà di scelta in relazione ai problemi dell'inizio della vita, – in particolare con riferimento all'aborto e all'accesso alle tecniche di fecondazione assistita – il diritto al rifiuto dei trattamenti sanitari nelle problematiche di fine alla vita, ecc. Con questa nuova generazione di nuovi diritti originati dalla privacy si diffonde sempre più la versione *libertarian* dei diritti umani"[9].

Inoltre, quando ci si riferisce alla privacy nel contesto odierno, non si può non tenere in considerazione lo straordinario valore che hanno i dati personali nell'economia contemporanea.

Da più parti questi sono stati descritti come il nuovo "oro nero" del commercio odierno; avere accesso ai dati e saperli analizzare significa possedere le informazioni necessarie per pianificare l'offerta dei propri servizi, anticipare le richieste del mercato e, perchè no, indirizzarle.

Non a caso sono sorte negli ultimi anni nuove figure professionali legate alla gestione, all'analisi e alla capitalizzazione dei dati (si pensi per esempio al Data Scientist, al Data Manager o al Data Engineer) e addirittura corsi di studio *ad hoc*.

Ultimo elemento da considerare, ma non per importanza, è legato agli aspetti geopolitici cui la tutela dei dati è intrinsecamente connessa; essere padrone dei dati significa infatti poter esercitare un controllo sulle persone, conoscerne gli orientamenti e stabilire gli aspetti sui quali è opportuno puntare, ad esempio, in una campagna elettorale e come indurre le persone a seguire una certa idea.

Non è un caso che, ad oggi, tutti i partiti e i movimenti politici maggiori si siano assicurati la collaborazione di esperti nell'analisi dei dati, grazie ai quali elaborare le strategie di comunicazione più adatte ai singoli contesti.

2.1. I monopoli dei dati e i timori dei cittadini

[9] Ivi, p. 13; sull'espressione *libertarian* l'autrice fa riferimento a: Glendon M.A., *Rights Talk*, New York, USA, 1991, p. 48 ss.

Soprattutto, la mole di dati generati dalle tecnologie di ultima generazione, fornisce a pochi grandi soggetti una concentrazione di conoscenze che non ha precedenti nella storia dell'umanità, non solo dal punto di vista quantitativo ma anche e soprattutto dal punto di vista qualitativo, vista l'invasività di strumenti tecnologici che sono ormai indispensabili per compiere decine e decine di azioni quotidiane, durante le quali raccolgono i dati di chi li usa.

È accaduto sovente che tali informazioni non siano state utilizzate in modo lecito e trasparente; basti pensare a quanto scandali vengano narrati nei notiziari per rendersi conto delle potenziali capacità di utilizzo di queste banche dati.

Non può non venire alla mente il celeberrimo romanzo di Orwell "1984" con il suo famoso "Grande Fratello" e tuttavia nemmeno la fantasia dello scrittore britannico avrebbe immaginato una tale capacità di ottenere informazioni, per giunta in modo del tutto libero e consenziente (anche se spesso non del tutto consapevole) da parte dei cittadini e non per mezzo di ordini o sotterfugi di tiranni.

Le informazioni in questione sono estremamente appetibili per grandi aziende, lobbies, criminalità internazionale e governi; le cronache d'altronde sono piene di episodi di violazioni più o meno gravi.

Tutto ciò ha fatto sì che, con il tempo, l'opinione pubblica sia passata da una visione entusiasta del mondo tecnologico e in particolare di internet, visto come la porta per una conoscenza potenzialmente infinita e come possibilità di comunicazione libera e democratica, ad una lettura più disincantata del fenomeno.

Così dunque, mentre si fa strada un nuovo mondo basato sull'*internet of things*, che altro non è che una "evoluzione della rete Internet grazie alla quale gli oggetti interagiscono tra loro attraverso sensori e senza l'intervento umano, scambiandosi informazioni e accedendo ai contenuti presenti nelle banche dati"[10] e vengono sviluppate tecnologie che, dall'essere strumenti nelle mani degli uomini, tendono a far diventare questi ultimi strumenti delle proprie elaborazioni, si è registrato negli ultimi anni anche il passaggio

[10] Gaeta M.C., *La protezione dei dati personali nell'internet of things: l'esempio dei veicoli autonomi* in "Diritto dell'Informazione e dell'Informatica (Il)", fasc.1, 2018, pag. 147.

da un approccio sostanzialmente indifferente al tema della privacy, ritenuto dalla maggior parte delle persone di un orpello normativo per addetti ai lavori o, al massimo, un prezzo accettabile da pagare per poter avere accesso a nuove sorprendenti forme di conoscenza, ad una odierna maggiore consapevolezza dell'importanza di un'adeguata tutela dei propri dati e dei propri diritti, sui quali si è sempre meno disponibili a scendere a compromessi sia con i governi che con i grandi colossi della rete.

3. Evoluzione del diritto alla privacy

Tutto quanto detto permette di considerare come la tutela dei dati personali non possa di certo essere definita un diritto statico.

Invero, le sue plurime manifestazioni e molteplici sfaccettature lo hanno sempre contraddistinto come un diritto di cui è difficile fornire una definizione ultima, perché caratterizzato da una natura dinamica e in perenne evoluzione.

Si dirà che, al giorno d'oggi, questo è un discorso che vale praticamente per ogni ambito del diritto, ma nel caso della privacy queste caratteristiche erano emerse già prima che l'avvento del mondo globalizzato, di internet e delle grandi tecnologie di comunicazione portassero gli ordinamenti giuridici a un inevitabile confronto con rapidi e imprevisti cambiamenti e con una diffusa contaminazione fra diverse culture giuridiche.

Gli approdi del diritto alla privacy sono stati diversi; si pensi che in America, che pure ne è stata culla naturale, l'evoluzione del diritto alla privacy è stata connotata da uno strano destino.

Da una parte infatti, esso è stato posto a fondamento di numerose battaglie civili ed è stato ampiamente approfondito dal punto di vista teorico e giurisprudenziale, mentre dall'altra la sua codificazione ha sempre latitato e quand' anche si è proceduto a tradurre il diritto in esame in norme positive, lo si è fatto in modo settoriale e non unitario.[11]

Questo consente di capire meglio per quale motivo, nella storia americana, il diritto alla privacy sia spesso entrato in conflitto con il diritto alla sicurezza nazionale, in particolare

[11] Cfr. cap. IV, p. 2.1. di questa Tesi.

dopo gli eventi dell'11 settembre 2001 e la legislazione d'emergenza che ne è derivata come conseguenza.

3.1 Le premesse in Europa: la tutela del domicilio domestico

Diversa sorte ha avuto il pensiero di Warren e Brandeis nel momento in cui ha attraversato l'Atlantico approdando in Europa.

Qui, in verità, vi era sempre stato un forte riconoscimento del valore del domicilio e della casa familiare risalente nel tempo e fatto proprio dai valori della società borghese; famosa è a tal proposito l'espressione "every man's home is his castle"[12]; in effetti l'appassionata difesa della propria dimora come luogo precluso alle incursioni del potere politico riemerge in modo cristallino nelle parole di Lord Chatham, che nel parlamento britannico del 1766 ebbe a esclamare: "The poorest man, may, in his cottage, bid defiance to all the forces of the Crown. It may be frail; its roof may shake; the wind may blow through it; the storm may enter; the rain may enter; but the King of England may not enter; all his forces dare not cross the threshold of the ruined tenement"[13].

Probabilmente per questo motivo, quando il concetto di privacy formulato dai due Giuristi di Boston giunse nel vecchio continente, trovò un terreno fertile in cui attecchire, pur se con caratteristiche differenti, che avrebbero prodotto frutti diversi rispetto a quelli americani. Una difformità destinata a durare e anzi, se possibile, a manifestarsi in maniera sempre più evidente fino ai giorni nostri, in cui permangono punti di vista sostanzialmente distanti nel modo di affrontare questo tema giuridico, tanto da creare spesso tensioni diplomatiche fra una sponda e l'altra dell'atlantico.

---

[12] La frase è da attribuirsi al giudice inglese Sir Edward Coke, che l'ha pronunciata nella sentenza in merito al *Semayne's Case*, con la quale venivano stabiliti limiti alla facoltà degli uomini del Re di irrompere nel domicilio di un suddito.

[13] Testo rivenuto in Fellman D., *The Defendant Rights Today*, The University of Wisconsin Press, Wisconsin, 1976, p. 256, il quale richiama a sua volta Cooley T.M., *Constitutional limitations*, 8th ed. (Boston: Little, Brown & Co., 1927), I: 611; Traduzione libera: "Il più povero degli uomini, può, nella sua casa, opporre la propria sfida a tutte le forze del Re. Per quanto possa essere fragile la casa, per quanto il vento possa soffiarvi attraverso, vi ci possa entrare la tempesta e piovere dentro, il Re di Inghilterra non può entrarvi e tutte le sue forze non possono attraversare quella soglia".

Quella che si è andata sviluppando in Europa in materia di privacy è infatti una cultura che ha messo al centro la libertà dal potere politico, rivendicata alla stregua di un vero e proprio diritto fondamentale della persona, soprattutto dal secondo dopoguerra in avanti, dopo la tragica esperienza degli Stati totalitari di matrice nazifascista e in funzione di opposizione al blocco sovietico[14].

È d'altronde noto ed evidente che il grado di tutela della privacy sia un ottimo indicatore del livello di democraticità e libertà di un sistema politico; non a caso uno dei principali intenti delle dittature è proprio quello di poter esercitare un controllo capillare di ogni forma di comunicazione senza alcun limite di tempo e luogo; così operavano la S.T.A.S.I., l'O.V.R.A. e il K.G.B.

Con diverse accezioni quindi, può dirsi che il rispetto della privacy faceva già parte dell'*humus* comune agli ordinamenti giuridici dei diversi stati europei e come tale è stato accolto in tutte le principali carte e trattati che hanno costituito o comunque influenzato la costruzione di quell'*unicum* fra i sistemi giuridici internazionali che è l'Unione Europea.

Essa infatti presenta elementi propri così inediti nella storia degli ordinamenti sovranazionali, che non è possibile ricondurla nell'alveo dei sistemi federali, né tantomeno nel novero degli ordinamenti dotati di sovranità[15], bensì deve essere considerata come un *tertium genus*, una architettura istituzionale di nuovo conio che però si fonda sulle tradizioni giuridiche comuni ai vari paesi che la compongono.

3.2. L'affermazione della privacy nel sistema dei diritti umani in Europa e in Italia

Già nel 1950 la Convenzione Europea per la salvaguardia dei Diritti dell'Uomo e delle libertà fondamentali aveva riconosciuto con l'articolo 8, il "*diritto al rispetto della vita privata e familiare*".

Tale riconoscimento, pur contenuto in un documento che era ed è cosa diversa rispetto al progressivo formarsi dell'ordinamento comunitario, è comunque indicativo di quanto

[14] cfr. Rodotà S. *Intervista su Privacy e Libertà* (a cura di Conti P.), Laterza, Bari, 2005.

[15] cfr. Adam R., Tizzano A., *Manuale di diritto dell'Unione Europea*, seconda edizione, Giappichelli Editore, Torino, 2017, p. 3-5.

poc'anzi affermato, e cioè della presenza originaria di una tutela della riservatezza nell'ambito domestico in tutto il territorio europeo.

Invero, l'articolo 8 della convenzione non riconosce un diritto alla privacy come modernamente inteso e a ben pensarci non potrebbe essere altrimenti, vista l'epoca storica in cui è stata stipulata la convenzione.

Tuttavia, è proprio su questo articolo 8 della CEDU che è intervenuta nel tempo la Corte europea dei diritti dell'uomo di Strasburgo, con un'attività interpretativa elaborata e capace di ricavare una tutela sempre più ampia e in linea con il mutare dei tempi[16].

Un ampio numero di sentenze[17] hanno fatto leva sul rispetto della vita privata per assicurare ai cittadini la tutela di un'ampia gamma di situazioni che ancora non erano provviste di forme di tutela ad hoc[18].

Nel frattempo, anche nell'ordinamento italiano si faceva strada la progressiva affermazione del diritto enunciato da Warren e Brandeis.

Non si è trattato in verità di un percorso scontato, perché i primi approdi giurisprudenziali tendevano a non riconoscere l'esistenza di un diritto alla riservatezza giuridicamente autonomo e separato da altri istituti giuridici già noti.

La prima statuizione rilevante in tal senso si ha con la sentenza n. 4487 del 22 Dicembre 1956 della Corte Suprema di Cassazione, la quale, appunto, non riconosceva un autonomo valore al diritto alla riservatezza.

Il caso è legato alla nota figura di un famoso artista, i cui parenti si erano opposti alla realizzazione di un film che ne narrasse le gesta, soprattutto perché venivano illustrati i suoi primi anni di carriera, connotati da una situazione economica alquanto incerta.

---

[16] Cfr. Rossi E.A., *Il diritto alla Privacy nel quadro giuridico europeo ed internazionale alla luce delle recenti vicende sulla sorveglianza di massa*, in "Diritto comunitario e degli scambi internazionali", n. 3/2014, p. 341-342.

[17] Si pensi a: Corte europea dei Diritti dell'Uomo, Grande Camera (Strasburgo) Caso *S. e Marper c. Regno Unito*, sentenza 4 dicembre 2008 (ricorsi nn. 30562/04 e 30566/04); Corte europea dei diritti dell'uomo, sentenza del 9 ottobre 2012, causa n. 42811/06; Corte europea dei diritti dell'uomo, sentenza del 3 aprile 2007, causa n. 62617/00, Corte europea dei diritti dell'uomo, sentenza del 28 gennaio 2003, causa n. 44647/98.

[18] Sul punto si veda anche Pizzetti F., *Privacy e il diritto europeo alla protezione dei dati personali, il regolamento europeo 2016/679*, Giappichelli Editore, Torino, 2016, pp. 225-254.

I parenti avevano ritenuto che, così facendo, erano stati rappresentati fatti che nulla avevano a che fare con un interesse pubblico a conoscere la vita del personaggio, essendo molte scene afferenti a una realtà familiare che veniva in tal modo violata nella sua riservatezza.

Gli ermellini in tale circostanza ritennero di non accogliere queste argomentazioni, giudicarono invece che non vi fosse all'interno dell'ordinamento italiano un fondamento normativo in base al quale rivendicare il diritto alla riservatezza, come invece accadeva per altri diritti soggettivi. Pertanto riprodurre, pure artisticamente e fantasiosamente, storie di vita di altre persone, di cui si aveva avuta conoscenza in maniera lecita, era da ritenersi pienamente legittimo[19].

A partire dagli anni '60 però, la tendenza ha iniziato a cambiare; in particolare con la sentenza numero 990 del 1963 della Suprema Corte di Cassazione.

La vicenda giudiziaria aveva stavolta ad oggetto alcuni articoli che un settimanale aveva dedicato ad aspetti intimi e inediti di un personaggio molto discusso e della sua famiglia, che andavano a investigare anche su aspetti di vita non legati ad una qualche rilevanza per l'interesse pubblico.

Pure in tal caso, la Suprema Corte confermava il diniego al riconoscimento di un autonomo diritto alla riservatezza della vita privata, tuttavia nel suo argomentare trapelava l'inizio di un mutamento di posizione:

> "sebbene non sia ammissibile il diritto tipico alla riservatezza. viola il diritto assoluto di personalità, inteso quale diritto *erga omnes* alla libertà di autodeterminazione nello svolgimento della personalità dell'uomo come singolo, la divulgazione di notizie relative alla vita privata, in assenza di un consenso almeno implicito, ed ove non sussista, per la natura dell'attività svolta dalla persona e del fatto divulgato, un preminente interesse pubblico di conoscenza"[20].

Un mutamento di orientamento progressivo quindi, che si sarebbe poi compiuto negli anni '70 con il riconoscimento definitivo del diritto alla riservatezza.

---

[19] Cfr. Corte di Cassazione, Sezione I Civile, Sentenza 22 Dicembre 1956, n. 4487.

[20] Corte di Cassazione Civ., Sentenza del 20 aprile 1963 n. 990, massima tratta da Allegri M. R., *Informazione e comunicazione nell'ordinamento giuridico italiano*, Giappichelli Editore, Torino, p. 24.

A tal proposito, viene in rilevo soprattutto la sentenza della Corte di Cassazione, sez. I civile, 27 maggio 1975, n. 2129.

La sentenza trae le mosse dalla richiesta dell'ex consorte di un monarca orientale che si era vista ripudiare dal marito a seguito della pubblicazione di alcuni scatti intimi con un altro uomo durante un soggiorno in Italia, circostanza che le aveva fatto perdere anche tutti i benefici economici connessi con la sua posizione.

Costei, viste le conseguenze evidentemente pregiudizievoli avute dalla non richiesta pubblicazione di quelle immagini, ritenendo che non vi fosse alcun motivo per cui queste dovessero essere fatte oggetto di attenzione da parte dell'opinione pubblica, chiese che le fosse riconosciuto il risarcimento dei danni subiti a causa della condotta dei giornalisti, che nulla aveva di meritevole per l'interesse pubblico e che era sconfinata in una inutile e dannosa ingerenza nella vita privata.

Sul punto, il Giudice di legittimità così ha statuito:

> "Deve ritenersi esistente nel nostro ordinamento un generale diritto della persona alla riservatezza, inteso alla tutela di quelle situazioni e vicende strettamente personali e familiari le quali, anche se verificatesi fuori del domicilio domestico, non hanno per i terzi un interesse socialmente apprezzabile, contro le ingerenze che, sia pure compiute con mezzi leciti, per scopi non esclusivamente speculativi e senza offesa per l'onore, la reputazione o il decoro, non siano giustificate da interessi pubblici preminenti"[21]

Ecco quindi che il diritto alla riservatezza, antesignano dell'odierna *data protection*, trovava la sua collocazione teorica all'interno del panorama giuridico italiano quale diritto della persona, inerente quindi alla dimensione individuale del singolo e non più solo come corollario della tutela sfera domiciliare.

[21] Massima a Corte di Cassazione, Sezione I civile; sentenza 27 maggio 1975, n. 2129 di Monteleone M. in "Il Foro Italiano", Vol. 99, 1976, Parte Prima: Giurisprudenza Costituzionale e Civile, p. 2896.

3.3. Dalla riservatezza alla data protection

Ora che il diritto aveva raggiunto le istanze che la società aveva manifestato da tempo, già si profilavano nuove sfide che ne avrebbero messo alla prova la capacità di adattamento.

Proprio dalla fine degli anni '70 infatti, è iniziato quel progressivo e inarrestabile percorso di sviluppo di strumenti elettronici capaci di immagazzinare e comunicare dati, che ha portato all'affermazione prima della società della comunicazione di massa e poi allo sviluppo del settore delle *Information Technologies* e infine all'*Internet of Things.*

Naturalmente, in un primo momento tali strumenti erano appannaggio solo di grandi strutture complesse ma nel corso degli anni si sono sviluppati rapidamente e diffusi capillarmente. Telefoni cellulari, computer, sistemi GPS, ecc.., che già negli anni '80 avevano iniziato a diffondersi, nell'ultima decade del millennio entreranno a tutti gli effetti nella vita quotidiana di milioni di persone divenendo indispensabili, soppiantando le precedenti tecnologie e comportando una vera rivoluzione anche nel mondo del lavoro, da momento che molti mestieri di antica tradizione si sono trovati ad essere del tutto obsoleti nell'arco di pochi anni.

3.3.1. La Convenzione di Strasburgo e la Direttiva 95/46/CE

Sin da subito le nuove soluzioni tecniche e i servizi realizzati attraverso queste tecnologie si sono contraddistinte per la necessità di utilizzare in maniera intensiva i dati personali che erano in grado di raccogliere.

Non è un caso quindi che già la Convenzione di Strasburgo, n. 108 del 1981, ratificata in Italia con l. n. 98 del 1989, avesse sancito la necessità di approntare una tutela specifica ai dati personali e non più semplicemente alla riservatezza della vita domestica e relazionale.

È logico ed evidente infatti che già in quegli anni si sentisse l'esigenza di tutelare le informazioni che i nuovi macchinari tecnologici erano capaci di processare e utilizzare, poiché era palese che quelle informazioni erano legate a soggetti fisici che meritavano tutela.

Pur se la mole di informazioni processata dalle tecnologie dell'epoca era decisamente inferiore rispetto ad oggi, risultavano già evidenti i rischi connessi alle capacità di controllo che era possibile esercitare attraverso tali strumenti sui soggetti che li utilizzavano e i percoli derivanti da eventuali sottrazioni o perdite di dati.

La Convenzione di Strasburgo del 1981 è un passaggio spesso trascurato dell'evoluzione della disciplina giuridica della privacy in Europa, tuttavia leggendone i contenuti si intravede chiaramente l'ossatura di quelli che saranno i successivi interventi normativi di stampo comunitario.

Ivi vengono infatti enunciati, per esempio, i principi di liceità e correttezza dei trattamenti e si distinguono particolari categorie di dati nei confronti delle quali occorre adottare cautele maggiori (le cd. "categorie speciali" di cui all'art.6 della convenzione).

L'importanza del passaggio realizzato con questa convenzione è data dal fatto che "essa segna un punto di svolta tra una visione del diritto alla *privacy* sostanzialmente statica (quella legata all'intangibilità della sfera privata dell'individuo) ad una dinamica che prende in considerazione i pericoli per la persona di fronte al crescente flusso di dati che la riguardano trattati con strumenti automatizzati"[22].

Su queste premesse si è poi sviluppata nel 1995 la famosa direttiva n. 46 della Comunità Europea, che sanciva definitivamente una nuova linea interpretativa del concetto di privacy, ora legato alla tutela dei dati personali, che rispetto al diritto alla riservatezza costituiva non più un semplice corollario ma si connotava come un'autonoma e distinta fonte di tutele nei confronti dei cittadini.

Non si trattava più di chiedere a un soggetto estraneo, che fosse lo Stato o i privati, di rimanere al di fuori di determinati ambiti della propria vita; ora il cittadino chiedeva di avere il controllo delle informazioni che della sua vita quotidiana circolavano grazie alle nuove tecnologie disponibili, di essere informato circa la raccolta e l'utilizzo dei dati che forniva, nonché di poter aggiornare ogni informazione lo riguardasse e, se del caso, ottenerne la cancellazione.

---

[22] Modafferi F., *Lezioni di diritto alla protezione dei dati personali, alla riservatezza e all'identità personale*, Lulu.com, Roma, 2015, p. 43.

È questa una fondamentale novità che si inseriva sulla scia di quanto già affermato dalla convenzione di Strasburgo dei 1981 e che era il frutto di un mutamento non solo tecnologico ma anche culturale.

Da una parte vi era la necessità di stabilire dei limiti di liceità al trattamento automatizzato dei dati, dall'altra quella di permettere a ciascun soggetto il potere di intervenire sulle informazioni che lo riguardavano, garantendogli, almeno formalmente, di esercitare il controllo e la gestione sulle informazioni che afferivano alla propria persona.

Sulla base della direttiva 46/95 è stata adottata in Italia prima la l. n. 675 del 1997 e poi d.lgs. n. 196 del 2003, che è stato a lungo considerato uno strumento di assoluta avanguardia legislativa, tant'è vero che ha resistito a lungo ed è tutt'ora vigente, pur se ampliamente ridimensionato e strutturalmente modificato ad opera del d.lgs. n. 101 del 10 agosto 2018, che è intervenuto per armonizzarlo con il Regolamento (UE) 2016/679.

3.4. La Carta di Nizza e la scissione fra riservatezza e protezione dei dati

Ultimo ma fondamentale passaggio per ricostruire il quadro europeo in materia di protezione dei dati personali è costituito dalla Carta dei Diritti Fondamentali dell'Unione Europea, detta anche carta di Nizza dal nome della città che il 7 dicembre 2000 ne ha accolto la stipula.

La carta fornisce un'interpretazione legislativa della privacy sicuramente più adeguata ai tempi rispetto a quella della CEDU.

Il passaggio più rilevante, ai fini che qui interessano, sta nell'aver scisso il "*rispetto della vita privata e della vita familiare*", enunciato all'articolo 7, dal "*diritto alla protezione dei dati personali*", enunciato all'articolo 8.

Da un certo punto di vista, il portato innovativo dell'art. 8 non ha solo l'esito di consacrare a un più alto livello la tutela dei dati, facendo emergere il *quid pluris* rispetto alla "semplice" riservatezza, ma soprattutto quello di riconoscere tale tutela come diritto proprio della persona e non come appendice del libero trasferimento di merci e servizi

nel mercato interno europeo, declinazione quest'ultima in cui la Direttiva tendeva a relegare il ruolo della *data protection*[23].

Veniva quindi solennemente consacrata la cesura fra questi due diritti, che l'opinione comune ancora accomuna nel concetto di *privacy*; entrambe le dimensioni afferiscono sì a diritti fondamentali della persona ma l'oggetto della tutela è diverso e tale diversità riflette l'esigenza di garantire strumenti adeguati a tutelare i cittadini dalle conseguenze nefaste di un uso distorto dei dati personali che al giorno di oggi possono essere realizzate specie per mezzo delle tecnologie informatiche.

Si tratta quindi di una gemmazione del concetto di privacy, ad oggi indiscussa e decisiva per una compiuta valutazione del quadro dei diritti fondamentali, a maggior ragione perché è stata recepita, insieme a tutta la Carta di Nizza, dall'art. 6 del Trattato sull'Unione Europea, firmato a Lisbona il 13 dicembre 2007, divenendo così giuridicamente vincolante per tutti gli stati membri.

4. Dati in pericolo, persone in pericolo

Potrà sembrare un esercizio futile, ma se si pensa per un momento a come sono mutate le abitudini quotidiane delle persone nell'ultimo ventennio, si riesce a comprendere bene la portata dei temi che si stanno affrontando, sia in termini quantitativi che qualitativi.

A cavallo del nuovo millennio, infatti, era già iniziato lo sviluppo di quelle tecnologie di comunicazione che oggi sono diventate parte integrante della quotidianità della popolazione, tuttavia si trattava di strumenti le cui funzionalità erano assai limitate e la cui presenza nella vita quotidiana era tutto sommato limitata.

Inoltre, e soprattutto, le implicazioni con il diritto alla privacy erano decisamente minori.

È sotto gli occhi di tutti come invece, nel contesto attuale, le capacità tecnologiche abbiano reso i dispositivi di uso quotidiano quasi delle "appendici naturali" del corpo umano, il cui funzionamento è pressochè costante perchè, una volta connessi alla rete internet, possono continuamente elaborare e inviare dati, indipendentemente dal se, dal

[23] Cfr. Pollicino O., *Un digital right to privacy preso (troppo) sul serio dai giudici di lussemburgo? il ruolo degli artt. 7 e 8 della carta di nizza nel reasoning di Google spain* in "Diritto dell'Informazione e dell'Informatica (Il)", fasc.4-5, 2014, pag. 572.

quando e dal quanto vengano effettivamente usati dai proprietari (costoro, in verità, li usano per le più svariate necessità, dal cercare un indirizzo al leggere una email, fino a sapere quante calorie contiene un pasto, ecc...).

Naturalmente, tutto questo si accompagna alla produzione di un'enorme mole di informazioni, che afferisce alla vita dei singoli individui come di intere popolazioni.

Non può ovviamente dirsi che le nuove tecnologie non abbiano portato dei vantaggi o che non aiutino lo svolgimento delle attività quotidiane, tuttavia non si deve dimenticare che, a fare da contraltare, vi è il moltiplicarsi dei rischi per la tutela dei dati, che poi si traducono sempre in pericoli per la dignità e la sicurezza della persona.

I dati raccolti permettono di conoscere le abitudini, le opinioni, le caratteristiche più recondite di un soggetto; possono essere analizzati fino ad ottenere una vera e propria profilazione, che i malintenzionati potrebbero utilizzare, all'occorrenza, per fini illeciti.

Da questo punto di vista, sono diversi i fronti dai quali possono giungere delle minacce. Numerose inchieste e scandali hanno segnato in questi anni il rapporto fra cittadini, tecnologie, politica e istituzioni nazionali. Se da una parte è necessario che le pubbliche autorità possano avere accesso ai dati dei propri cittadini quando è necessario svolgere attività di sicurezza e sorveglianza, è altrettanto vero che sulla base di questa premessa sono state realizzate in alcune occasioni anche forme di controllo illecite, sproporzionate ed inutilmente pervasive, come è avvenuto per il caso del *Datagate*, che si avrà di approfondire nel corso del quarto capitolo.

Allo stesso modo, se è vero che è lecito fare uso di dati per fini di propaganda politica, è chiaro ed evidente che nel perseguire tali finalità occorra particolare sensibilità alla conformità normativa delle azioni poste in essere, cosa che sembra essere mancata in numerosi casi, anche recenti, in cui si sono rese manifeste le implicazioni di analisi talmente personalizzate da fare addirittura riflettere se sia configurabile, ad esempio, un contrasto fra l'uso delle applicazioni sociali ed il libero e segreto esercizio del proprio voto[24].

[24] Cfr. Frosini T. E., *Internet e democrazia*, in "Diritto dell'Informazione e dell'Informatica (Il)", fasc.4-5, 2017, p. 669, nel quale comunque l'autore ritiene di non condividere tale preoccupazione; sul rapporto fra democrazia e tecnologie di comunicazione un approfondimento interessante è stato

Ciò detto, è indubbio che le maggiori preoccupazioni di cittadini e imprese riguardino la crescita del fenomeno del *cybercrime*, che si è sviluppato in uno allo sviluppo della rete internet e che si serve proprio di dati personali carpiti o utilizzati illecitamente per dare seguito a progetti criminosi.

Purtroppo, la casistica in questo settore è estremamente vasta e alcune tipologie di condotte illecite sono oramai divenute note anche all'opinione pubblica, data la loro diffusione. Si pensi alla clonazione di carte di credito, al phishing, al furto di dati finalizzato all' estorsione, alle conseguenze che può avere la pubblicazione online di dati, immagini e informazioni sottratte da archivi informatici[25] o ai potenziali esiti dell'intrusione in sistemi informatici, specie quelli che servono a trattare i dati in strutture strategiche o particolarmente delicate, quali gli ospedali[26].

Man mano che aumentano le capacità degli strumenti tecnologici, di pari passo aumenta l'abilità della criminalità organizzata nello sviluppare sistemi idonei ad attentare alla segretezza delle comunicazioni, all'integrità dei dati e alla loro riservatezza.

Nel mentre, non sempre il diritto vigente dispone degli strumenti necessari per garantire quella tutela attesa dai cittadini, circostanza particolarmente evidente in Italia, dove il tema dei reati informatici è rimasto principalmente disciplinato dalla l. 23 dicembre 1993,

---

svolto in Ciarlo P., *Democrazia, partecipazione popolare e populismo al tempo della rete* in "Rivista AIC", n. 2/2018; ivi l'autore, dopo aver dato atto a p. 10 che "Il microtargeting politico, cioè un tipo di comunicazione capace di raggiungere persona per persona i singoli elettori in modo sostanzialmente occulto, ormai è una realtà", invita a p. 11 a riflettere sul fatto che "Bisogna essere confidenti nel fatto che i poteri della rete possono trovare adeguati bilanciamenti. Il più pericoloso dei poteri della rete è quello di manipolare il voto. Questo potere può determinare la fine della democrazia. Orwell lo aveva già intuito, ma se possibile la rete è andata anche oltre. Si tratta di riconsiderare la categoria della "democrazia totalitaria" utilizzata per indicare quei sistemi istituzionali che nel rispetto formale delle procedure della democrazia instaurano dei sistemi nella sostanza totalitari. Non possiamo rassegnarci a che la persuasione digitale sia la fine della ragione."

[25] A titolo di esempio, si pensi che nel 2015 degli hacker riuscirono a sottrarre e pubblicare i dati contenuti nei database di un sito canadese, noto per offrire la possibilità di incontri extraconiugali. La rivelazione dei nominativi delle persone iscritte ha portato a crisi coniugali, alla fine di carriere professionali e, soprattutto, al suicidio di alcune delle persone coinvolte.

[26] Significativo è a tal proposito il passaggio del Discorso del Presidente dell'autorità garante, Antonello Soro, in occasione della presentazione della relazione annuale 2017, nel quale sottolinea l'attenzione del Garante rispetto all'utilizzo delle tecnologie di intelligenza artificiale il cui utilizzo, pur incoraggiato, ha dato luogo ad alcuni *data breach*; v. Garante per la protezione dei dati personali, *Discorso del Presidente Antonello Soro, Relazione 2017, Proteggere i dati per governarne la complessità*, Roma, 10 luglio 2018, p. 18-19. Il testo è disponibile sul sito del Garante Privacy (www.garanteprivacy.it)

n. 547, secondo logiche che a volte sono apparse frammentarie ed eccessivamente complesse[27].

La criminalità informatica è fenomeno di grande rilievo, dalle caratteristiche sfuggenti, che richiede indagini particolarmente elaborate e preoccupa molto professionisti, aziende e semplici cittadini.

Per organizzare una risposta soddisfacente occorrono senz'altro strumenti tecnici e giuridici all'altezza da parte degli operatori di polizia e della magistratura, tuttavia si ritiene che ciò solo non basti, perché è necessario essere in grado di organizzare una difesa della privacy che parta "dal basso", da una cultura condivisa e attenta a questi temi, per poi poterne garantire la tutela "all'esterno", poiché l'orizzonte d'azione è per forza di cose la scena internazionale.

Entrambi questi aspetti emergono dalla lettura della novella europea in materia di protezione dei dati, che si procede ora a illustrare nei suoi passaggi salienti.

5. La riforma europea sulla protezione dei dati

Giunti a questo punto occorre interrogarsi su quali pilastri il legislatore europeo abbia voluto fondare la tutela dei dati offerta dal Regolamento (UE) 2016/679, affinché la stessa possa rivelarsi efficace davanti alle minacce che sorgono in maniera sempre più aggressiva nel contesto odierno.

Senza dubbio una delle maggiori preoccupazioni che emergono dai lavori preparatori, iniziati nel 2012[28], è stata quella di riuscire a garantire una normativa concretamente applicabile, coerente e, soprattutto, il più possibile uniforme, in modo da essere riconosciuta e osservata a livello internazionale dal momento che, soprattutto grazie

[27] Cfr. Flor R., *Phishing, identity theft e identity abuse. Le prospettive applicative del diritto penale vigente*, in "Rivista italiana di diritto e procedura penale", fasc.2-3, 2007, pp. 938-946.

[28] In data 25 gennaio 2012 la Commissione europea ha adottato la *Proposta di Regolamento Del Parlamento Europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (regolamento generale sulla protezione dei dati) /* COM/2012/011 final - 2012/0011 (COD) */*, dando inizio così a un iter legis durato quattro anni.

all'avvento di internet, il valore di distanze e confini oggi risulta assai relativo rispetto al passato[29].

D'altronde, le continue rivelazioni su scandali legati a crimini o comunque ad operazioni scorrette in materia di dati personali avevano portato a un clima di sfiducia rispetto al quale era necessario porre un argine[30]; davanti a questa sfida le istituzioni dell'Unione hanno risposto non solo predisponendo una nuova legislazione ma anche, soprattutto, chiedendo di adottare una nuova mentalità.

Su queste premesse, in data 27 aprile 2016 sono stati approvati il Regolamento n. 679 del 2016, sulla quale si concentrerà maggiormente l'analisi in questa dissertazione, e la Direttiva n. 680 del 2016[31].

---

[29] Sul punto, fra i tanti interventi, merita menzione il considerando n. 11 del documento del Parlamento Europeo *Posizione del Parlamento europeo definita in prima lettura il 12 marzo 2014 in vista dell'adozione del regolamento (UE) n. .../2014 del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (regolamento generale sulla protezione dei dati)* del 12 marzo 2014, che così si esprimeva: "Per garantire un livello uniforme di protezione delle persone in tutta l'Unione e prevenire disparità che possono ostacolare la libera circolazione dei dati nel mercato interno, è necessario un regolamento che garantisca certezza del diritto e trasparenza agli operatori economici, comprese le micro, piccole e medie imprese, offra alla persona in tutti gli Stati membri il medesimo livello di diritti giuridicamente tutelati, definisca obblighi e responsabilità dei responsabili del trattamento e degli incaricati del trattamento e assicuri un monitoraggio costante del trattamento dei dati personali, sanzioni equivalenti in tutti gli Stati membri e una cooperazione efficace tra le autorità di controllo dei diversi Stati membri".

[30] Cfr. Ivi, Cons. n. 6; sul punto vedi anche: Commissione Europea, *Comunicazione della Commissione al Parlamento Europeo e al Consiglio Ripristinare un clima di fiducia negli scambi di dati fra l'UE e gli USA*, Bruxelles, COM (2013) 846 final, 27.11.2013., redatto in risposta alle rivelazioni sul *Datagate*.

[31] I nomi per esteso di questi atti legislativi sono: *Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)* e *Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio*.
Entrambi gli atti legislativi sono stati pubblicati sulla Gazzetta ufficiale dell'Unione europea L 119 del 4 maggio 2016 ed entrambi sono stati rettificati il 23 Maggio 2018. Per completezza, fra le misure adottate nella giornata del 27 aprile 2016 in materia di protezione di dati personali va ricordata anche la *Direttiva (Ue) 2016/681 del Parlamento Europeo e del Consiglio del 27 aprile 2016 sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi*.

Per quanto concerne il regolamento, esso fa sicuramente propri molti aspetti della precedente direttiva 95/46/CE e della elaborazione giurisprudenziale da questa è scaturita nel tempo ma, pur riconoscendo una continuità con la disciplina pregressa, è necessario sottolineare la presenza di modifiche strutturali nel modo di intendere la tutela dei dati personali.

Per ciò che in questa sede interessa, è d'uopo rilevare come non sarebbe possibile affrontare il tema del Data Protection Officer senza prima svolgere una panoramica dei principi che caratterizzano il General Data Protection Regulation.

5.1. I Principi fondamentali del Regolamento (UE) 2016/679

Da questo punto di vista, la prima osservazione va svolta in relazione al principio di trasparenza; esso è enunciato principalmente all'articolo 12 del Reg. (UE) 2016/679 e costituisce la *condicio sine qua non* per qualsiasi trattamento di dati voglia definirsi lecito. In particolare, la norma sottolinea l'importanza di fornire informazioni che siano non solo esaurienti ma anche chiare, concise e facilmente comprensibili da parte degli interessati, anche minori[32].

Non solo, corollario del principio di trasparenza è la funzione agevolatrice che il titolare del trattamento deve svolgere nei confronti dei diritti dell'interessato; il regolamento, sotto questo profilo, insiste sulla funzione proattiva che le diverse figure chiamate ad assumere responsabilità in ordine alla protezione dei dati devono essere in grado di esercitare[33].

Si tratta di una nuova lettura del ruolo del titolare del trattamento, che si può rinvenire anche in un ulteriore passaggio importante, che riguarda il principio di portabilità dei dati (*right to data portability* nella versione inglese), in ragione del quale è necessario che i dati possano essere facilmente trasferibili da parte di un interessato fra diversi supporti

[32] Cfr. art. 12, par. 1 Reg. (UE) n. 2016/679.

[33] Cfr. art. 12, par. 2 - 5 Reg. (UE) n. 2016/679; per quanto concerne la relazione fra trasparenza e portabilità dei dati, cfr. Pizzetti F. (a cura di), *La protezione dei dati personali e la sfida dell'intelligenza artificiale*, in "I diritti nella 'rete' della rete", collana diretta da Pizzetti F., Giappichelli Editore, Torino, 2018, pp. 19-23.

nel caso in cui il trattamento, oltre che su di una base lecita, avvenga per mezzo di strumenti automatizzati[34].

Inoltre, non può non essere menzionato in questa lista il famoso "diritto all'oblio", (*right to be forgotten*) che in verità era già stato introdotto per via giurisprudenziale[35] e che ora è stato positivizzato all'art. 17 del regolamento.

Esso prevede la possibilità per l'interessato di chiedere la cancellazione dei dati che lo riguardano e che siano stati acquisiti illecitamente o rispetto ai quali non sussista più un interesse pubblico al trattamento o perché si è esaurito lo scopo per il quale erano stati raccolti ed è venuta meno la base giuridica per la liceità del trattamento.

Non deve trarre in errore il fatto che si senta spesso parlare di diritto all'oblio in relazione a personaggi famosi; il campo di applicazione d tale diritto è infatti ben più ampio e riguarda potenzialmente ciascun cittadino che si trovi nella condizione di voler chiedere la cancellazione dei propri dati da un determinato servizio che non intende più utilizzare o che voglia comunque impedire la diffusione di notizie sul suo conto che siano state pubblicate per errore o che comunque dovrebbero essere rettificate.

Si tratta di operazioni tecnicamente non sempre facili e che il legislatore europeo impone in capo al titolare, il quale dovrà provvedervi a richiesta dell'interessato e, inoltre, dovrà informare della necessaria cancellazione anche gli altri eventuali soggetti cui i dati siano stati forniti.

A tal fine egli dovrà disporre delle tecnologie e delle competenze necessarie per realizzare lo scopo e si tratta di un compito tutt'altro che semplice, che dimostra con evidenza la difficoltà di accordare tecnica e diritto.

Ne discende che, per poter attuare concretamente e diffusamente tanto il diritto alla portabilità quanto il diritto all'oblio, occorre predisporre a monte soluzioni tecniche idonee.

Questo porta quindi a focalizzare l'attenzione su altri fondamentali principi strutturali del Regolamento Europeo.

---

[34] Cfr. art. 20, par. 1 Reg. (UE) n. 2016/679.

[35] La sentenza di riferimento a tal proposito è la Sentenza della Corte (Grande Sezione) del 13 maggio 2014, Causa C-131/12.

L'art. 25 prescrive la necessità di predisporre la "protezione dei dati fin dalla progettazione" e la "protezione dei dati per impostazione predefinita"; tali disposizioni sono meglio note con la definizione inglese di *privacy by design* e *privacy by default*.

In base alle disposizioni del regolamento, per assicurarsi che i sistemi e le tecnologie che trattano i dati personali siano in grado di rispettare la privacy, si prevede che essi, sin dalla fase di ideazione e progettazione, debbano essere organizzati in modo da tutelare i dati e le informazioni che dovranno elaborare conformemente alla normativa. In tal modo i nuovi sistemi potranno operare solo ed esclusivamente nel rispetto dei dati degli utenti, come per impostazione predefinita, appunto.

Per essere operativo, questo approccio necessita giocoforza di una combinazione di più fattori: il diritto, la tecnica e la capacità di organizzazione, che sono elementi indispensabili per far sì che i diritti della persona, e con il essi il valore del singolo individuo, non si vadano perduti nell'ambiente informatizzato[36]; ben può dirsi che invece il sistema che si vuole implementare deve prevedere che quegli stessi strumenti tecnologici, dai quali può giungere il pericolo per la tutela delle posizioni giuridiche che qui interessano, siano volti in funzione servente rispetto alle queste ultime ed essere utilizzati per garantirne *ab origine* il rispetto.

Merita menzione, inoltre, la previsione secondo la quale i titolari dovranno fare ora riferimento a una sola autorità di controllo in caso di ricorsi attinenti alla violazione dei dati personali.

È questo il meccanismo nominato *one-stop-shop*, o "sportello unico" nella definizione italiana, il quale dispone che in caso di aziende con sedi dislocate in diversi paesi, si debba fare riferimento a una sola autorità di controllo e cioè quella competente con riferimento alla sede principale dell'azienda, in presenza delle altre condizioni di cui all'articolo 56, che disciplina la fattispecie.

A ben vedere, si possono rintracciare in queste disposizioni due preoccupazioni di fondo: vi è senz'altro l'esigenza di permettere ai cittadini di esercitare effettivamente i

[36] Cfr. Calzolaio S., *Protezione dei dati personali*, in *Digesto delle Discipline Pubblicistiche - Aggiornamento* - diretto da Sacco R.; Bifulco R., Celotto A., Olivetti M. (a cura di), Utet Giuridica, Milano, 2017, pp. 610-611.

propri diritti ma, ancor di più, quella di garantire un'uniforme interpretazione e applicazione del regolamento in tutta l'Unione Europea[37], ragione quest'ultima che sottende al meccanismo dello "sportello unico", che se per certi versi risulta complesso per il cittadino, che può vedersi costretto a rivolgersi ad autorità di altri paesi , per contro permetterà nel tempo, almeno questo è l'auspicio, di garantire una difesa dei diritti più chiara e condivisa nello spazio europeo.

Si scorge, in questa tensione all'uniformità, la consapevolezza da parte del legislatore europeo che sarà ben difficile ottenere il rispetto per i dati dei cittadini dell'Unione da parte delle grandi potenze mondiali se, dal canto suo, l'Unione e gli Stati membri non saranno in grado di raggiungere una legislazione, una prassi e una cultura veramente condivise.

Tutto questo, tuttavia, non potrebbe comprendersi né tantomeno realizzarsi se non alla luce del principio di accountability, reso in italiano con la definizione di "responsabilità del titolare del trattamento", il cui valore permea tutto il regolamento.

[37] Sul punto è illuminante un passaggio del documento del Garante Europeo per la Protezione dei dati, *Sintesi esecutiva del parere del Garante europeo della protezione dei dati: «La risposta alle sfide dei megadati: richiesta di trasparenza, controllo da parte degli utilizzatori, protezione dei dati fin dalla progettazione e responsabilità»* del 19.11.2015, in cui si legge: "Nel parere 3/2015, accompagnato da raccomandazioni per un testo integrale della proposta di regolamento, abbiamo precisato che gli attuali principi di protezione dei dati, compresi la necessità, la proporzionalità, la minimizzazione dei dati, la limitazione delle finalità e la trasparenza, devono rimanere i principi chiave. Essi forniscono la linea di base necessaria per proteggere i nostri diritti fondamentali in un mondo di megadati. Al contempo, questi principi devono essere rafforzati e applicati con maggiore efficacia e in modo più moderno, flessibile, creativo e innovativo. Devono altresì essere integrati da nuovi principi, come la responsabilità e la privacy dalla progettazione e per default. Maggiore trasparenza, ampi diritti di accesso e portabilità dei dati, ed efficaci meccanismi di accesso-recesso potrebbero fungere da requisiti per assicurare agli utilizzatori un maggiore controllo sui propri dati e contribuire altresì a mercati più efficienti per i dati personali, a vantaggio sia dei consumatori, sia delle aziende."

5.2 L'accountability come chiave di lettura della nuova privacy

Il principio è espresso in particolare all'articolo 24 ed è di fondamentale importanza nell'architettura teorica e pratica della nuova normativa perché prevede che il titolare, nella gestione della privacy dei trattamenti che vengono compiuti sotto la sua responsabilità, sia tenuto ad organizzare misure adeguate al fine di garantire la tutela dei dati e la loro sicurezza.

Si tratta di una disposizione apparentemente semplice ma in realtà portatrice di una rivoluzione nell' approccio a questa materia.

Infatti, la previgente Direttiva n. 95/46/CE e il d.lgs. 196/2003, aderendo ad una impostazione formalistica, avevano stabilito una serie di adempimenti che, se rispettati, assicuravano la conformità normativa[38].

Ebbene, una soluzione del genere si era rivelata, negli ultimi anni, del tutto insoddisfacente davanti a problematiche che si presentano sempre più fluide, in perenne mutamento e sfuggenti, come quelle che scaturiscono dal quotidiano confronto con la necessità di garantire la sicurezza dei dati[39].

Il diritto, per sua natura, non deve essere sfuggente nei suoi contenuti, anche se forse sarebbe meglio utilizzare il condizionale in questa frase, dal momento che è oramai esperienza comune constatare come, a causa del fenomeno della globalizzazione e della continua evoluzione delle conoscenze tecniche, in tutti gli ambiti del diritto si assista ad un rimodellamento continuo di normative un tempo giudicate statiche e pressoché immodificabili, che comportano anche una contaminazione di modelli e categorie giuridiche fra diversi ordinamenti.

---

[38] In base all'art. 34 del d.lgs. 196/2003, oggi abrogato adopera del d. lgs. 101/2018, era prevista, in caso di trattamento effettuato con strumenti elettronici, l'adozione di una serie di misure contenute nel Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Codice Privacy)

[39] A tal proposito merita di essere menzionato il documento del Comitato Economico e Sociale Europeo, *Parere del Comitato economico e sociale europeo in merito alla Proposta di regolamento del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (regolamento generale sulla protezione dei dati), COM(2012) 11 final – 2012/0011 (COD)*, Bruxelles, 23 maggio 2012, che al par. 3.6 esplicita: "Il CESE accoglie con favore l'orientamento generale della Commissione e riconosce che gli obiettivi della direttiva 95/46/CE consolidata rimangono attuali, anche se, dopo 17 anni, e con tutti i cambiamenti tecnologici e sociali intervenuti nell'ambiente digitale, una revisione profonda delle norme è ormai indispensabile"

Ad ogni buon conto, quel che è certo è che la rivoluzione portata dallo sviluppo delle tecnologie informatiche ha costretto il giurista a inseguire i continui aggiornamenti di tali tecnologie per cercare risposte alle problematiche sempre nuove che queste hanno posto; con ciò il diritto è stato spinto verso nuove soluzioni, in grado di privilegiarne la natura dinamica a discapito di quella statica.

Il principio di accountability altro non è che un'espressione di questa linea di sviluppo del diritto contemporaneo; non dispone "cosa fare" ma impone, in capo al titolare, quello che è di fatto un obbligo di risultato: garantire la conformità normativa del trattamento attraverso l'adozione di strumenti adeguati a tal fine.

A questo risultato, il titolare addiviene secondo due fondamentali vie: in primo luogo il ricorso ad ogni misura idonea a ridurre al minimo i rischi connessi al trattamento, anche in relazione alle caratteristiche intrinseche dello stesso. In secondo luogo e conseguentemente, attraverso la capacità di dimostrare di aver messo in campo tutti gli interventi disponibili per garantire la correttezza del trattamento e la sicurezza dei dati degli interessati[40].

Fondamentalmente, al titolare è lasciata libertà di manovra circa le modalità per realizzare questo obiettivo e pertanto, dal punto di vista degli adempimenti richiesti, il principio di accountability si contraddistingue per il fatto di essere un contenitore vuoto, il cui riempimento è lasciato alla competenza del titolare.

Certamente da un lato questo assicura la flessibilità e la dinamicità che occorrono per assicurare una *compliance* credibile ma dall'altra è forte il rischio di lasciare i titolari del trattamento senza punti di riferimento, con la difficoltà di comprendere tutte le implicazioni insite nel proprio ruolo.

Dimostrare di avere approntato tutte le misure idonee, infatti, appare come un criterio assai valutativo, soprattutto alla luce della tradizione giuridica italiana, che è legata a

[40] Cfr. Calzolaio S., Ferola L., Fiorillo V., Rossi E. A., Timiani M., *La responsabilità e la sicurezza del trattamento* in Califano L., Colapietro C. (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati nel Regolamento UE 2016/679*, in "Università degli Studi Roma Tre - Collana CRISPEL - Sezione di diritto pubblico italiano ed europeo – Collettanee",, Editoriale scientifica, Napoli, 2017, in particolare il paragrafo 4, pp. 162 – 170, cui si rimanda per un confronto, è stato scritto da Timiani M.

criteri prescrittivi ben più definiti, ma allo stesso tempo si ha motivo di credere che, se correttamente interpretato, il principio di accountability potrà effettivamente fare da perno per quel cambiamento di mentalità che è così fondamentale per garantire la tutela della privacy di fronte alle insidie della criminalità organizzata e al dilagare delle pratiche scorrette.

Una prima soluzione per rispondere alle richieste di chiarezza da parte degli operatori potrebbe essere l'adozione di una serie di atti di *soft law*, quali linee guida del Garante Privacy, dell'European Data Protection Board, del Garante Europeo per la Protezione dei Dati, ecc..., in modo da creare appigli, *de facto* vincolanti, sui quali innestare una giurisprudenza di riferimento.

Una soluzione del genere però è da sconsigliarsi perché, operando in tal modo, ci si ritroverebbe di nuovo al punto di partenza, avendo da fare i conti con una serie di prescrizioni nemmeno più contenute in un testo di legge ma ricavabili da una pluralità di fonti, con la confusione che da ciò deriverebbe e con il rischio di tornare a un sistema statico e inutilmente complesso, che andrebbe ad attingere a una serie indefinita di fonti normative e giurisprudenziali.

Non solo, occorre considerare che su questa scia, è probabile che ogni paese giungerebbe a produrre delle proprie specifiche discipline e questo rischierebbe di vanificare la tensione all'uniformità degli ordinamenti europei in materia di privacy, che è invece condizione essenziale per la tutela dei dati non solo all'interno ma anche all'esterno dei confini dell'Unione Europea.

Non si vuole dire che non dovrebbero essere adottati documenti del tipo di quelli citati ma è importante che questi siano intesi come indicazioni e che non divengano, di fatto, dei vincoli cui ancorare l'attività di protezione dei dati.

Il regolamento sembra infatti indicare una diversa direzione, ossia un approccio incentrato sulla formazione e sulla diffusione di una cultura basata sul rispetto dei dati. Non si tratta più di affidare determinati compiti al personale addetto e fare riferimento a indicazioni prestabilite ma di generare, diffondere e condividere una *modus operandi* ispirato al continuo miglioramento che coinvolga tutti e che abbia al vertice la responsabilità del titolare del trattamento, il quale dovrà individuare gli strumenti più

adatti ad assicurare il rispetto delle disposizioni normative in relazione alle caratteristiche peculiari della struttura in cui opera e della tipologia di trattamento in questione, secondo un approccio *case by case*.

La condizione imprescindibile perché ciò avvenga è che sia presa seriamente in considerazione la necessità di acquisire competenze specifiche.

A ben vedere, infatti, in un settore così particolare e delicato, fare ricorso al principio di accountability è forse l'unica strada percorribile per raggiungere una sicurezza adeguata, tuttavia perché da esso possano veramente discendere pratiche virtuose occorre prestare la massima attenzione all'aspetto della formazione.

Non si può risolvere la cosa con leggerezza; occorre che siano presenti, all'interno della struttura che tratta i dati, quelle competenze capaci di portare uno sguardo critico e allo stesso tempo costruttivo alla gestione degli adempimenti legati alla privacy.

È seguendo questo ragionamento che si arriva alla figura del Data Protection Officer, che si avrà modo di analizzare nel prossimo capitolo e che ha proprio il compito di fornire l'apporto di sapere specializzato che è necessario affinchè l'ingranaggio pensato dal legislatore europeo possa girare fluidamente.

Ben può dirsi che il D.P.O. sia un risvolto concreto, forse il più evidente ed importante, del principio di accountability.

CAPITOLO II

LA FIGURA DEL D.P.O. NEL *"GENERAL DATA PROTECTION REGULATION"*[41]

1. Il D.P.O: i riferimenti normativi e i documenti delle istituzioni - 2. Chi deve dotarsi di un D.P.O.? - 2.1. Il Data Protection Officer negli uffici pubblici - 2.2. Il Data Protection Officer per i trattamenti che richiedono il "monitoraggio regolare e sistematico su larga scala" - 2.3. Il Data Protection Officer nei trattamenti su larga scala di particolari categorie di dati - 3. Cosa si intende per "trattamento di dati su larga scala"? - 4. Competenze e caratteristiche del D.P.O. - 5. La nomina del D.P.O. - 6. La posizione del D.P.O: all'interno della struttura - 6.1 Indipendenza - 6.2. Disponibilità delle risorse - 6.3. Conflitto di interessi – 6.4. Raggiungibilità - 6.5. Responsabilità del D.P.O: aspetti generali.

1. Il D.P.O: i riferimenti normativi e i documenti delle istituzioni

Nell'analizzare i contenuti del nuovo Regolamento Europeo n. 679/2016, una delle novità più rilevanti che emergono, soprattutto se raffrontata alla previgente disciplina, riguarda la figura del *Data Protection Officer* (il *Responsabile per la Protezione dei Dati*).

Si tratta infatti di una figura che non era presente nel precedente apparato normativo, le cui caratteristiche vengono descritte alla sezione IV del regolamento, agli Artt. 37, 38, e 39.

Sulla base di tali disposizioni normative, si apprende che un D.P.O. deve essere nominato *in primis* in tutte le pubbliche amministrazioni, con l'eccezione dell'autorità

[41] Il presente capitolo riproduce gran parte del contributo dell'autore (cap. I: *La figura del DPO nel regolamento europeo n. 2016/679*) all'opera "*Il Data Protection Officer. Il responsabile della protezione dei dati dopo il D.Lgs. 10 agosto 2018 n. 101*", a cura dello stesso autore, in "Le nuove leggi del diritto" (collana), Dike Giuridica Editrice, Roma, 2018, cui sono state apportate alcune modifiche e aggiornamenti per integrarlo con la presente tesi.

giurisdizionale[42], in secondo luogo in tutti i casi in cui i trattamenti richiedano il monitoraggio regolare e sistematico su larga scala degli interessati e infine nelle ipotesi in cui vengano trattate le particolari categorie di dati ex articolo 9 e 10.

Nell'architettura delineata dal regolamento si stabilisce inoltre che la posizione del Data Protection Officer debba godere di particolari tutele volte a garantirgli la possibilità di svolgere in maniera autonoma e completa le proprie funzioni, che si andranno fra breve ad analizzare.

Oltre a veder riconosciuta la propria indipendenza, il Data Protection Officer ha diritto ad essere coinvolto nella gestione di tutte le problematiche inerenti alla privacy e a poter usufruire di risorse adeguate per realizzare i compiti che il regolamento gli affida, esplicitati nel dispositivo dell'art. 39 del regolamento (UE) n. 679/2016 e consistenti principalmente nel fornire consulenza al titolare o al responsabile in merito agli obblighi normativi, previsti sia dal regolamento che ogni altra legislazione inerente alla privacy, sorvegliare sull'effettiva applicazione della normativa sui dati personali all'interno della struttura in cui opera, esprimersi in merito alla valutazione di impatto sulla protezione dei dati, interfacciarsi con l'autorità di controllo in determinate occasioni, come nelle ipotesi di violazioni di dati (*Data breach*)[43].

Di fatto, si tratta di una figura che si integra con le altre già previste dalla pregressa normativa, ossia il Titolare del trattamento e il Responsabile del trattamento.

Tuttavia, nelle intenzioni del legislatore europeo, il Data Protection Officer si pone come un soggetto quasi *super partes* rispetto agli altri attori che nell'azienda o nella struttura pubblica si occupano di tutelare i dati e questo avviene proprio grazie a una serie di prerogative che il regolamento intende assicurargli.

Concretamente parlando, il Data Protection Officer si traduce in una sorta di controllore interno, chiamato a valorizzare e dare attuazione a quel principio di *accountability* che è

[42] Va pur detto che il legislatore italiano, intervenuto con il d.lgs. n. 101 del 10 agosto 2018, ha previsto la nomina del Data Protection Officer anche per l'autorità giudiziaria; sul punto si spenderanno maggiori considerazioni nel capitolo V di questa tesi.

[43] Cfr. art. 39, par. 1, Regolamento (UE) 2016/679.

così importante e decisivo nell'economia globale della gestione della privacy a seguito del Regolamento (UE) 2016/679.

Come accade spesso davanti a una novità legislativa, vi è ancora incertezza su quali siano effettivamente i confini di azione e le caratteristiche della nuova figura.

Sotto questo profilo, un aiuto fondamentale in viene dal raffronto con il Considerando 97, che parla di un soggetto che deve avere una "conoscenza specialistica" ed essere in grado di affiancare l'attività del titolare del trattamento, riuscendo in tal modo a sorvegliare il corretto svolgimento delle procedure inerenti alla privacy nella struttura in cui opera[44].

Le indicazioni fornite dal testo del regolamento, tuttavia, non si sono rivelate sufficienti a dissipare i dubbi relativi ad una compiuta definizione del D.P.O. e quindi, vista anche la grande attesa che si è venuta a creare sin da subito intorno a questa figura, il 13 dicembre 2016 il Gruppo di lavoro articolo 29 ha emanato delle Linee Guida[45] specificamente dedicate, comprensive anche di una serie di F.A.Q. per aiutare gli operatori del settore a orientarsi e recepire correttamente la nuova disciplina.

Su quella base il Garante per la protezione dei dati personali ha adottato un ulteriore documento utile, costituito dalle *Nuove Faq sul Responsabile della Protezione dei Dati (RPD)*

---

[44] Vale la pena riportare per intero il testo del Considerando 97 del Regolamento (UE) n. 2016/679: "Per i trattamenti effettuati da un'autorità pubblica, eccettuate le autorità giurisdizionali o autorità giudiziarie indipendenti quando esercitano le loro funzioni giurisdizionali, o per i trattamenti effettuati nel settore privato da un titolare del trattamento le cui attività principali consistono in trattamenti che richiedono un monitoraggio regolare e sistematico degli interessati su larga scala, o ove le attività principali del titolare del trattamento o del responsabile del trattamento consistano nel trattamento su larga scala di categorie particolari di dati personali e di dati relativi alle condanne penali e ai reati, il titolare del trattamento o il responsabile del trattamento dovrebbe essere assistito da una persona che abbia una conoscenza specialistica della normativa e delle pratiche in materia di protezione dei dati nel controllo del rispetto a livello interno del presente regolamento. Nel settore privato le attività principali del titolare del trattamento riguardano le sue attività primarie ed esulano dal trattamento dei dati personali come attività accessoria. Il livello necessario di conoscenza specialistica dovrebbe essere determinato in particolare in base ai trattamenti di dati effettuati e alla protezione richiesta per i dati personali trattati dal titolare del trattamento o dal responsabile del trattamento. Tali responsabili della protezione dei dati, dipendenti o meno del titolare del trattamento, dovrebbero poter adempiere alle funzioni e ai compiti loro incombenti in maniera indipendente".

[45] Gruppo di lavoro Articolo 29 per la protezione dei dati, *Linee guida sui responsabili della protezione dei dati adottate il 13 dicembre 2016*, emendate in data 5 aprile 2017.

in ambito privato; il Garante inoltre interviene continuamente sul punto al fine di chiarire dubbi interpretativi e applicativi di questa figura come di altre innovazioni apportate dal regolamento.

2. Chi deve dotarsi di un D.P.O.?

Con riferimento al quesito riguardante quali soggetti debbano di un Data Protection Officer, occorre rifarsi a quanto stabilito dall'articolo 37 del G.D.P.R.

Sulla base di quanto vi si legge, infatti, vi sono fondamentalmente tre circostanze particolari nelle quali è necessaria la nomina del D.P.O. anche se, è bene sottolinearlo sin d'ora, può rivelarsi senz'altro opportuno provvedere alla nomina di questa figura anche al di fuori di quei casi in cui ciò sia considerato strettamente vincolante a livello normativo.

Questa è, d'altronde, l'opinione fatta propria anche dal Gruppo di lavoro articolo 29 il quale, nelle linee guida citate esplicita: *"Anche ove il regolamento non imponga in modo specifico la designazione di un RPD, può risultare utile procedere a tale designazione su base volontaria. Il Gruppo di lavoro "Articolo 29" (Gruppo di lavoro) incoraggia gli approcci di questo genere"*[46].

Ad ogni buon conto, si procede a illustrare i casi in è prevista l'obbligatorietà del D.P.O.

2.1. Il Data Protection Officer negli uffici pubblici

Una prima ipotesi in cui il D.P.O. è considerato necessario si ha, sulla base dell'art. 37, par. I, lett. a) del regolamento, allorquando: *"il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali"*.

Ebbene, è del tutto evidente come tale definizione non consenta di rintracciare criteri di identificazione univoca degli "organismi pubblici" e delle "autorità pubbliche".

[46] Gruppo Di Lavoro Articolo 29 per la protezione dei dati, *Linee guida sui responsabili della protezione dei dati,* op. cit., par. 1 (introduzione), p. 5.

La molteplicità e la eterogeneità dei soggetti astrattamente riconducibili alle citate categorie ed esercenti una pubblica funzione rende infatti difficile comprendere quali uffici possano essere classificati come tali.

Le linee guida del gruppo articolo 29 precisano solo che dovranno dotarsi di D.P.O. tutti i soggetti che esercitano pubblici poteri[47]; a tal proposito il gruppo dei garanti richiama le definizioni di "ente pubblico" e "organismo di diritto pubblico" fatte proprie dalla direttiva 2003/98/CE del Parlamento europeo e del Consiglio, del 17 novembre 2003, art. 2, par. 1 e 2[48].

Di conseguenza, diviene importante verificare come il diritto interno di ciascun paese dell'Unione sia in grado di circoscrivere l'ambito di applicabilità del regolamento riguardo a questo punto.

Su questa scia si è inserita quindi il Garante Privacy, che in data 15 Dicembre 2017 ha emanato delle F.A.Q. specificamente dedicate all'ambito pubblico, in virtù delle quali sono da ritenersi vincolati alla nomina di un D.P.O. i soggetti citati agli articoli 18 - 22 del D. lgs 196/2003[49].

2.2. Il Data Protection Officer per i trattamenti che richiedono il "monitoraggio regolare e sistematico su larga scala".

Altra situazione in cui la designazione di un D.P.O. è obbligatoria, ai sensi dell'art. 37, par. I, lett. b) del regolamento, è quella in cui *"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"*.

Anzitutto, non deve trarre in inganno l'espressione "attività principali", che potrebbe far intendere che il D.P.O. sia una figura necessaria nel solo caso in cui il trattamento dei dati sia la prestazione tipicamente svolta all'interno di una struttura.

---

[47] Gruppo di lavoro articolo 29, *Linee guida sui responsabili della protezione dei dati*, op.cit., par. 2.1.1, p. 8.
[48] Ibidem.
[49] Garante per la protezione dei dati personali, *Nuove Faq sul Responsabile della Protezione dei dati (RPD) in ambito pubblico*, par. 1.

Così in effetti non è; infatti il senso di tale definizione sta nel prevedere l'obbligatorietà della nomina del D.P.O. in tutti qui casi in cui il trattamento dei dati sia di fatto inscindibile dalla normale attività portata avanti dal titolare, configurandosi come *condicio sine qua non* per la liceità dei servizi resi[50].

Anche con riferimento all'espressione "monitoraggio regolare e sistematico degli interessi su larga scala", si deve constatare come non sia di immediata comprensione il significato di tale lemma.

Ancora una volta, quindi, è bene rifarsi alle Linee Guida del Gruppo di lavoro articolo 29.

Al punto 2.1.4. esse stabiliscono che con "regolare" si deve intendere quel tipo di trattamento che avvenga "in modo continuo", a "intervalli definiti per un arco di tempo definito", ovvero sia "ricorrente o ripetuto a intervalli costanti", ovvero avvenga "in modo costante o a intervalli periodici"[51].

Peraltro, sempre nello stesso paragrafo delle linee guida, si stabilisce che l'aggettivo "sistematico" debba intendersi riferito a quel trattamento che "avviene per sistema", che sia "predeterminato, organizzato o metodico" ovvero che si svolga "nell'ambito di un progetto complessivo di raccolta di dati" ovvero ancora che sia "svolto nell'ambito di una strategia"[52].

A tal proposito preme precisare a questo punto che le forme di tracciamento e profilazione online sono da considerarsi senz'altro fra quei trattamenti che comportano un monitoraggio regolare e sistematico dei dati, così da necessitare della nomina di un D.P.O.

Contrariamente a quanto si è soliti pensare, trattamenti del genere possono aversi anche senza l'utilizzo delle più moderne tecnologie e della rete internet[53].

---

[50] Cfr. Maglio M., *Il responsabile per la protezione dei dati personali* in Maglio M., Tilli N., Polini M. (a cura di), *Manuale di diritto alla protezione dei dati personali*, Maggioli Editore, Santarcangelo di Romagna, 2017, p. 157.

[51] I virgolettati sono ripresi da Gruppo di lavoro articolo 29, *Linee guida sui responsabili della protezione dei dati*, op. cit., p. 2.1.4.

[52] I virgolettati sono ripresi da: Ibidem; sugli aggettivi "sistematico" e "regolare" Cfr. Maglio M., *Il responsabile per la protezione dei dati personali*, in Maglio M., Tilli N., Polini M. (a cura di), op. cit. p. 158-159.

[53] Cfr. Ibidem.

2.3. Il Data Protection Officer nei trattamenti su larga scala di particolari categorie di dati

L'ultima ipotesi di obbligatorietà, prevista dall'art. 37, par. I, lett. c) del regolamento, riguarda *"le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10"*.

I dati in questione sono quelli idonei a rivelare "l'origine razziale o etnica di un soggetto, le sue opinioni politiche, convinzioni religiose, filosofiche o l'appartenenza sindacale"[54]. In questa fattispecie ci si riferisce anche a quei trattamenti che coinvolgano "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"[55]; inoltre l'art. 10 si preoccupa di sottolineare come il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza possa avvenire soltanto sotto il controllo della pubblica autorità.

3. Cosa si intende per "trattamento di dati su larga scala"?

Come visto, un fondamentale riferimento operato dall'articolo 37, lettere b) e c) per individuare quali tipologie di trattamento siano idonee a far sorgere l'obbligo di nomina di un D.P.O., è il requisito della "larga scala".

Esso costituisce un ulteriore, fondamentale, presupposto su cui si fonda l'obbligo di dotarsi di un D.P.O. e merita una particolare attenzione.

Anche la definizione di trattamento operato su "larga scala" tuttavia, di per sé considerato, risulta eccessivamente generico e soltanto operando un riferimento al considerando 91 si riesce a ricavare qualche maggiore informazione e a realizzare che sono tali quei trattamenti i quali *"mirano al trattamento di una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che potrebbero incidere su un vasto numero di interessati e che potenzialmente presentano un rischio elevato"*[56].

[54] art. 9, par .1, Regolamento (UE) 2016/679.
[55] Ibidem.
[56] Considerando 91, Regolamento (UE) 2016/679.

Lo stesso considerando esclude però che si debba parlare di trattamento su "larga scala" nel caso di dati raccolti e trattati da medici relativamente ai pazienti o di clienti da parte di avvocati, dando così a intendere che ad oggi, in linea generale, non si debba dare luogo alla nomina di un D.P.O. per l'attività dei professionisti[57], soprattutto in un contesto come quello italiano, nel quale gli studi professionali sono nella gran parte di dimensioni piccole o addirittura individuali.

Anche con riferimento a questo aspetto, è comunque bene riferirsi alle Linee Guida del Gruppo di lavoro articolo 29. Le diverse Autorità garanti degli stati membri dell'Unione Europea in tale documento hanno specificato quali aspetti debbano essere tenuti in considerazione per definire un trattamento su larga scala, indicando come criteri:

- "il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento;
- il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento;
- la durata, ovvero la persistenza, dell'attività di trattamento;
- la portata geografica dell'attività di trattamento"
- trattamento di dati (metadati, contenuti, ubicazione) da parte di fornitori di servizi telefonici o telematici" [58].

Per contro, non sono considerati di "larga scala", a titolo di esempio, i seguenti trattamenti:

- "trattamento di dati relativi a pazienti svolto da un singolo professionista sanitario;
- trattamento di dati personali relativi a condanne penali e reati svolto da un singolo avvocato"[59]

[57] Garante per la protezione dei dati personali, *Nuove Faq sul Responsabile della Protezione dei Dati (RPD) in ambito privato*, par. 4.

[58] Gruppo di lavoro articolo 29 per la protezione dei dati, *Linee guida sui responsabili della protezione dei dati*, op. cit., par. 5.3, p. 28, dove si trova anche un utile elenco delle attività che possono essere considerate quali "trattamenti su larga scala".

[59] Ibidem.

4. Competenze e caratteristiche del D.P.O.

In relaziona all'articolo 37, particolare attenzione deve essere prestata al quinto paragrafo, laddove si specifica che un D.P.O. dovrebbe possedere qualità professionali adatte al ruolo che è chiamato a svolgere.

Tali qualità professionali si sostanziano in una forte competenza sugli aspetti normativi, sulle prassi operative e nella capacità di assolvere i compiti descritti all'articolo 39[60].

Tali competenze dovrebbero essere parametrate alla difficoltà del trattamento richiesto, come si evince dal contenuto del Considerando n. 97.

Ancora una volta, si deve rilevare come l'utilizzo di siffatti parametri porti comunque a difficoltà interpretative per cui è bene rifarsi sia alle più volte citate linee guida del Gruppo di lavoro articolo 29, che a un chiarimento del Garante per la protezione dei dati personali del 28 luglio 2017, con cui l'autorità italiana ha fornito indicazioni più dettagliate in proposito[61].

---

[60] Così l'art. 39 del Regolamento (UE) 2016/679:
"Compiti del responsabile della protezione dei dati:
1. Il responsabile della protezione dei dati è incaricato almeno dei seguenti compiti:
a) 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 presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
b) sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione 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;
c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35;
d) cooperare con l'autorità di controllo;
e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.
2. Nell'eseguire i propri compiti il responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo".

[61] Garante per la Protezione dei Dati Personali, *Regolamento privacy: come scegliere il responsabile della protezione dei dati. Le prime indicazioni del garante: necessarie competenze specifiche non attestati formali*, rinvenibile sul sito istituzionale del Garante per la protezione dei dati personali, in newsletter n.432 del 15 settembre 2017, (https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/6826945#1).

Con riferimento alle prime, vi si ribadisce che sono di fondamentale importanza al riguardo la conoscenza da parte del D.P.O. "della normativa e delle prassi nazionali ed europee in materia di protezione dei dati", cui si deve aggiungere una formazione adeguata e continua. È importante altresì "la conoscenza dello specifico settore di attività e della struttura organizzativa del titolare del trattamento"[62]; viene inoltre sottolineata l'importanza delle qualità personali e professionali del D.P.O., che dovrebbero rispondere a criteri deontologici particolarmente elevati, dal momento che sarà proprio costui ad occuparsi della promozione di una nuova sensibilità diffusa in materia di privacy, da realizzarsi sia attraverso l'osservanza della normativa che attraverso azioni che portino a una maggiore consapevolezza da parte dei vertici, dei dipendenti e financo degli utenti dell'azienda o organismo pubblico in cui egli opera.[63].

Con riferimento invece al citato documento del 28 Luglio 2017 del Garante per la protezione dei dati personali, ivi sono presenti alcune importanti precisazioni. Si legge infatti:

> "nella selezione sarà poi opportuno privilegiare soggetti che possano dimostrare qualità professionali adeguate alla complessità del compito da svolgere, magari documentando le esperienze fatte, la partecipazione a master e corsi di studio/professionali (in particolare se risulta documentato il livello raggiunto). Gli esperti individuati dalle aziende ospedaliere, ad esempio, in considerazione della delicatezza dei trattamenti di dati effettuati (come quelli sulla salute o quelli genetici) dovranno preferibilmente vantare una specifica esperienza al riguardo e assicurare un impegno pressoché esclusivo nella gestione di tali compiti.
> L´Autorità ha inoltre chiarito che la normativa attuale non prevede l´obbligo per i candidati di possedere attestati formali delle competenze professionali. Tali attestati, rilasciati anche all´esito di verifiche al termine di un ciclo di formazione, possono rappresentare un utile strumento per valutare il possesso di un livello adeguato di conoscenza della disciplina ma, tuttavia, non equivalgono a una "abilitazione" allo svolgimento del ruolo del RPD. La normativa attuale, tra l´altro, non prevede

[62] Gruppo di lavoro articolo 29 per la protezione dei dati, *Linee guida sui responsabili della protezione dei dati*, op. cit., par. 2.5, p. 15.
[63] Ibidem.

> l´istituzione di un albo dei "Responsabili della protezione dei dati" che possa attestare i requisiti e le caratteristiche di conoscenza, abilità e competenza di chi vi è iscritto.
> Enti pubblici e società private dovranno quindi comunque procedere alla selezione del RPD, valutando autonomamente il possesso dei requisiti necessari per svolgere i compiti da assegnati." [64]

Quanto riportato nulla toglie, naturalmente, al fatto che la frequenza di corsi e Master, pur non formalmente necessaria allo stato attuale, sia fatto un elemento indispensabile e funzionale all'acquisizione di quella competenza richiesta al D.P.O.

Certamente, infatti, avventurarsi nello svolgimento di questo ruolo senza aver assimilato la necessaria preparazione teorica è decisamente sconsigliabile, visti gli alti profili di responsabilità e i potenziali rischi dell'attività in quesitone.

È tuttavia opportuno sapere che non è prevista una vera e propria procedura abilitativa[65] né il possesso di determinati titoli o certificazioni, come peraltro recentemente ribadito dalla sentenza n. 287 del 13 settembre 2018 del TAR Friuli Venezia Giulia[66], per cui ad oggi è prioritario che coloro che si candidano a svolgere questo compito abbiano un'esperienza consistente delle delicate problematiche professionali in cui rischiano di imbattersi.

In sintesi, quindi, tanto il Gruppo di lavoro articolo 29 che il Garante per la protezione dei dati personali hanno sottolineato l'importanza di una preparazione solida sulla normativa nazionale ed europea, oltre a un'esperienza consolidata nell'ambito del trattamento dei dati personali e questi al momento sono i termini di riferimento nel momento in cui si deve effettuare la scelta del D.P.O.

Ad ogni buon conto, una volta selezionato il D.P.O., il titolare o il responsabile del trattamento hanno l'obbligo di pubblicare i suoi dati di contatto e di comunicarli alle

---

[64] Garante per la protezione dei dati personali, *Regolamento privacy, come scegliere il responsabile della protezione dei dati*, 28.07.2018 in Newsletter n. 432 del 15 settembre 2017, reperibile sul sito istituzionale "www.garanteprivacy.it"; nei documenti dell'autorità italiana si usano gli acronimi RPD e RGDP in luogo di DPO e GDPR, versioni inglesi che in questa tesi vengono invece preferite.

[65] Comellini S., *Il Responsabile per la protezione dei Dati (Data Protection Officer-DPO)*, Maggioli Editore, Santarcangelo di Romagna, 2018, cap. 7, par. 5, p. 31.

[66] La sentenza in questione ha annullato un concorso per l'accesso al ruolo di D.P.O. di un ente pubblico, nel quale era previsto che i candidati fossero in possesso della certificazione Auditor/Lead Auditor ISO/IEC/27001.

Autorità di controllo giacchè, in base alle disposizioni del regolamento, tale figura funge da punto di contatto da una parte con gli interessati e dall'altra con le autorità pubbliche. Qualora poi il D.P.O. operi all'interno di una pubblica amministrazione e debba essere scelto fra i dipendenti i di quest'ultima (il D.P.O. infatti può essere interno o esterno alla struttura, Cfr. par. 5 successivo), i requisiti di indipendenza e di esperienza previsti dalla normativa fanno pensare che esso debba essere designato a livello dirigenziale fra figure dotate di alta professionalità[67]; solo così infatti si scongiurerebbe il rischio di una subalternità alle decisioni dei superiori gerarchici.

Questo rilievo consente anche di ribadire che il *Data Protection Officer* non ha un ruolo meramente passivo; non si limita infatti a verificare la correttezza delle procedure inerenti alla gestione dei dati personali all'interno della struttura in cui opera.

Al contrario, egli ha anche un ruolo proattivo sia nei confronti di titolare e responsabile del trattamento, sia nei confronti dell'intera realtà in cui opera., essendo suo compito sensibilizzare utenti e lavoratori per favorire lo sviluppo di buone pratiche e di comportamenti corretti in materia di privacy.

Questo rilievo è particolarmente significativo perché rappresenta il *quid pluris* che caratterizza il D.P.O. rispetto alle preesistenti figure e consente di apprezzare la logica di fondo che permea il nuovo regolamento, che ha senza dubbio il merito di voler favorire lo sviluppo di una cultura diffusa sulla tutela dei dati.

In quest'ottica i D.P.O. sono coloro che non sono solo chiamati a implementare gli aspetti tecnici e normativi del trattamento dei dati ma anche a sviluppare una vera e propria etica in questo settore, che coinvolga professionisti e semplici utenti.

5. La nomina del D.P.O.

L'articolo 37 del regolamento europeo lascia libertà sulla decisione relativa alla nomina di un D.P.O. interno o esterno alla struttura.

[67] Garante per la Protezione dei dati personali, *Nuove Faq sul Responsabile della Protezione dei dati (RPD) in ambito pubblico*, par. 2.

Egli potrà quindi essere un dipendente chiamato a svolgere questa specifica funzione insieme alle sue altre mansioni, in alternativa, potrebbe essere chiamato all'uopo un soggetto esterno.

Non vi è una preferenza del regolamento in tal senso anche se, ad avviso di chi scrive, la soluzione "interna" presenta, almeno astrattamente, maggiori profili di rischio.

Anzitutto, il dipendente che acquisisce questa mansione dovrebbe poter disporre di tempo e risorse necessarie per dedicarvisi ed andrebbe quindi sgravato, almeno in parte, degli altri compiti cui in precedenza era demandato.

In secondo luogo, occorrerebbe avere a disposizione una figura già formata in ambito privacy, caratteristica che molto difficilmente si può rinvenire in soggetti che abbiano svolto ruoli diversi e quindi acquisito competenze diverse; specie se si guarda al tessuto produttivo italiano, formato per la maggior parte da piccole e medie imprese con un numero ridotto di dipendenti.

Da ultimo, va pur detto che, nonostante tutte le prerogative di cui gode in virtù del regolamento poc'anzi descritte, il D.P.O. che sia già dipendente della struttura correrà sempre il rischio di venire influenzate dai propri superiori nelle sue scelte o di assecondare logiche aziendali che possono andare in conflitto con la privacy.

Per questo motivo appare preferibile rivolgersi a professionisti esterni per lo svolgimento di questa mansione.

Beninteso, ogni situazione va analizzata in concreto perché anche questa seconda scelta non è esente dagli stessi rischi pur se in via generale è lecito ritenere che avvalersi di professionisti comporti maggiori garanzie in termini di disponibilità di tempo, di aggiornamento professionale e di effettiva indipendenza.

Ad ogni buon conto, nulla vieta che possa essere nominata anche una persona giuridica[68].

Nella stipula del contratto le parti hanno una certa libertà di individuare ulteriori compiti e responsabilità in capo al D.P.O. ed è per questo che, una volta inserita

[68] Gruppo Di Lavoro Articolo 29 Per La Protezione Dei Dati, *Linee guida sui responsabili della protezione dei dati*, Adottate il 13 dicembre 2016 Versione emendata e adottata in data 5 aprile 2017, par. 2.5; sul punto Cfr. anche Comellini S., op. cit., cap. 8, pg. 33-35.

all'interno della struttura, sarebbe bene che questa figura possa mantenere un legame stabile con la stessa perché anche la conoscenza dei meccanismi interni, garantita da un'esperienza diretta e consolidata, è un elemento fondamentale per il corretto svolgimento del ruolo, purchè non si traduca, ovviamente, in subalternità rispetto a tali meccanismi.

6. La posizione del D.P.O: all'interno della struttura

L'articolo 38 del G.D.P.R. prevede che il D.P.O. debba essere sempre coinvolto in ogni questione che riguardi la protezione dei dati personali.

Ciò deve avvenire in qualsiasi momento della gestione dei dati ma risulta particolarmente importante assicurare la presenza e il contributo del Data Protection Officer nella fase di pianificazione perché è proprio in quel momento delicato che il suo apporto in termini di competenza specifica viene maggiormente in rilievo e può aiutare l'azienda o la pubblica amministrazione a evitare potenziali situazioni di rischio, facendo così salva la "prospettiva di un trattamento che fin dalla progettazione incorpora l'esigenza della protezione dei dati personali"[69].

In considerazione di quanto detto in precedenza, quindi, non si deve in alcun modo pensare che la partecipazione del D.P.O. ai processi decisionali sia puramente simbolica. Tutt'altro, in virtù del suo compito di sorvegliante della conformità normativa, egli dovrà presenziare attivamente alle riunioni, essere informato di qualsiasi decisione riguardi la protezione dei dati ed intervenire sistematicamente per favorire la risoluzione di eventuali problemi.

6.1. Indipendenza

Affinché il D.P.O. possa operare per il perseguimento degli obiettivi posti dal Regolamento, è previsto che egli debba godere di autonomia, che si concretizza nel fatto di non dover ricevere alcuna istruzione dall'esterno nell'esecuzione dei propri compiti.

[69] Calzolaio S., *Protezione dei dati personali*, in *Digesto delle Discipline Pubblicistiche - Aggiornamento* - diretto da Sacco R.; Bifulco R., Celotto A., Olivetti M. (a cura di), Utet Giuridica, Milano, 2017., p. 633.

Ciò non significa, beninteso, che egli non possa accogliere consigli e suggerimenti da parte del titolare o da altri soggetti all'interno della struttura, nell'ottica di una normale collaborazione tra diversi attori chiamati a gestire la protezione dei dati. Deve essere chiaro, però, che il D.P.O. non può e non deve in alcun modo essere sottoposto a un potere direttivo da parte di chicchessia. Nel caso in cui la figura designata sia un dipendente della struttura, così come nel caso che la stessa venga individuata in un soggetto esterno, deve comunque poter godere di indipendenza di giudizio nell'espletamento delle proprie mansioni, delineate dall'articolo 39[70].

Funzionale a tale indipendenza è la previsione secondo cui il D.P.O. non può essere rimosso né penalizzato dal titolare o dal responsabile del trattamento per le decisioni assunte nell'espletamento dei propri compiti[71].

Tale disposizione mira ovviamente a garantire la libertà di scelta del D.P.O., il quale non dovrà temere eventuali ritorsioni per quanto operato nell'ottica di proteggere i dati personali.

L'impossibilità di rimuovere o comunque di penalizzare il D.P.O. a motivo di decisioni da questi prese nell'esercizio delle proprie funzioni e nell'assolvimento dei propri compiti è funzionale alla finalità di mettere il D.P.O. al sicuro da eventuali condotte punitive del titolare o del responsabile del trattamento che non vedessero di buon occhio le decisioni da egli assunte.

Si tratta di una previsione di fondamentale importanza perché, in mancanza, questa nuova figura sarebbe facilmente influenzabile nelle proprie scelte, con la logica ed inevitabile conseguenza che non sarebbe in grado di svolgere quella funzione di garanzia e di diffusione di una cultura attenta alla privacy che invece il regolamento le affida.

Altro discorso riguarda invece le penalizzazioni o addirittura la rimozione che dipendono da altri fattori; in assenza di indicazioni sul punto, deve ritenersi che il D.P.O. non goda di alcun particolare regime di vantaggio.

---

[70] Cfr. Considerando 97 reg. UE 2016/679.

[71] Cfr. art. 38, par. 3, reg. UE 2016/679.

D’altronde, questo è del tutto comprensibile, poiché la *ratio* della particolare posizione in cui viene posto il D.P.O. sta nella necessità di evitare condizionamenti che incidano negativamente sulla qualità della protezione dei dati personali, ma non rende il D.P.O. estraneo ad altre dinamiche tipiche dei rapporti di lavoro; ad esempio, in caso di una crisi aziendale che porti alla necessità di ridurre il personale, nulla vieta che anche chi ricopre l’incarico di D.P.O. possa essere coinvolto negli esuberi per quanto, va pur detto, la delicatezza e la specificità del suo ruolo lo rendono probabilmente meno esposto rispetto ad altre figure.

Il punto è comunque delicato perché si pone il rischio di spiacevoli abusi o situazioni *borderline*, nelle quali dietro penalizzazioni o a rimozioni formalmente imputabili a circostanze lecite, potrebbe nascondersi un comportamento ritorsivo finalizzato a “punire” un D.P.O. che si sia mostrato troppo indipendente e non allineato ai *desiderata* dei vertici della struttura.

Tutto questo porta a considerare due importanti fattori.

Da una parte, sicuramente, sarà necessaria una forte azione di vigilanza per evitare distorsioni che vadano nel senso di una compressione dell'autonomia e della libertà del D.P.O. e che siano finalizzate ad ottenere una gestione della privacy più "spicciola" e meno scrupolosa.

D’altra parte, ciò consente di comprendere ancora di più quanto sia fondamentale scegliere un soggetto che abbia le qualità professionali necessarie per svolgere questo ruolo, sia in relazione alle competenze che alle capacità di interazione con le altre figure coinvolte nelle decisioni in materia di privacy. Infatti, una volta inserito all'interno dell'azienda o comunque legato ad essa da un contratto, l'eventuale sostituzione risulterà particolarmente complessa e potenzialmente foriera di contenziosi giurisdizionali dall'esito incerto.

6.2. Disponibilità delle risorse

Di fondamentale importanza, per il corretto assolvimento dei compiti assegnatigli, è che il D.P.O. abbia a disposizione le risorse necessarie per farvi fronte, così come espressamente previsto dall'articolo 38 del G.D.P.R.

Risorse, quindi, sia relativamente alle capacità di spesa, sia per quel che riguarda la fornitura di strumenti capaci di implementare la tutela dei dati personali e il controllo sui trattamenti effettuati in azienda.

Si ritiene poi che alla voce "risorse" debba essere ricondotta anche la garanzia di un supporto adeguato da parte di tutta la struttura aziendale, che deve collaborare attivamente con il D.P.O. comunicando ogni dato utile e recuperando le informazioni richieste, e che debba inoltre esservi adeguata diffusione delle informazioni che il D.P.O. intende far circolare all'interno dell'azienda o pubblica amministrazione in cui è inserito[72].

Egli, inoltre, sempre a norma dell'articolo 38, deve essere messo nella condizione di poter investire nel proprio aggiornamento professionale, così da poterlo mettere a servizio di tutta la struttura in cui è inserito.

D'altronde se è vero, come si è già avuto modo di sottolineare, che il regolamento europeo intende accordare al D.P.O. l'indipendenza e l'autonomia di giudizio, tale autonomia risulterebbe del tutto frustrata se egli non avesse facilità nell'accedere ai dati e ai documenti necessari per avere una visione d'insieme e una corretta consapevolezza dell'effettiva situazione relativa alla gestione della privacy all'interno della struttura, così come non potrebbe operare efficacemente se non gli fosse consentita la realizzazione degli accorgimenti atti a garantire la sicurezza dei dati tramite l'investimento in nuove soluzioni tecniche o, ancora, se gli fosse preclusa la possibilità di un costante aggiornamento, quantomai necessario in un ambito che risente in modo particolarmente significativo dell'influsso delle trasformazioni tecnologiche e che pertanto impone conoscenze sempre nuove per garantire l'adeguamento agli obiettivi posti dalla normativa[73].

[72] Cfr. Comellini S., op. cit., pg. 36-37.

[73] Cfr. Maglio M., *Il responsabile per la protezione dei dati* in Maglio M. Polini M., Tilli N. (a cura di) *Manuale di diritto alla protezione dei dati personali*, op. cit., 2017.

6.3. Conflitto di interessi

Sempre nell'ottica appena descritta si inquadra quanto stabilito dall'articolo 38, par. 6, che stabilisce che il D.P.O. possa svolgere altre attività all'interno dell'azienda o pubblica struttura in cui opera, a condizione però che tali ulteriori compiti non si traducano in un conflitto di interessi rispetto alla sua funzione.

Per questo motivo è chiaro che il D.P.O. non potrà svolgere i compiti di titolare o responsabile del trattamento ma nemmeno altre funzioni le cui caratteristiche intrinseche possano confliggere con le attribuzioni sue proprie [74].

Le ipotesi sono diverse e coinvolgono sia quei ruoli cui viene affidato il potere di spesa, sia quelli a cui viene affidato il potere di gestione e direzione di un'azienda o pubblica amministrazione e che in qualche modo influiscono sulle politiche in materia di trattamento dei dati.

Non vi è un elenco tassativo aprioristicamente determinato e d'altronde è perfettamente normale che sia così, perché le situazioni possono essere talmente variegate da non poter prescindere da un'analisi in concreto in base alla quale operare una valutazione di merito sulla sussistenza o meno di un conflitto di interessi.

Ad ogni buon conto, le linee guida già più volte citate al punto 3.5 forniscono utili indicazioni in tal senso, insieme a una serie di criteri utili per individuare e prevenire le situazioni potenzialmente rischiose[75].

Va da sé che gli ulteriori e diversi compiti assegnatigli devono lasciare al Data Protection Officer tempo sufficiente per occuparsi delle mansioni tipiche del suo ruolo e anche da questo punto di vista occorrerà vigilare per evitare abusi.

6.4. Raggiungibilità

Come detto in precedenza, Il D.P.O. è una figura che funge da snodo, da una parte nei confronti della struttura in cui opera, all'interno della quale deve sorvegliare sulla

---

[74] Cfr. Garante per la protezione dei dati personali, *Nuove Faq sul Responsabile della Protezione dei dati (RPD) in ambito pubblico,* par. 7, p. 4.

[75] Cfr. Gruppo Di Lavoro Articolo 29 Per La Protezione Dei Dati, *Linee guida sui responsabili della protezione dei dati*, op. cit. , par. 3.5. pp. 20-21.

corretta applicazione del regolamento e sovraintendere allo sviluppo di una cultura di maggiore attenzione alla privacy, dall'altra parte confronti delle autorità, in particolare dell'Autorità garante per la protezione dei dati personali.

Ben si comprende allora non solo l'obbligo della pubblicazione dei dati di contatto, ma anche la previsione dell'articolo 37, par. 2, che vuole che il D.P.O. sia "facilmente raggiungibile da ciascun stabilimento".

Non sorprende questa previsione perché nel caso si debbano prendere decisioni rilevanti per la tutela dei dati, egli dovrebbe essere informato e dovrebbe parteciparvi.

Questa disposizione è poi particolarmente rilevante in ambito pubblico, laddove l'articolo 37, par. 3 prevede la possibilità di designare un unico D.P.O. per più di una pubblica amministrazione, se le dimensioni struttura organizzativa consentono questa possibilità.

6.5. Responsabilità del D.P.O: aspetti generali.

Per quanto concerne il regime di responsabilità del D.P.O., occorre sgombrare il campo da un possibile equivoco.

Il ruolo del D.P.O. è intrinsecamente separato e distinto da quello del titolare del trattamento, sul quale ricade la responsabilità ultima per il trattamento dei dati personali e per la conformità di tale trattamento a quanto previsto dal regolamento europeo incombe in ogni caso in capo al titolare del trattamento, come ricordano anche le linee guida del gruppo dei garanti europei[76].

Ciò detto, il titolare ha l'obbligo di coinvolgere il D.P.O. su tutte le questioni che riguardano la privacy all'interno della struttura e a collaborare con lui interpellandolo in proposito.

Il titolare del trattamento non è tenuto ad adottare tutte le soluzioni proposte dal D.P.O. e rimane libero di scegliere soluzioni diverse da quelle propostegli ma naturalmente dovrà assumersene la responsabilità e, in determinate circostanze, dovrà dare conto delle ragioni sulle quali si fonda la propria posizione[77].

---

[76] Cfr. Gruppo di Lavoro articolo 29, *Linee guida sui responsabili della protezione dei dati*, op. cit., p. 22.
[77] Ivi, par. 4.2, p. 23.

Ciò non esime il D.P.O. da qualsiasi profilo di responsabilità, giacchè egli risulterà responsabile in relazione all'assolvimento dei propri compiti, indicati con l'atto con cui viene nominato e riferiti a quanto stabilito dall'articolo 39 del regolamento. Tali compiti si traducono nel "sorvegliare l'osservanza" del G.D.P.R. e delle altre norme in materia di privacy, secondo una formula sintetica ed efficace utilizzata dal Regolamento e ripresa anche dal Gruppo di lavoro articolo 29[78].

In buona sostanza, egli non si sostituisce alle tradizionali figure del titolare o del responsabile del trattamento; piuttosto si integra con essi e, per quanto concerne l'ambito delle sue funzioni, potrà eventualmente essere chiamato a rispondere di inadempienze relative ai compiti affidatigli, per assolvere ai quali abbia ricevuto tutti gli idonei strumenti e goduto di tutte le opportune garanzie da parte dalla struttura per la quale svolge il servizio.

Un fattore importante da considerare per leggere correttamente il quadro in cui si inserisce il discorso regime di responsabilità del D.P.O. riguarda la centralità che ha l'analisi del rischio nel regolamento europeo

Quando si parla di approccio basato sul rischio si fa riferimento a una mentalità che sta alla base del regolamento dati europeo in esame e che viene ivi espressa in più punti, che contribuiscono a delineare il principio di *accountability*.

Con riferimento al Data Protection Officer, ciò che più rileva è il secondo paragrafo dell'articolo 39 in base a quale egli deve considerare "debitamente i rischi inerenti al trattamento tenuto conto della natura e l'ambito di applicazione del contesto e delle finalità del medesimo"[79].

Fondamentalmente, questo comporta la previsione di un ordine di priorità che consenta di individuare e tenere costantemente monitorati i trattamenti in corso secondo un ordine che permetta di concentrare l'attenzione *in primis* su quelli più rischiosi e gradatamente su quelli più ordinari.

[78] Ivi, par. 5.11, p. 33.

[79] art. 39, par. 2 Regolamento (UE) 2016/679/

In questo modo, il D.P.O. sarà maggiormente in grado di fornire la sua consulenza in ordine a quali attività sia opportuno programmare per assicurare la *compliance* della struttura e di tutti i trattamenti che vi vengono posti in essere[80].

Si avrà modo nel prossimo capitolo di approfondire il rapporto fra il titolare, le altre figure previste dal regolamento e il D.P.O., nonché il tema della responsabilità penale di quest'ultimo. Quel che è certo sin d'ora però è che risulta decisivo il momento dell'accordo contrattuale in quanto, al di là delle disposizioni del regolamento, è in quella sede che possono essere previsti e definiti ulteriori compiti e quindi ulteriori responsabilità per il D.P.O.

[80] Maglio M., *Il responsabile per la protezione dei dati personali* in Maglio M., Tilli N., Polini M. (a cura di), *Manuale di diritto alla protezione dei dati personali*, op. cit., cap. 6.4, p. 169.

CAPITOLO III

LA RESPONSABILITÀ DEL D.P.O. PROFILI PENALISTICI

1. Le differenze fra D.P.O., titolare del trattamento e responsabile del trattamento - 1.1. Il quesito sulla responsabilità del D.P.O. - 2. L'ipotesi di una responsabilità ex art. 40 c.p. - 2.1. Le posizioni di garanzia - 2.1.1. Il D.P.O. e la posizione di garanzia - 3. L'ipotesi di una responsabilità per concorso nel reato - 3.1. La responsabilità concorsuale del D.P.O: spunti di riflessione. - 4. Data Protection Officer e R.S.P.P: un confronto utile - 5. Conclusioni

1. Le differenze fra D.P.O., titolare del trattamento e responsabile del trattamento.

L'architettura dei ruoli descritta dal Regolamento Europeo, pur ricalcando quanto in precedenza previsto dalla direttiva 95/46/CE e dal d. lgs 196/2003, comprende elementi di novità importanti.

Prima di entrare nel merito del quesito concernente l'eventuale sussistenza di una responsabilità penale in capo al D.P.O. è quindi opportuno rivedere la nuova architettura dei ruoli e delle figure chiamate a interessarsi della gestione dei trattamenti di dati.

Infatti, per quanto appaiano confermate le figure del titolare del trattamento e del responsabile del trattamento, già presenti nella previgente disciplina, il dato normativo risulta decisamente più complesso da interpretare di quanto possa apparire a prima vista.

È indubbio che non venga meno la centralità della figura del titolare del trattamento.

Su di lui infatti incombe la responsabilità di mettere in atto le "misure tecniche e organizzative adeguate" [81] , atte a garantire la regolarità del trattamento dei dati in ossequio al già citato principio di accountability.

[81] Regolamento UE 2016/679, art. 24, par. 1.

È sempre sul titolare, inoltre, che incombe l'obbligo di garantire l'osservanza pratica dei principi di *privacy by design* e *privacy by default*[82].

Qui già si incontra un'importante innovazione; infatti l'ampiezza e la delicatezza delle problematiche che si possono incontrare in questo settore e la volontà di presidiare tutti gli aspetti legati alla privacy hanno fatto sì che il legislatore europeo stabilisse, con l'art. 26, la possibilità di istituire una contitolarità nel trattamento dei dati.

Si tratta di una novità rilevante, non prevista nella precedente direttiva, che consente a più titolari di concordare "in modo trasparente" e "tramite un accordo interno" [83] i rispettivi ambiti di competenza e di responsabilità.

Di tale ripartizione degli oneri, deve essere messo al corrente anche l'interessato che, a prescindere da quanto stabilito fra i contitolari, può richiedere l'osservanza dei propri diritti solidalmente a ciascuno di essi, come espressamente si evince dal contenuto dall'articolo 82 del regolamento che prevede in capo a ciascun contitolare l'obbligo di risarcire integralmente i danni causati dalla violazione delle norme del regolamento[84].

Resta ferma la possibilità, per il titolare, di nominare un responsabile del trattamento.

Deve trattarsi di un soggetto che sia in grado di offrire idonee garanzie dal punto di vista professionale, tali da assicurare il soddisfacimento di tutti i requisiti previsti dal regolamento per il trattamento dei dati e la tutela dei diritti di coloro cui i dati si riferiscono[85].

L'incarico in questione deve essere necessariamente dato per iscritto, con contratto o altro atto giuridico valevole secondo il diritto dell'Unione o degli Stati membri[86] l'atto con il quale avviene la nomina deve inoltre prevedere espressamente almeno gli ambiti di competenza definiti al terzo paragrafo dell´art. 28[87].

---

[82] Cfr. Regolamento UE 2016/679, art. 25, par. 1.

[83] Entrambi i virgolettati si riferiscono all' art. 26, par. 1 del Regolamento UE 2016/679.

[84] Cfr. Cairo L., Roberto G. (a cura di), *Figure e ruoli (artt. 4; 24; 26-29; 37-39) Contitolare e ripartizione delle responsabilità (Artt. 4, 26, 82)*, in "In Pratica GDPR", Leggi D'Italia, Wolter Kluwer, 2018.

[85] Cfr. art. 28, par 1, Regolamento (UE) 2016/679.

[86] Cfr. art. 28, par. 3, Regolamento (UE) 2016/679.

[87] Il paragrafo terzo dell'art. 28 stabilisce che il responsabile debba agire in base alle istruzioni del titolare del trattamento, dovendo inoltre garantire riservatezza e sicurezza dei dati, utilizzare "misure tecniche e organizzative adeguate", assistere il titolare "nel garantire il rispetto degli obblighi, oltre ad assicurare la cancellazione o la restituzione dei dati personali una volta terminata la prestazione e a

Il soggetto chiamato a svolgere il compito di responsabile del trattamento, come già avveniva in precedenza, assume importanti responsabilità tant'è vero che se, nell'esercizio delle sue funzioni, egli non si attiene a quanto stabilito dal regolamento, ne risponde come fosse il titolare[88].

Costui, tuttavia, non potrà nominare ulteriori responsabili del trattamento *sua sponte* ma potrà eventualmente esservi autorizzato dal titolare del trattamento[89].

I soggetti così individuati, detti *sub-responsabili* del trattamento[90], hanno il compito di coadiuvare il responsabile nel verificare la correttezza di specifiche attività di trattamento, sempre in osservanza degli obblighi assunti dal responsabile nei confronti del titolare del trattamento; nel caso in cui dovessero verificarsi illeciti attribuibili alla condotta di un sub-titolare, sarà pur sempre il responsabile a risponderne.

---

fornire ogni altra informazione utile al titolare del trattamento. L'atto che sancisce la nomina deve prevedere almeno che il responsabile:
"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;
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 da 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.".

[88] Regolamento (UE) 2016/679, art. 28, par 10.

[89] Secondo l'art. 28, par. 2 del regolamento, il titolare può concedere un'autorizzazione specifica, in relazione ad una richiesta avanzata dal responsabile, o generale. In questa seconda ipotesi tuttavia, il responsabile deve comunque avvisare il titolare ogniqualvolta proceda alla nomina di un nuovo sub-responsabile, onde ottenerne l'approvazione. In ogni caso l'autorizzazione deve essere scritta.

[90] Regolamento (UE) 2016/679, art. 28, par. 4.

Si favorisce così lo sviluppo di una tutela a più livelli e, nelle intenzioni del legislatore europeo, più specializzata. Se infatti al titolare spetta il compito di sovraintendere la gestione di tutta la filiera del trattamento, il responsabile e i sub responsabili devono, in quel contesto, occuparsi di specifici settori del trattamento, permettendo così un controllo più capillare e attento.

Nulla dice invece il Regolamento per quanto concerne la figura dell'incaricato del trattamento, già disciplinata dall'art. 30 del d.lgs. 196/2003.

Ciò tuttavia non deve trarre in inganno in quanto, anche se tale figura non viene espressamente richiamata, da nessuna parte si ricava la volontà di abolirne l'adozione e anzi, nulla osta al fatto che possa essere comunque individuata.

A questa conclusione si addiviene soprattutto alla luce del disposto di cui all'art. 4 n. 10 del regolamento, che nel fornire la definizione di "terzo" così si esprime:

> "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile".

Se ne deduce che possano esservi, appunto, altre *persone autorizzate* al trattamento dei dati all'infuori del titolare e del responsabile.

L'incaricato, cui ai sensi dell'art. 29 del regolamento devono essere fornite le istruzioni su come lavorare sui dati ed eseguire i trattamenti, si connota come una figura "esecutiva", che non deve possedere particolari qualità professionali, o meglio a cui non vengono richieste un'esperienza e una preparazione teorica comparabili a quelle che dovrebbero avere il titolare e il responsabile, anche se naturalmente le sue capacità professionali devono essere idonee alle funzioni che deve andare a esercitare.

Così ricostruito il quadro relativo ai soggetti che entrano in gioco nel trattamento dei dati, parrebbe dedursi che nell'architettura delle competenze e delle responsabilità delineata dal regolamento i ruoli chiave siano rimasti gli stessi rispetto alla previgente legislazione e che, per l'effetto, i soggetti chiamati ad assumere responsabilità in caso di

mancata tutela dei dati siano, in buona sostanza, il titolare e, in presenza di determinate condizioni, il responsabile del trattamento[91].

1.1. Il quesito sulla responsabilità del D.P.O.

Il quesito che ci si pone a questo punto riguarda il posizionamento del Data Protection Officer all'interno del quadro appena descritto, non già sotto il profilo del ruolo e delle prerogative, di cui si è dato atto nel capitolo precedente, quanto dal punto di vista del regime delle responsabilità in cui egli si inserisce e in base al quale può essere chiamato a rispondere.

Va premesso che sul punto un ruolo fondamentale, specie per quanto attiene agli aspetti civilistici, ricade sull'atto con cui si incarica il D.P.O., che può disciplinare più dettagliatamente i compiti e le responsabilità del soggetto incaricato, nei limiti concessi all'autonomia contrattuale delle parti.

Ciò detto, poiché è comunque necessario fare riferimento a quanto disciplinato dal regolamento (UE) 2016/679, occorre sin d'ora dare atto che, secondo un'interpretazione assai diffusa fra gli osservatori, il Data Protection Officer svolgerebbe fondamentalmente un ruolo di tipo consulenziale negli interessi della struttura, senza però risultare gravato da responsabilità.

A sostegno di questa lettura giova il dato testuale del regolamento, che all'art. 24 ha posto in capo al titolare il compito di predisporre gli strumenti opportuni, dal punto di vista tecnico e organizzativo, per assicurare la conformità dei trattamenti alle disposizioni normative in ossequio al principio di accountability.

Su questo presupposto le già più volte richiamate Linee guida del Gruppo di lavoro articolo 29 sui responsabili della protezione dei dati, intervenendo a specificare il portato del compito di "sorvegliare l'osservanza" del regolamento hanno stabilito in modo chiaro che "Il controllo del rispetto del regolamento non significa che il RPD *(DPO, ndr)* sia personalmente responsabile in caso di inosservanza. (...) Il rispetto delle norme in

[91] Cfr. Patalano A. (a cura di), *Reg. (CE) 27-04-2016, n. 2016/679/UE, Articolo 29 - Trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento*, in "In Pratica GDPR", Leggi D'Italia, Wolter Kluwer, 2018, p. 4.

materia di protezione dei dati fa parte della responsabilità d'impresa del titolare del trattamento, non del RPD *(DPO, ndr)*"[92].

Agli occhi di molti interpreti questa disposizione, lapidaria, è tale da escludere, *sic et simpliciter* responsabilità in capo al Data Protection Officer.

Invero, si ritiene che una conclusione di questo tipo sia tutt'altro che pacifica e che, anzi, sia necessario andare ad approfondire i possibili titoli di responsabilità che potrebbero essere addebitati al D.P.O. per cercare di avere un quadro più esauriente di quale sia la situazione attuale e soprattutto di quali potrebbero essere gli sviluppi normativi e giurisprudenziali sul punto.

Pur nel rispetto di quanto affermato sulla necessità di armonizzare le discipline dei diversi ordinamenti nazionali degli Stati membri dell'Unione e quindi nella consapevolezza dell'importanza del lavoro svolto in passato dal Gruppo di lavoro articolo 29 e ora dall'European Data Protection Board a questo fine, è bene ricordare che le linee guida in questione non rappresentano strumenti giuridicamente vincolanti, pur assumendo senza dubbio un valore strategico ed interpretativo indubbio.

È del tutto lecito avanzare soluzioni diverse, specie nell'ambito del diritto penale, che fra i vari settori di un ordinamento giuridico è quello più ancorato alla cultura giuridica di un determinato paese come riconoscono gli stessi atti legislativi dell'Unione, tant'è vero che il regolamento non contiene disposizioni penali, lasciando agli stati membri ogni valutazione relativa alle modalità attraverso le quali apprestare questo tipo di tutela.

Ne discende che in presenza di situazioni tali, secondo i canoni di un ordinamento nazionale, tale da far valutare la sussistenza di una responsabilità penale, un documento di *soft law* come le citate linee guida potrebbe al più costituire una chiave di interpretazione che orienti il giudice ma non un certo un elemento che sia *tout court* ostativo al riconoscimento di una posizione penalmente rilevante.

Vieppiù, se bene si riflette, le citate linee guida si limitano a sottolineare che l'onere di una corrispondenza dell'organizzazione aziendale ai dettami del regolamento non

[92] Gruppo di lavoro Articolo 29, *Linee guida sui responsabili della protezione dei dati* adottate il 13 dicembre 2016, versione emendata e approvata in data 5 aprile 2017, p. 22.

ricade in capo al D.P.O. ma al titolare de trattamento, come si ricava in effetti dal tenore letterale del G.D.P.R., ma non afferma che il D.P.O. debba essere ritenuto irresponsabile per eventuali errori, omissioni, condotte illecite poste in essere nello svolgimento dei propri compiti.

In effetti una soluzione che opti per l'irresponsabilità tout court del D.P.O. appare del tutto inedita e illogica se si pensa che la sua introduzione rappresenta una delle novità più rilevanti del regolamento per gli operatori giuridici ed economici, che in questi anni hanno monitorato, e continuano a monitorare con grande attenzione, il progressivo definirsi di questa figura che fornisce consulenza, ha accesso a tutto ciò che riguarda la privacy all'interno della struttura in cui opera e comporta delle rilevanti implicazioni in termini di prerogative, formazione, posizione, ecc... oltre ad avere il compito di svolgere una funzione di supervisione generale e di contribuire alla diffusione capillare di una sensibilità che valorizzi la tutela dei dati, sia nei confronti della sua struttura che nei confronti degli interessati. È quindi del tutto logico chiedersi come debba essere considerata la sua posizione dal punto.

In effetti, pur risultando ad oggi difficile immaginare quale sarà lo sviluppo giurisprudenziale su questo tema, si ritiene che la centralità del D.P.O. nel quadro del regolamento europeo e le sue attribuzioni specifiche non consentano di risolvere sbrigativamente la questione, rendendo invece necessario svolgere degli approfondimenti per proporre delle ipotesi di risposta, anche prendendo come riferimento altre figure professionali in qualche modo similari.

2. L'ipotesi di una responsabilità ex art. 40 c.p.

Un primo profilo da analizzare riguarda la responsabilità ex articolo 40 c.p.

Come noto, la norma stabilisce testualmente:

> "nessuno può essere punito per un fatto preveduto dalla legge come reato, se l'evento dannoso o pericoloso, da cui dipende la esistenza del reato, non è conseguenza della sua azione od omissione.

> Non impedire un evento, che si ha l'obbligo giuridico di impedire, equivale a cagionarlo".

La semplice lettura dell'articolo in questione consente di apprezzare come sia centrale il ruolo attribuito al rapporto di causalità, che si rivela come elemento indispensabile affinché possa determinarsi la sussistenza di una condotta penalmente rilevante, ciò a maggior ragione se si considera che l'articolo 41 c.p. prevede che l'irrilevanza di eventuali concause ai fini dell'esclusione del rapporto di causalità, e quindi della punibilità della condotta, salvo che queste siano state da sole sufficienti a causare l'evento dannoso.

Il nesso di causalità delineato dall'articolo 40 ricorre sia in caso di azioni che in caso di omissioni da parte dell'agente[93].

Nel primo caso, il concetto di causalità si estrinseca nel manifestarsi di un evento dal punto di vista naturalistico; l'evento previsto e punito dalla norma dovrebbe cioè manifestarsi in un accadimento percepibile esteriormente come esito di una determinata condotta pur se da questa logicamente distinguibile.

Nel secondo caso, trattandosi di condotta di tipo omissivo, si dà luogo a un'altra lettura, attenta a verificare che sia arrecata offesa al bene giuridico al quale l'ordinamento intende offrire particolare protezione attraverso la disposizione penale, non essendo necessario che vi sia un effetto materialmente constatabile della condotta illecita.

Come è noto, i reati omissivi possono essere propri qualora la condotta incriminata, il semplice *non faceat quod debeatur*, integri *sic et simpliciter* un illecito penale ovvero impropri qualora, oltre alla condotta omissiva, sia necessario anche il ricorrere di un fatto esteriore.

In merito all'individuazione del nesso causale ex art. 40 c.p. sono state proposte diverse letture.

[93] Cfr. Cocca A., *La distinzione tra reati ad evento naturalistico e reati di mera condotta in funzione di disciplina*, in "Giurisprudenza Penale Web", 2017, 5, p. 7-8, (http://www.giurisprudenzapenale.com/wp-content/uploads/2017/05/cocca_gp_2017_5-1.pdf), ultima cons. 02.09.2018.

In primo luogo, va citata la teoria *condizionalistica*, secondo la quale si ha nesso eziologico qualora la condotta imputabile all'agente costituisca *condicio sine qua non* per la verificazione dell'evento.

Al riconoscimento della responsabilità si addiviene, in questo caso, in seguito a un accertamento condotto sulla base di leggi scientifiche[94] che porti a ritenere che, eliminando la causa in esame, la successione degli eventi sarebbe stata diversa e non si sarebbe realizzato il fatto previsto come reato.

Una seconda lettura fornita dalla dottrina e dalla giurisprudenza è la cd. *teoria della causalità adeguata* e fa leva sul criterio dell'*id quod plerumque accidit*; con tale impostazione si intende valorizzare non qualsiasi anello della catena di concause che hanno portato alla verificazione dell'evento illecito ma solo quelli che, secondo la comune esperienza e la probabilità statistica, portano effettivamente al risultato penalmente rilevante.

Un'ultima interpretazione di cui tenere nota è rappresentata dalla teoria della causalità umana, che amplia notevolmente la portata della punibilità dell'art. 40 c.p., andando a ricomprendere tutti quegli accadimenti che possono essere ricondotti alla capacità di controllo dell'uomo sulla realtà ed escludendo solo quei casi, invero assai rari, in cui l'agire umano è condizionato da accadimenti naturali del tutto imprevedibili[95].

2.1. Le posizioni di garanzia

Quanto detto è propedeutico all'approfondimento del tema delle *posizioni di garanzia,* istituto fondamentale del diritto penale contemporaneo e fondato sul concetto di "obbligo giuridico" di impedire un determinato evento, espresso dall'art. 40 c.p.

---

[94] Cfr., ex plurimis, Cassazione civile, sez. III, n. 24073 del 13 ottobre 2017, che afferma "In caso di mancata attuazione della condotta "dovuta" (come nel caso di specie in cui l'esame bioptico estemporaneo è prescritto dal protocollo operatorio chirurgico), la sussistenza della relazione eziologica non può che essere ipoteticamente dedotta alla stregua di un criterio di prevedibilità oggettiva (desumibile da regole statistiche o leggi scientifiche), verificando se il comportamento omesso poteva o meno ritenersi idoneo - in quanto causalmente efficiente - ad impedire l'evento dannoso, con la conseguenza che deve escludersi dalla serie causale l'omissione di quella condotta che non sarebbe riuscita in alcun modo ad evitare l'evento".

[95] La teoria è enunciata in: Antolisei F. *Il rapporto di causalità nel diritto penale,* G. Giappichelli, Torino, 1934, p. 190-192.

Sono quindi considerati in posizione di garanzia quei soggetti che devono attivarsi per far sì che determinate normative siano effettivamente osservate all'interno di una struttura e che alcune tipologie di eventi, considerati dannosi per la salvaguardia di diritti e beni giuridici tutelati dall'ordinamento, non abbiano a verificarsi.

Ne consegue, naturalmente, la messa a disposizione di tutti gli strumenti giuridici per agire in tal senso.

Plurime sono le situazioni in cui possono venirsi a instaurare delle posizioni di garanzia.

È in posizione di garanzia, ad esempio, il medico nei confronti del paziente, nella misura in cui è tenuto ad assicurare tutte le prestazioni idonee ad assicurarne la salute, non solo nella fase operatoria ma anche in quella diagnostica, preparatoria all'intervento e successiva allo stesso[96];

In virtù delle medesime ragioni, si trovano in posizione di garanzia anche gli infermieri che, essendo ormai formati e qualificati come "professionisti sanitari", presidiano con la loro competenza aspetti peculiari del percorso terapeutico, distinti da quelli del medico al quale hanno comunque l'obbligo di segnalare ogni anomalia ed emergenza di cui vengano a conoscenza nello svolgimento delle proprie mansioni[97].

Sempre valorizzando l'elemento della formazione ricevuta e dei ruoli effettivamente svolti, sono stati ritenuti titolari di una posizione di garanzia anche l'autista soccorritore[98], il medico soccorritore volontario[99] o figure di tutt'altro tipo come il parroco[100].

Occorre a questo punto interrogarsi su come venga identificata la sussistenza di una posizione di garanzia.

---

[96] Sul punto, *ex plurimis*, vale la pena segnalare la recente Cass., Sez IV, sent. n. 2354/2018, ud. del 21 dicembre 2017, che in relazione alla posizione di garanzia dei medici che lavorano in *equipe*, occorre verificare i compiti e le responsabilità dei singoli operatori sanitari che intervengono a tutela del medesimo bene giuridico.

[97] Cfr. Cass., Sez. IV, sent. n. 2541 del 21 gennaio 2016.

[98] Cfr. Cass., Sez. IV, sent. n. 14007 del 02 Aprile 2015.

[99] Cfr. Cass., Sez. IV, sent. n. 14142 del 08 aprile 2015.

[100] Cfr. Cass., Sez. IV, sent. n. 19029 del 20 aprile 2017, che pure ha annullato con rinvio la sentenza della Corte d'Appello di Roma che aveva riconosciuto un parroco responsabile della morte di un giovane avvenuta per la caduta di una porta da calcio all'interno della parrocchia, riconoscendo la Corte che occorreva la verifica dell'effettiva prova nel caso concreto della gestione della cosa.

Tre risultano essere le principali concezioni che vengono in rilievo a tale proposito.

La prima di esse, la *concezione formalistica*, ancora il riconoscimento di una posizione di garanzia alla presenza di un chiaro imperativo di legge o di una base contrattuale che indichi un determinato soggetto quale destinatario di un obbligo precisamente identificato[101].

La seconda concezione, detta invece *sostanzialistica*, richiede un'analisi della realtà dei rapporti sociali, onde verificare in quali di esse vengono a instaurarsi dei vincoli rilevanti per l'ordinamento perché posti a garanzia di situazioni giuridiche particolarmente sensibili.

La dottrina tuttavia tende a favorire la cd. *tesi mista* per la quale un soggetto è considerato responsabile penalmente nel caso abbia un obbligo giuridico di agire e i poteri per farlo[102]. Si cerca in questo modo di pervenire ad una sintesi fra l'elemento formale, identificabile con la previsione normativa, e l'elemento sostanziale, coincidente con il ruolo effettivamente svolto e dalle prerogative assicurate a un determinato soggetto.[103]

Orbene, ora che si sono ricostruiti i tratti fondamentali dell'istituto occorre chiedersi se si possano rintracciare gli elementi caratteristici della posizione di garanzia con riferimento alla figura del Data Protection Officer.

A tal proposito si ritiene che il perno della questione sia costituito dal concetto di "obbligo giuridico" enunciato dall'art. 40 c.p.

Sussiste, secondo il regolamento, un obbligo di questo tipo in capo al Data Protection Officer?

È bene ribadire ancora che per avere una risposta precisa occorrerà monitorare gli approdi giurisprudenziali e le eventuali novità normative sul punto ma, allo stesso tempo, è possibile articolare una riflessione sulla base degli elementi a disposizione.

---

[101] Cfr. Fiandaca G., Musco E., *Manuale di diritto penale, parte generale*, Zanichelli, Bologna, 2014, p. 640-642.

[102] Cfr. Ivi, p. 643-644.

[103] Cfr. Mantovani F., *L'obbligo di garanzia ricostruito alla luce dei principi di legalità, solidarietà, di libertà e di responsabilità personale* in "Rivista Italiana di Diritto e Procedura Penale", Fasc. II, 2001, p. 340 ss.

2.1.1. Il D.P.O. e la posizione di garanzia

Secondo una prima lettura, se si analizzano i dati testuali contenuti del regolamento, né al primo paragrafo né al secondo paragrafo dell'articolo 39 sarebbero esplicitati obblighi di impedire determinati eventi, quali ad esempio violazioni di dati personali, pratiche scorrette, reati commessi attraverso l'utilizzo di dati conservati presso la struttura, *et similia.*

In sé considerati non apparirebbero sufficienti al fine di incardinare una posizione di garanzia né i compiti di "informare e fornire consulenza" in merito agli obblighi previsti dal regolamento di cui all'art. 39, par. 1, lett. a), né quello di fornire a richiesta il parere sulla valutazione di impatto ex art. 39, par. 1 lett. c), così come non sarebbe indicativo a tal fine il compito di fungere da punto di contatto fra la propria struttura e l'Autorità garante in caso di consultazione preventiva ex art. 36.

Nell'ambito di tali funzioni, il soggetto che ricopre la carica di Data Protection Officer potrebbe certamente vedersi rimproverata un'eventuale mancanza di diligenza, prudenza o perizia, ma ciò non sarebbe sufficiente a far concludere per la sussistenza di una posizione di garanzia, stante la mancanza di poteri di gestione da una parte e di obblighi specifici dall'altra.

Più complessa risulta, in questa ricostruzione, l'interpretazione del disposto della lettera b) del primo paragrafo dell'art 39 in quanto la previsione del compito di "sorvegliare l'osservanza" sia del regolamento che delle altre normative nazionali ed europee in materia di tutela dei dati, potrebbe postulare la sussistenza di un obbligo giuridicamente rilevante di garantire il rispetto di tutte le normative in materia di privacy.

Invero, un'espressione di tal fatta è inedita nell'ordinamento italiano, sì che ben potrebbe darsi adito a interpretazioni differenti sull'effettivo contenuto prescrittivo della stessa.

Si potrebbe sostenere che l'ampiezza di questa previsione vada letta sistematicamente con il resto del regolamento, il quale in effetti non prevede un potere di intervento diretto sulla gestione dei trattamenti da parte del D.P.O.

Perciò, mancando sia obblighi legali univoci volti a impedire determinati eventi, sia strumenti operativi per intervenire direttamente anche solo su aspetti particolari della gestione dei trattamenti, le prerogative del Data Protection Officer si esaurirebbero

nell'esercizio di una *moral suasion* che non valicherebbe mai il confine dell'imputabilità al medesimo di un'eventuale mancata *compliance* al regolamento, giacchè tale responsabilità ricadrebbe solo ed esclusivamente in capo al titolare, come affermato anche dalle citate linee guida del Gruppo di lavoro articolo 29.

In quest'ottica, si dovrebbe ritenere che ipotizzare la sussistenza di una posizione di garanzia in capo al Data Protection Officer sia in contrasto non solo con il dato normativo ma anche con i principi fondamentali del diritto penale: tassatività, determinatezza, precisione e soprattutto con il principio di legalità.

Poiché quindi il regolamento non si esprimerebbe nel senso di accordare al D.P.O. obblighi specifici rispetto ai quali egli sia tenuto ad assicurare determinati risultati di *compliance* normativa, non sarebbe corretto pervenire al medesimo risultato a seguito di interpretazione giurisprudenziale perché questa sarebbe giocoforza *ultra legem* e per ciò solo inammissibile.

A ben vedere tuttavia, partendo da una diversa interpretazione dell'art 39, par. 1 lett. b), non è peregrino rileggere le disposizioni relative ai compiti del D.P.O. sotto altra luce, ritenendo che con tale locuzione si possa incardinare su di esso quantomeno la responsabilità di monitorare lo stato dei trattamenti svolti all'interno della struttura e, nel caso egli ravvisi irregolarità o anomalie, avvisare il titolare o il responsabile del trattamento.

Tale lettura consentirebbe senz'altro di dare un significato preciso e precettivo a questo compito di sorveglianza del Data Protection Officer, che altrimenti risulterebbe tanto "roboante" nella sua formulazione quanto privo di portati applicativi apprezzabili.

Inoltre, non va dimenticato che Il D.P.O., quando fornisce consulenze e pareri, deve considerare "debitamente"[104] i rischi connessi al trattamento, che è titolato ad intervenire in ogni aspetto che riguardi la privacy all'interno della struttura, avendo anche la funzione proattiva di incentivare l'adeguamento normativo all'interno della struttura in cui opera.

[104] art. 39, par.2, Regolamento (UE) 2016/679.

A ciò si sommano le rilevanti prerogative riconosciute dall'ordinamento al D.P.O. in termini di indipendenza, inamovibilità, disponibilità di risorse, ecc...

D'altronde, al Data Protection Officer viene garantita una formazione adeguata e si richiede per la sua nomina il possesso di requisiti professionali particolarmente qualificanti[105].

Si tratta di caratteristiche che connotano anche altre figure cui la giurisprudenza ha effettivamente ricondotto un obbligo di garanzia e anche in questo caso appare legittimo ritenere che ad un quadro giuridico così articolato debbano corrispondere oneri proporzionati.

La posizione di garanzia del D.P.O. si estrinsecherebbe da una parte nel sorvegliare che non siano compiuti illeciti o operazioni comunque rischiose per la sicurezza dei dati, segnalandole nel caso si dovessero verificare, e dall'altra nel garantire una completa e corretta informazione sugli aspetti legali e tecnici dei trattamenti compiuti all'interno della struttura, così che coloro che sono titolari di poteri di gestione effettiva possano prendere le proprie decisioni in un quadro di piena consapevolezza circa le prospettive e le problematiche insite in determinati trattamenti.

3. L'ipotesi di una responsabilità per concorso nel reato

Com'è noto, il codice penale italiano prevede la possibilità di imputare un reato a più soggetti che siano incorsi nella commissione dello stesso.

La norma di riferimento è l'articolo 110 c.p., il quale testualmente recita:

> "Quando più persone concorrono nel medesimo reato, ciascuna di esse soggiace alla pena per questo stabilita, salve le disposizioni degli articoli seguenti".

[105] Sul punto vale la pena richiamare Cass. Pen. , sez IV, Sent. n. 45862 del 14 settembre 2017 e Cass. Pen., sez. 45853 del 13 settembre 2017, che hanno riconosciuto la sussistenza di una posizione di garanzia in capo al coordinatore per la sicurezza sui luoghi di lavoro in quanto, pur non essendo i titolari dell'obbligo di garantire la sicurezza nei luoghi di lavoro, in virtù delle mansioni che la legge gli affida e delle caratteristiche professionali che devono possedere, sono posti a presidio della correttezza di determinati aspetti delle procedure di sicurezza.

La giurisprudenza e la dottrina hanno molto discusso al fine di identificare l'area di applicabilità di questa norma e il dibattito è tutt'altro che sopito con riferimento a una pluralità di situazioni che si presentano come *borderline.*

Dall'elaborazione teorico-giurisprudenziale sul tema si evincono alcuni elementi strutturali che connotano la fattispecie in esame sia dal punto di vista oggettivo che soggettivo.

Con riferimento al primo aspetto, vengono in rilievo la necessità di intervento da parte di una pluralità di agenti che contribuiscono al realizzarsi di una fattispecie tipica considerata penalmente illecita dall'ordinamento; sotto il profilo soggettivo invece vengono in rilievo la presenza di dolo o di colpa nelle condotte incriminate.

Orbene, è ovvio che nel caso di scuola che veda una banda di malviventi accordarsi per commettere una rapina dividendo a tal fine i compiti fra i suoi vari componenti, non vi siano dubbi sulla sussistenza di un concorso di persone nel reato ex articolo 110 c.p.

Tuttavia, le situazioni in cui la giurisprudenza si è imbattuta e quotidianamente continua a imbattersi sono spesso e volentieri ben più articolate e di difficile interpretazione, motivo per cui si sono venute a delineare diverse letture relative all'istituto del concorso di persone nel reato, che comportano ora l'ampliamento, ora la riduzione della portata punitiva della norma.

È quindi necessario cercare di comprendere se, nell'ambito delle possibili interpretazioni fornite dalla giurisprudenza, siano state in qualche modo accolti orientamenti che consentono di ricomprendere anche l'operato di un professionista come il Data Protection Officer e se il regolamento offra degli appigli normativi in tal senso.

Una prima interpretazione da prendere in considerazione, detta anche della "accessorietà", prevede che per ravvisarsi il coinvolgimento di un soggetto ex art. 110 c.p. in una fattispecie criminosa debbano necessariamente ravvisarsi nella sua condotta tutti gli elementi richiesti dalla norma incriminatrice[106].

[106] La tesi della accessorietà è stata declinata anche in versione "estrema", per cui non sarebbe sufficiente la realizzazione di tutti gli elementi tipici della fattispecie antigiuridica, dovendo esservi anche gli elementi della colpevolezza e della punibilità; Cfr. Piazza M. *Un recente arresto della cassazione in tema di molestia o disturbo alle persone: alcuni spunti di riflessione* in "Diritto Penale Contemporaneo" ,

Per converso, secondo altra teoria, detta della *fattispecie plurisoggettiva eventuale*, l'incontro fra le singole condotte coinvolte in un disegno criminoso e l'articolo 110 c.p. permetterebbe di realizzare una nuova autonoma fattispecie[107] nella quale gli elementi costitutivi dell'illecito penale vengono realizzati da più soggetti attraverso gli apporti dei singoli, eziologicamente connessi fra loro.

In base a questa teoria, anche nel caso gli apporti in questione siano *ex se* irrilevanti dal punto di vista penale, essi concorrono comunque insieme al raggiungimento di un risultato criminoso unitario.

Altra declinazione di questa soluzione è rappresentata dalla *teoria delle fattispecie plurisoggettive differenziate*, in ragione della quale l'art. 110. c.p., nel momento in cui si va a congiungere con le varie fattispecie penali di speciale, genera non una sola bensì una pluralità di "fattispecie plurisoggettive"[108] che, pur avendo una base comune, devono essere valutate singolarmente sotto il profilo dell'apporto materiale e morale al piano criminoso.

Sul punto occorre inoltre segnalare la differenza fra concorso materiale e concorso morale.

Il primo si ha nel momento in cui un soggetto compie azioni concretantesi nella realtà esteriore, che possono costituire elemento tipico di una fattispecie criminosa ovvero connotarsi come atipiche rispetto alle previsioni normative ma comunque fondamentali per la realizzazione del fatto di reato.

Il secondo non si estrinseca in un'azione materiale dell'agente che si concretizza nella realtà esteriore, bensì nell'opera di convincimento che, con qualsiasi mezzo, egli pone in essere nei confronti di altri soggetti affinchè siano questi a realizzare i fini illeciti che lo animano; sul punto vi sono diverse figure che vengono in rilievo quali l'istigatore, il mandante o il determinatore; alcune di queste figure sono anche al centro di fattispecie penali *ad hoc*.

19.04.2012, (https://www.penalecontemporaneo.it/d/1428-un-recente-arresto-della-cassazione-in-tema-di-molestia-o-disturbo-alle-persone-alcuni-spunti-di-ri#), ultima cons. 03.09.2018.

[107] Cfr. Fiandaca, G., Musco E., op. cit., p. 517.

[108] Cfr. Ibidem, p. 519.

L'analisi giurisprudenziale, nella valutazione di queste ipotesi, ha nel tempo mostrato un *favor*, in particolare con riferimento all'ipotesi del concorso materiale, per la teoria della cd. "prognosi postuma", la quale prevede un giudizio sull'attività svolta dall'agente effettuato in base a una valutazione *ex ante*, ossia con riferimento alla capacità di quella determinata condotta di favorire la realizzazione dell'evento criminoso in esame, al di là del fatto che poi tale evento si sia o meno verificato.

Su questa premessa, la giurisprudenza ha stabilito che, al fine di ricostruire una responsabilità penale in capo ad un determinato soggetto, occorre che vi sia un accertamento dell'effettiva influenza operata dai suoi comportamenti, sia dal punto di vista materiale che morale, rispetto alla realizzazione del fatto di reato.
In particolare è necessario verificare quale sia stato il rapporto di causalità senza del quale il reato non si sarebbe concretizzato, anche in caso di condotte atipiche[109].

All'esito di tale accertamento, nel contesto giurisprudenziale odierno l'attenzione viene posta in particolare sulla effettiva capacità della condotta in esame di agevolare la realizzazione del disegno criminale, cosa che può avvenire con qualsiasi modalità di condotta che sia idonea ad agevolare, anche indirettamente, la realizzazione di un fatto di reato, sia essa commissiva o omissiva, materiale o morale[110], come si evince anche da una recente pronuncia della Suprema Corte che statuisce:

---

[109] Cfr., ex plurimis, Cass. pen. Sez. I, 18 febbraio 2009, n. 10730, la quale peraltro si inserisce in un solco ampiamente confermato: Cfr. Cass. Pen, Sez. I, 19 febbraio 2015 n. 7643, Cass. Pen. Sez. Unite, 24 novembre 2003 n. 45276 cui si richiama anche Basile E., *Consiglio tecnico e responsabilità penale - Il concorso del professionista tramite azioni neutrali*, in "Itinerari di Diritto Penale (collana)", Giappichelli Editore, Torino, 2018, p. 38, nota n. 72.

[110] Cfr, ex plurimis, Corte di Cassazione, Sez. VI penale, n. 36125 del 13 maggio 2014. che al punto 3.1. così afferma: "La seconda doglianza è, del pari, infondata. Costituisce infatti ius receptum, nella giurisprudenza di questa Corte , che il ruolo concorsuale di un soggetto possa esplicarsi attraverso le condotte più varie . L'attività costitutiva del concorso può infatti essere rappresentata da qualsiasi comportamento che fornisca un apprezzabile contributo alla realizzazione dell'altrui proposito criminoso o che agevoli l'opera dei concorrenti ,in tutte o in alcune delle fasi di ideazione ,organizzazione ed esecuzione della condotta criminosa (istigazione o determinazione all'esecuzione del delitto; agevolazione alla sua preparazione o consumazione; mera adesione o autorizzazione o approvazione per rimuovere ogni ostacolo alla realizzazione di esso (Sez. U.30-10-2003,n 45276, Cass. pen 2004, 811; Cass Sez 1, 17-1-2008, n. 5631, Rv. 238648; Sez 1, 18-2-2009n.10730, Rv 242849) . Ne deriva che la distinzione tra connivenza non punibile e concorso nel reato risiede nel fatto che la prima postula che l'agente mantenga un comportamento meramente passivo, inidoneo ad apportare un contributo alla realizzazione del reato mentre, nel concorso, è richiesto un contributo partecipativo, morale o materiale, alla condotta criminosa altrui, caratterizzato, sotto il profilo psicologico,dalla coscienza e

> "Per la configurabilità del concorso di persone è necessario, dunque, che il concorrente abbia posto in essere un comportamento esteriore idoneo ad arrecare un contributo apprezzabile alla commissione del reato, mediante il rafforzamento del proposito criminoso o l'agevolazione dell'opera degli altri concorrenti e che il partecipe, per effetto della sua condotta, idonea a facilitarne l'esecuzione, abbia aumentato la possibilità della produzione del reato (Sez. 4, n. 4383 del 10/12/2013, dep. 2014, Merola, Rv. 258185; Sez. 6, n. 2297 del 13/11/2013, dep. 2014, Paladini, Rv. 258244)"[111]

Quanto affermato sino ad ora deve essere integrato dalla considerazione secondo la quale, affinché sia riconosciuta una responsabilità penale del concorrente nelle diverse sfumature testè citate, è necessario ravvisare in capo allo stesso la presenza di un elemento soggettivo costituito da dolo ovvero da colpa a seconda della tipologia di reato che viene in rilievo.

Tale elemento soggettivo non necessariamente deve essere il medesimo in tutti i soggetti coinvolti nel concorso, potendosi avere la possibilità delle cd. ipotesi di concorso misto, nelle quali alcuni agenti partecipano a titolo colposo ed altri a titolo doloso alla realizzazione di una offesa tipica.

3.1. La responsabilità concorsuale del D.P.O: spunti di riflessione.

Così riepilogati i termini del concorso di persone nel reato, è bene andare a raffrontare l'istituto con la figura del Data Protection Officer alla luce del Regolamento Europeo n. 679/2016.

Ebbene, anche in questo caso potrebbe apparire arduo, in prima battuta, ipotizzare una responsabilità per concorso nel reato in capo al D.P.O.

Infatti, ai sensi del più volte citato già citato articolo 39 del Regolamento (UE) 2016/679, i compiti assegnati a questa figura, pur di primaria importanza, non sfociano mai in un

volontà di arrecare un apporto concorsuale alla realizzazione dell'evento illecito (Cass. , Sez VI , 18-2-2010 n. 14606 , Rv. 247127). Dunque il concorso si realizza non soltanto con la partecipazione all'esecuzione materiale ma anche con qualsiasi condotta cosciente e volontaria,diretta a rafforzare l'altrui proposito criminoso (Cass. Sez.2, 28-2-2007, n. 8 16625, Giust. pen. 2007, Il, 622), anche solo assicurando al concorrente un maggiore senso di sicurezza e uno stimolo all'agire (Cass. Sez 1, 14-2-2006 n.15023, Rv. 234128)".

[111] Corte di Cassazione, Sez VI penale, n. 1986 del 06 dicembre 2017, punto 4.

effettivo potere di intervento diretto nel trattamento dei dati, risolvendosi invece nel fornire consulenze, informazioni e, quindi, nell'assistere il titolare e/o il responsabile del trattamento nelle loro funzioni.

Non è mai riconosciuta, in sintesi, la possibilità di indirizzare autonomamente i processi decisionali dai quali tipicamente scaturiscono delle responsabilità, anche di carattere penale.

Piuttosto, apparirebbe corretto considerare il Data Protection Officer alla stregua di un professionista che svolge un ruolo fondamentalmente consulenziale, figura che nell'opinione tradizionale della giurisprudenza non viene coinvolta negli illeciti penali commessi dai soggetti per i quali presta la propria attività proprio perché, salvo diversa statuizione fra le parti, il consulente si limita a mettere a servizio la propria competenza per agevolare le decisioni che altri, il proprio cliente o committente, sono tenuti a prendere, assumendosene la paternità.

Eppure, alla luce di quanto anzidetto in merito alla rilevanza di qualsiasi tipo di "condotta agevolatrice" e di alcuni recenti arresti giurisprudenziali, la soluzione che vede un possibile coinvolgimento del D.P.O. ex art. 110 c.p. merita di essere approfondita.

Questo tipo di figure professionali infatti, da qualche tempo sono al centro di un interessante fermento giurisprudenziale che le vede valorizzate sia sotto il profilo civilistico che penalistico.

A tal proposito risulta di grande interesse una recente pronuncia in tema di concorso del professionista nella realizzazione di reati fiscali.

La Suprema Corte ha stabilito, nella sentenza n. 1999/2018 del 14-18 Novembre 2017, che il consulente possa essere chiamato a rispondere a titolo di concorso nel reato commesso dal cliente.

Nel caso di specie il professionista, consulente fiscale, si era reso domiciliatario di numerose società e aveva ideato uno schema operativo per realizzare indebite

compensazioni tributarie attraverso un *modus operandi*[112] che era già stato ritenuto illecito dall'Agenzia delle Entrate in quanto elusivo della normativa fiscale[113].

Ai fini che qui interessano, è rilevante analizzare la posizione difensiva espressa nel ricorso del professionista, che fondamentalmente sosteneva come un suo concorso colposo non potesse avere rilevanza penale, cosa che si sarebbe avuta invece se la propria condotta fosse stata preordinata a supportare in qualche modo il cliente a realizzare il proprio intento illecito, fornendo un contributo materiale o morale in tal senso[114].

Chiamata a esprimersi sulla vicenda, la Cassazione ha affermato il seguente principio di diritto:

> "In tema di reati tributari, è responsabile a titolo di concorso il consulente fiscale per la violazione tributaria commessa dal cliente (nella specie, per il delitto di indebita compensazione), quando il primo sia l'ispiratore della frode, ed anche se solo il cliente abbia beneficiato della operazione fiscalmente illecita"[115].

È però importante andare a vedere in base a quale argomentazione la corte arrivi a tale conclusione.

Ricostruiti i fatti di causa, i giudici di legittimità, dopo aver fornito del "professionista" una definizione estensiva e connotata dal requisito della serialità delle condotte[116], hanno rilevato che le operazioni poste in essere dall'agente erano andate ben oltre il ruolo che asseriva di aver assunto, avendo egli non solo fornito suggerimenti e consigli ma altresì ideato, partecipato e agevolato con proprie condotte la realizzazione del piano criminoso.

---

[112] Il reato di indebita compensazione tributaria di cui all'art. 10 *quater*, D. Lgs. n. 74 del 2000; veniva realizzato "mediante la trasmissione telematica dei modelli F24 relativi a crediti fittizi posti in compensazione mediante l'accollo del debito tributario di terzi"; v. Corte di Cassazione Sez. III Pen. Sentenza 18 gennaio 2018, n. 1999, punto 2.

[113] Cfr. Agenzia delle Entrate, Risoluzione del 15 novembre 2017, n. 140/E.

[114] Cfr. Corte di Cassazione, Sez. III Penale, Sentenza 14 novembre 2017 – 18 gennaio 2018, n. 1999, punto. 3.1.

[115] Ivi, punto 12.

[116] Cfr. Attanasio D., *La responsabilità concorsuale del professionista nell'esercizio dell'attività di consulenza fiscale: è necessaria la "serialità" della condotta per l'integrazione della nuova circostanza aggravante*, in "Diritto penale contemporaneo", fasc, 5/2018, p. 334.

Così operando costui era da considerarsi a pieno titolo responsabile ai sensi dell'art. 10 quater del d.lgs 74/2000, che pure prevede una fattispecie di reato proprio, normalmente commesso dagli amministratori di una società.

Infatti, in assenza di diversa disposizione di legge, l'avviso del Giudice di legittimità è che l'identificazione dei soggetti che possono incorrere nel reato va operata "non tanto su una qualifica soggettiva ma su un soggetto qualsiasi che peraltro si qualifica in base a ciò che compie"[117].

Inoltre, come affermato nel principio di diritto sopra esposto, è stato ritenuto del tutto irrilevante che le condotte fossero state poste in essere a vantaggio delle società assistite e non del professionista[118].

Orbene, dalla lettura della decisione della Suprema Corte non si evince di certo un'indiscriminata apertura alla responsabilità penale del professionista che svolga attività di consulenza.

Nel caso in esame infatti, la condotta del professionista è apparsa connotata da una evidente finalità di agevolazione del reato; la sussistenza del dolo e il fatto che tale condotta avrebbe valicato i confini della funzione di mera consulenza, hanno aggiunto quel *quid pluris* in ragione del quale è stata riconosciuta la punibilità dell'agente.

Si tratta di una decisione che non sorprende perché è ovvio che in presenza di una *intentio criminis* che si ripercuota in atteggiamenti omissivi o, come nel caso in esame, in azioni concrete volte consapevolmente a favorire la realizzazione di un illecito, si è sempre in presenza di una condotta agevolatrice punibile.

Ciò che però si evince dal ragionamento operato dalla Corte è l'accento posto sulla rilevanza della competenza tecnica posseduta dal professionista, in virtù del quale egli non poteva ritenersi inconsapevole o estraneo alla finalità criminosa sottesa al progetto.

Il punto è che ogni odierna considerazione in tema di responsabilità professionale va svolta alla luce del progressivo specializzarsi delle competenze in tutti gli ambiti

[117] Corte di Cassazione, Sez. III Penale, Sentenza 14 novembre 2017 – 18 gennaio 2018, n. 1999, punto 6.

[118] Ivi, par. 11.

dell'umano sapere, che ha portato ad una sempre più marcata importanza dell'apporto specialistico fornito da consulenti, periti e figure similari.

Basti pensare a quanto avviene nella quotidianità dei processi, dove è sempre più astratta dalla realtà l'espressione secondo la quale il giudice è *peritus peritorum*, dovendosi nella gran parte dei casi fare ricorso alle conoscenze extragiuridiche di un consulente tecnico d'ufficio per avere reale contezza di determinate situazioni.

Insomma, è facilmente constatabile come di fronte a problematiche di particolare difficoltà tecnica il contributo di uno specialista divenga nei fatti decisivo ai fini delle decisioni da adottare da parte degli organi dirigenziali di un'azienda, di una società, di un ente pubblico o di qualunque altro soggetto si trovi nella necessità di ricorrere alla prestazione qualificata.

È logico quindi che la giurisprudenza segua questa linea evolutiva, sottolineando come le caratteristiche professionali possedute dal soggetto agente abbiano una rilevanza ai fini dell'individuazione della rilevanza penale delle condotte da questi poste in essere[119].

Un soggetto qualificato, che eserciti le proprie mansioni con serialità e abitualità, difficilmente potrà dirsi ignaro dei propositi criminosi di un cliente che ricadano nell'ambito delle competenze tipiche della sua professione, se i dati fornitigli dal cliente sono completi e veritieri.

Certamente, egli potrà invocare l'assenza di un suo avallo o di qualsiasi condotta agevolatrice del piano illecito, per cui nella maggior parte dei casi si potrebbe configurare al più una connivenza, come tale non punibile[120], tuttavia ciò non toglie il fatto che, nonostante le condotte in commento richiedano la presenza dell'elemento soggettivo del dolo, egli potrebbe trovarsi spesso e facilmente nella situazione,

---

[119] A titolo di esempio, in Cass. Pen. sez. VI, n. 36125 del 2014, il giudice ha ritenuto che un parere autorevole fornito in seno ad un organo decisionale, quando idoneo anche solo a rafforzare il proposito criminoso altrui, integra una condotta sussumibile ex art. 110 c.p.

[120] Secondo Cass. Pen, sez. VI, n. 1986 del 2017, "la connivenza, traducendosi in una condotta meramente passiva ed inerte dinanzi ad un reato di cui pur si conosca la sussistenza, è, giustappunto, la scienza che altri sta per commettere o commetta un reato, e come tale non basta a dar vita ad una forma di concorso, richiedendo che il soggetto, all'infuori di qualsiasi concerto preventivo di adesione al proposito criminoso da altri concepito, si trovi soltanto ad essere consapevole della perpetrazione del reato e si astenga dal porvi ostacolo, pur potendolo fare, quando a ciò non sia tenuto per specifico suo obbligo giuridico".

spiacevole, di veder giudicati i propri comportamenti al fine di discernere la presenza di un concorso o di una mera connivenza.

Sono, queste, considerazioni che coinvolgono anche la figura del Data Protection Officer, che in virtù delle sue competenze e prerogative specifiche assume una posizione rilevante all'interno della struttura, pur se non connotata da poteri di gestione.

Trattandosi di un soggetto qualificato, i suoi pareri e consigli sono senz'altro idonei a influenzare le decisioni di un'azienda, società o ente.

Inoltre egli dovrebbe aver presente tutta la situazione relativa ai trattamenti che vi si svolgono, per cui è lecito ritenere che sarebbe nelle condizioni di accorgersi di eventuali condotte illecite, specie se commesse dal titolare o dal responsabile del trattamento, con i quali ha i rapporti più diretti: si tratta di elementi, non decisivi ma che sarebbero certamente tenuti in considerazione ai fini di un eventuale giudizio che vedesse vagliata la sua posizione.

4. Data Protection Officer e R.S.P.P: un confronto utile

In questa sede risulta assai utile, per completare il quadro e fornire ulteriori spunti di riflessione, operare un riferimento a una figura che presenta tratti caratteristici in comune con il Data Protection Officer, ossia il R.S.P.P. (Responsabile del Servizio di Prevenzione e Protezione).

Questa professionalità, che opera nell'ambito della sicurezza sul lavoro, è disciplinata dal d.lgs n. 81 del 2008, agli articoli 31 e seguenti.

Analizzando le mansioni attribuite dalla legge al R.S.P.P., si comprende che il suo ruolo fondamentale consiste nell' individuazione dei rischi che si possono concretizzare nel luogo di lavoro in base all'attività che vi sono svolte.

Il responsabile, al fine di evitare sinistri, fornisce consigli per assicurare l'incolumità dei lavoratori, predispone la formazione e l'elaborazione di misure di sicurezza, oltre a partecipare alle consultazioni in materia di salute e sicurezza sul lavoro[121].

[121] Così l'art. 33, c.1, d. lgs. 81/2008:
"Il servizio di prevenzione e protezione dai rischi professionali provvede:

In questo senso, la sua opera nel campo della sicurezza sul lavoro risulta similare a quella del Data Protection Officer in ambito privacy.

Non a caso chi aspira a svolgere queste funzioni deve possedere determinati requisiti ed esservi appositamente nominato, così come avviene per il D.P.O. [122].

Vi sono quindi delle forti similitudini fra le due figure, amplificate anche dal ruolo consulenziale svolto, seppur non esclusivamente, dal R.S.P.P.[123], evidenziato anche dagli *Ermellini*, che lo definiscono come "una sorta di consulente del datore di lavoro ed i risultati dei suoi studi e delle sue elaborazioni, come pacificamente avviene in qualsiasi altro settore dell'amministrazione dell'azienda, vengono fatti propri dal datore di lavoro che lo ha scelto, con la conseguenza che quest'ultimo delle eventuali negligenze del consulente è chiamato comunque a rispondere"[124].

Risulta quindi utile ai fini dell'indagine svolta in questa sede andare a verificare come la giurisprudenza si sia mossa nel valutare quelle situazioni in cui si siano verificati illeciti tali da paventare ipotesi di responsabilità penale del R.S.P.P.

Se inizialmente l'inquadramento normativo del R.S.P.P. non aveva dato adito a dubbi circa l'assenza di responsabilità in capo al soggetto chiamato a svolgere questa funzione, con l'evoluzione normativa, segnata in particolare dal d.lgs. n. 81/2008, le cose hanno

---

a) all'individuazione dei fattori di rischio, alla valutazione dei rischi e all'individuazione delle misure per la sicurezza e la salubrità degli ambienti di lavoro, nel rispetto della normativa vigente sulla base della specifica conoscenza dell'organizzazione aziendale;
b) ad elaborare, per quanto di competenza, le misure preventive e protettive di cui all'articolo 28, comma 2, e i sistemi di controllo di tali misure;
c) ad elaborare le procedure di sicurezza per le varie attività aziendali;
d) a proporre i programmi di informazione e formazione dei lavoratori;
e) a partecipare alle consultazioni in materia di tutela della salute e sicurezza sul lavoro, nonche' alla riunione periodica di cui all'articolo 35;
f) a fornire ai lavoratori le informazioni di cui all'articolo 36".

[122] Cfr. art. 32 d.lgs. 81/2008.

[123] È tuttavia doveroso segnalare che la disciplina del d.lgs. n. 81/2008 si caratterizza per una maggiore specificazione e responsabilizzazione della figura del R.S.P.P. rispetto alla prima definizione data alla figura dal d.lgs 626/1994.

[124] Cass. pen., sez. IV, 15 gennaio 2010, n. 1834, richiamata anche in Pascucci P. *La consulenza e la giurisprudenza*, Relazione presentata al Convegno regionale su "Il lavoro e la salute nelle Marche: le possibili strategie per un intervento comune", organizzato dal Comitato regionale di coordinamento per la salute e sicurezza nei luoghi di lavoro delle Marche, Jesi, 27 settembre 2010 (http://www.cpt.sr.it/index.php?option=com_docman&task=cat_view&gid=66&limit=10&limitstart=10&order=name&dir=ASC&Itemid=87&jjj=1534795759063) ultima cons. 20.08.2018.

iniziato a cambiare poiché, da semplice consulente che non necessitava di particolari attestazioni o competenze, l' R.S.P.P. è divenuto un soggetto cui sono richieste una competenza specialistica e requisiti professionali tali da permettergli di fornire una prestazione qualificata e adeguata alla delicatezza della mansione svolta.

Questa evoluzione è stata gravida di conseguenze a livello giurisprudenziale.

Vari sono gli arresti che vengono in rilievo ma vale la pena citare, perché esemplificativa, la sentenza della Cassazione Penale, Sez. IV n. 2814 del 27 gennaio 2011.

Il caso *de quo* scaturisce dalla morte di un lavoratore addetto alla movimentazione di carrozze ferroviarie il quale, durante una manovra in retromarcia, era scivolato in una fossa di ispezione ed era rimasto poi schiacciato dalle ruote del mezzo.

In tale circostanza il R.S.P.P. era stato chiamato a rispondere sotto il profilo penale per non aver adeguatamente valutato i profili di rischio relativi a questo tipo di manovre, così che in capo allo stesso erano stati ravvisati "profili di colpa generica e specifica"[125].

In verità la stessa Corte non negava la posizione di garanzia detenuta dal datore di lavoro, sul quale comunque pende l'obbligo di effettuare la valutazione dei rischi e di produrre il documento relativo alle misure di sicurezza e di prevenzione, insieme e con la collaborazione del R.S.P.P.[126].

Cionondimeno, la mancanza di un'esplicita previsione sanzionatoria in capo al R.S.P.P. non ne escludeva aprioristicamente la responsabilità penale.

Illuminante è un passaggio della sentenza ove la Corte così si esprime:

> "relativamente alle funzioni che la normativa di settore attribuisce al RSPP, l'assenza di capacità immediatamente operative sulla struttura aziendale non esclude che l'eventuale inottemperanza a tali funzioni - e segnatamente la mancata o erronea individuazione e segnalazione dei fattori di rischio delle lavorazioni e la mancata elaborazione delle procedure di sicurezza nonché di informazione e formazione dei lavoratori- possa

[125] Cassazione Penale, Sez. IV, 27 gennaio 2011, n. 2814, fatto-diritto, capoverso 3.

[126] Cfr. Cassazione Penale, Sez. IV, 17 dicembre 2012, n. 49031, citata in: Allegrezza R., *La Responsabilità penale del RSPP* in "Osservatorio per il monitoraggio permanente della legislazione e giurisprudenza sulla sicurezza del lavoro presso la Facoltà di Giurisprudenza dell'Università degli Studi di Urbino "Carlo Bo", pg.1. (http://www.cpt.sr.it/index.php?option=com_docman&task=cat_view&gid=66&limit=10&limitstart=10&order=name&dir=ASC&Itemid=87&jjj=1534795759063), ultima cons. 21.08.2018.

> integrare una omissione rilevante per radicare la responsabilità tutte le volte in cui un sinistro sia oggettivamente riconducibile ad una situazione pericolosa ignorata o male considerata dal responsabile del servizio"[127]

Sulla base di questa argomentazione e richiamando precedente giurisprudenza che aveva aperto la via alla corresponsabilità penale del R.S.P.P.[128], la Corte arriva a stabilire la correità del R.S.P.P., in uno al datore di lavoro, per aver colposamente mancato al rispetto all'osservanza degli obblighi impostigli dalla legge, avendo fornito valutazioni rivelatesi inadeguate a fronteggiare i potenziali fattori di rischio presenti sul luogo di lavoro.

Un orientamento, questo, tutt'altro che peregrino e che è stato poi confermato nella giurisprudenza successiva[129].

Quanto detto porta ad alcune riflessioni anche in relazione alla figura del Data Protection Officer.

Come accennato, le due figure hanno peculiarità simili, quali la necessità di una formazione specialistica e il possesso di requisiti professionali adeguati; inoltre il compito di supporto che offerto dal D.P.O. nei confronti del titolare del trattamento dei dati non appare così distante rispetto a quanto è tenuto a fare il R.S.P.P. nei confronti del datore di lavoro.

Il Data Protection Officer, come il R.S.P.P. non ha autonomia di spesa né poteri di gestione diretta, tuttavia il suo contributo specialistico risulta di fondamentale importanza ai fini delle decisioni da adottare in seno alla struttura.

Certamente le due figure non sono completamente sovrapponibili in quanto, come si è già avuto modo di considerare, i compiti del Responsabile del Servizio di Protezione e

---

[127] Cassazione Pen., Sez. IV, 27 gennaio 2011, n. 2814, fatto-diritto, capoverso 23.

[128] In particolare, la Corte cita: "Sezione IV, 13 marzo 2008, Reduzzi ed altro; Sezione IV, 15 febbraio 2007, Fusilli; Sezione IV, 20 aprile 2005, Stasi ed altro; di recente, Cfr. Sezione IV, 2 febbraio 2010, Proc. Rep. Trib. Gorizia in proc. Visintin ed altro", ma anche "Sezione IV, 15 luglio 2010, Scagliarmi".

[129] Cfr. *ex plurimis*, Cassazione Pen., sez. IV del 03 Febbraio 2015, n. 12223; Cass. pen. sez. IV, 11 Marzo 2013, n. 11492; Cass. pen. S.U. 18 settembre 2014, n. 38343, queste ultime richiamate anche in Pascucci P., *La tutela della salute e della sicurezza sul lavoro: il titolo I del d.lgs. n .81/2008 dopo il Jobs Act*, in "Quaderni di Olympus "(collana), Aras Edizioni, Fano, 2017, pp. 196-199.

Prevenzione sono maggiormente dettagliati e stringenti rispetto a quanto, ad oggi, è previsto per il D.P.O.

Egli, a seguito degli interventi legislativi che si sono succeduti nel tempo è destinatario di obblighi specifici rispetto ai quali è, legittimamente, chiamato a rispondere.

Lo stesso non può dirsi per il D.P.O., che è tratteggiato come una figura che ha sì una serie di prerogative ma i cui obblighi giuridici appaiono più sfumati.

Al momento appare improbabile che in sede giurisprudenziale si dia luogo a un pieno parallelismo fra le due figure: la mancanza di un potere di organizzazione in capo al D.P.O., mentre lo stesso è rinvenibile in capo al R.S.P.P., rende difficile immaginare che ci si spinga sin da subito a riconoscere ipotesi di responsabilità a titolo colposo in capo allo stesso.

Cionondimeno, chi scrive ritiene che non sia peregrino immaginare uno sviluppo giurisprudenziale che nel tempo valorizzi il disposto normativo fino ad arrivare a risultati analoghi, sia facendo leva sul concetto di "*sorvegliare l'osservanza*"[130] e sul compito di "considerare debitamente i rischi inerenti al trattamento"[131] piuttosto che sul valore del parere fornito su richiesta del titolare in caso di D.P.I.A. o sullo svolgimento della stessa, così come fatto, nel caso del R.S.P.P. per il dovere di "*individuazione dei fattori di rischio e valutazione dei rischi*"[132].

5. Conclusioni

In attesa che sui temi affrontati intervengano elementi chiarificatori di matrice giurisprudenziale o legislative, in questa sede giova considerare che l'ampiezza delle previsioni normative riferite al Data Protection Officer, contenute nel regolamento, potrebbe rivelarsi terreno ideale sul quale far fiorire orientamenti divergenti, con il rischio concreto di lasciare nell'incertezza coloro che sono chiamati a svolgere questo delicato ruolo.

[130] Regolamento UE n. 679/2016, art. 39 par. 1 lett. a).
[131] Regolamento UE n. 679/2016, art. 39 par. 2.
[132] D.lgs. n. 81/2008, art. 33, par.1 lett. a).

Rebus sic stantibus, è fondamentale mantenersi aggiornati sia sulle evoluzioni legislative che sugli interventi delle istituzioni nazionali ed europee sul tema e sugli apporti dottrinali sul punto.

Ciò detto, si ha motivo di ritenere che, in prospettiva futura, alla luce della valorizzazione delle competenze specialistiche che già sono necessarie nel mondo di oggi, e lo saranno ancor di più nel mondo di domani, appare probabile che le caratteristiche intrinseche della figura del D.P.O., la delicatezza dei suoi compiti e sua la centralità in aziende, enti pubblici e realtà professionali strutturate andrà determinando una sempre maggiore definizione dei doveri e delle responsabilità del ruolo, anche dal punto di vista penalistico.

Allo stato, si ritiene che sulla base del regolamento si possa senz'altro ipotizzare la sussistenza di una posizione di garanzia, consistente non tanto nell'assicurare la *compliance* della struttura, che certamente fa capo al titolare, quanto nell'obbligo di attivarsi e segnalare ogni situazione che non sia conforme al regolamento, così operando quel ruolo di sorveglianza impostogli dall'ordinamento.

A ciò potrebbe aggiungersi l'ipotesi di un concorso con altri soggetti ex art. 110 c.p. nel caso in cui il D.P.O. sia partecipe dell'*intentio criminis* comune e muova la sua attività in modo da favorirne la realizzazione; si tratta ad ogni modo di una ipotesi di responsabilità che andrebbe verificata caso per caso.

CAPITOLO IV

I PRESUPPOSTI DI LICEITA' NELLA CIRCOLAZIONE INTERNAZIONALE DEI DATI[133]

Premessa: Il ruolo del D.P.O. davanti alla sfida della tutela transazionale dei dati - 1. La direttiva 95/46/CE e il trasferimento di dati personali - 2. Il trasferimento dei dati personali e il rapporto con gli USA: dalla sentenza C-362/14 al *Privacy Shield* - 2.1. Il Safe Harbor - 2.2. Il Datagate e la reazione delle istituzioni europee. - 2.3. L'apporto della Corte di Giustizia - 2.4. L'invalidamento del Safe Harbor: la sentenza C-362-14. - 2.5. Il Privacy Shield. - 3. I principali richiami al trasferimento di dati personali verso Paesi terzi nelle disposizioni introduttive e nel testo del regolamento europeo n. 679/2016. - 3.1. Il Capo V - 3.1.1. Il principio generale - 3.1.2. Il trasferimento in base a una decisione di adeguatezza. - 3.1.3. Il trasferimento soggetto a garanzie adeguate - 3.1.4. Le norme vincolanti di impresa. - 3.1.5 Trasferimento o comunicazione non autorizzati dal diritto dell'Unione. - 3.1.6. Le deroghe in specifiche situazioni - 3.2. La cooperazione internazionale per la protezione dei dati personali.

Premessa: Il ruolo del D.P.O. davanti alla sfida della tutela transazionale dei dati

Ora che si è tratteggiata la disciplina dettata dal nuovo Regolamento Europeo con riguardo al Data Protection Officer, analizzando le peculiarità e le responsabilità di questo ruolo, è necessario inserire la sua figura nel contesto delle odierne problematiche in materia di privacy.

Chi scrive ritiene che il compito del Data Protection Officer non possa essere relegato alla mera ottemperanza di adempimenti legislativi anche perché, come si è già avuto di sottolineare, non è questo lo spirito che anima la nuova normativa e non e in questo modo che si può fare dare efficace attuazione al principio di *accountability*.

---

[133] Il presente capitolo riproduce, con le opportune modifiche e aggiornamenti, gran parte del contributo dell'autore (Cap.VII: *Il trasferimento di dati personali verso paesi terzi e organizzazioni internazionali*) all'opera: *Manuale di diritto alla protezione dei dati personali*, Maglio M., Tilli, N., Polini M. (a cura di), in "Professionisti e imprese" (collana), Maggioli Editore, Santarcangelo di Romagna, 2017.

Tutto questo va tenuto bene a mente se si considera che la grande sfida per la tutela dei dati personali al giorno di oggi risiede nella dimensione internazionale che tale tutela deve avere e nella predisposizione di strumenti che siano in grado di permettere un controllo effettivo sui dati anche quando questi non si trovano nella diretta disponibilità dell'interessato e delle Autorità del suo Paese.

È scontato dire che ad amplificare le cose in maniera esponenziale è stato lo sviluppo di internet e degli strumenti di comunicazione.

Innumerevoli sono gli ambiti in cui emerge la difficoltà di assicurare una reale osservanza dei diritti e delle prerogative di legge che le normative dell'Unione Europea e dei suoi stati membri garantiscono ai propri cittadini.

D'altronde è proprio nel contesto internazionale che le normative diventano più incerte e diventa più difficile attuale, considerato anche che, come osservato anche nel corso del primo capitolo, la gestione del flusso dei dati a livello internazionale e il controllo sugli stessi hanno importanti ricadute a livello sociale, economico e geopolitico.

È qui allora che viene in gioco ancora una volta il ruolo del Data Protection Officer, che non deve solo indicare, grazie alla sua conoscenza specialistica, quali strumenti siano idonei a garantire la liceità dei trasferimenti, bensì deve anche essere in grado di fornire indicazioni che abbiano un valore "etico"; deve cioè essere capace di valutare le situazioni in cui si trova e stabilire se sia necessario e opportuno trasferire determinati dati al di fuori dei confini europei oppure no e nel fare ciò dovrà bilanciare i diritti degli interessati con le esigenze della ricerca e le legittime aspettative delle aziende.

Si tratta di un compito non facile che richiede non solo competenze tecniche ma anche una notevole maturità umana e professionale.

Prima di entrare nel merito e al fine di comprendere meglio la portata della tematica analizzata, sarà opportuno illustrare quale sia la normativa descritta dal regolamento in tema di trasferimento di dati all'estero.

Chi intende svolgere il ruolo di D.P.O. deve infatti tenere bene a mente le indicazioni che il regolamento fornisce a questo proposito perché, se pure è vero che i mezzi di comunicazione oggi permettono di mettersi in contatto rapidamente con tutto il mondo, è vero anche che le distanze e i confini degli stati, e quindi degli ordinamenti giuridici,

sono una realtà con cui bisogna fare i conti e quindi trasferire dei dati fuori dai confini europei significa comunque perdere la possibilità di un controllo diretto e immediato sugli stessi.

Trasferire i dati è possibile, ma occorre che chi li riceve sia in grado di rispettare standard di tutela elevati, altrimenti perderebbero valore tutti gli sforzi fatti dalle istituzioni dell'unione sul tema della privacy, sia perché gli interessati, cioè i cittadini, si troverebbero a vedersi riconosciuti diritti che poi di fatto non avrebbero la possibilità di esercitare, sia perché quelle forme di criminalità che ambiscono ad appropriarsi dei dati al fine di commettere reati, avrebbero buon gioco a realizzare queste condotte laddove le attenzioni ai diritti e alla sicurezza sono più deboli.

Prescindere dalle vie legali predisposte dal regolamento significherebbe quindi rischiare di incorrere in pensanti ripercussioni a livello sanzionatorio, anche a livello penale come si potrà approfondire in seguito.

Le regole previste dal regolamento per i trasferimenti transnazionali tuttavia non sono certo improvvisate, ma si pongono in continuità con quanto già previsto dalla direttiva n. 46 del 1995.

1. La direttiva 95/46/CE e il trasferimento di dati personali

Dato il valore primario attribuito alla privacy in Europa, non stupisce che la direttiva 95/46/CE avesse previsto una serie di principi, regole, e misure di sicurezza atte a garantire la tutela dell'individuo all'interno del mercato globale, anche nella nascente dimensione digitale.

Per quanto riguarda il traffico transazionale dei dati, la direttiva vi dedicava il capo IV, consistente in due articoli (art. 25 e art. 26).

Vale la pena ripercorrere le fattispecie in questione anche se ormai abrogate in virtù di quanto disposto dall'art. 94 del nuovo Regolamento (UE) 2016/679.

All'articolo 25 venivano infatti enunciati i principi di riferimento della materia, *in primis* la subordinazione del trasferimento di dati personali da uno Stato membro verso un Paese terzo alla fornitura da parte di quest'ultimo di un "livello di protezione adeguato", da valutarsi con riferimento a "tutte le circostanze relative ad un trasferimento o ad una

categoria di trasferimenti di dati", cosa che implica una valutazione che tenga conto di molteplici elementi: dalla natura dei dati trattati, alle finalità del trattamento, alle norme di diritto presenti nei paesi di origine[134].

Nulla stabiliva però la direttiva circa l'identità dei soggetti chiamati a farsi carico di questo riconoscimento, lasciando così tale compito alle legislazioni nazionali.

La Commissione europea e gli Stati membri erano chiamati a collaborare insieme per individuare quali Paesi non fornissero l'adeguata tutela, con la possibilità, per la Commissione di richiedere agli Stati l'adozione delle misure idonee a garantire l'interruzione del flusso di dati verso i Paesi giudicati insicuri, almeno fino alla rinegoziazione degli accordi con questi.

L'art. 26 contemplava però una serie di eccezioni a questi principi.

Infatti, gli Stati membri potevano consentire il trasferimento anche in una serie di casi ivi descritti al primo paragrafo[135] nonché, in via generale, nel caso in cui il responsabile del trattamento presentasse "garanzie sufficienti", tali da permettere l'individuazione di un regime di rispetto per i diritti e le libertà fondamentali della persona, comprensivo

---

[134] Sul concetto di adeguatezza, il Gruppo di lavoro articolo 29 era intervenuto con il documento di lavoro *Trasferimento di dati personali verso paesi terzi: applicazione degli articoli 25 e 26 della direttiva europea sulla tutela dei dati* del 24 luglio 1998.

[135] Così l'art. 26, par.1 della direttiva 95/46/CE:

"In deroga all'articolo 25 e fatte salve eventuali disposizioni contrarie della legislazione nazionale per casi specifici, gli Stati membri dispongono che un trasferimento di dati personali verso un paese terzo che non garantisce una tutela adeguata ai sensi dell'articolo 25, paragrafo 2 può avvenire a condizione che:

a) la persona interessata abbia manifestato il proprio consenso in maniera inequivocabile al trasferimento previsto, oppure

b) il trasferimento sia necessario per l'esecuzione di un contratto tra la persona interessata ed il responsabile del trattamento o per l'esecuzione di misure precontrattuali prese a richiesta di questa, oppure

c) il trasferimento sia necessario per la conclusione o l'esecuzione di un contratto, concluso o da concludere nell'interesse della persona interessata, tra il responsabile del trattamento e un terzo, oppure

d) il trasferimento sia necessario o prescritto dalla legge per la salvaguardia di un interesse pubblico rilevante, oppure per costatare, esercitare o difendere un diritto per via giudiziaria, oppure

e) il trasferimento sia necessario per la salvaguardia dell'interesse vitale della persona interessata, oppure

f) il trasferimento avvenga a partire da un registro pubblico il quale, in forza di disposizioni legislative o regolamentari, sia predisposto per l'informazione del pubblico e sia aperto alla consultazione del pubblico o di chiunque possa dimostrare un interesse legittimo, nella misura in cui nel caso specifico siano rispettate le condizioni che la legge prevede per la consultazione".

della possibilità di ricorrere a strumenti giurisdizionali e contenuto in "clausole contrattuali appropriate".

In questi casi, era onere dello Stato membro informare la Commissione dell'autorizzazione concessa e compito di quest'ultima decidere su eventuali opposizioni provenienti da altri Stati membri.

Sulla base della direttiva, è stata adottata in Italia la l. n. 675 del 31 dicembre 1996, poi sostituita dal d.lgs. n. 196 del 30 giugno 2003, che disciplinava la materia al Titolo VII, rubricato: *Trasferimenti di dati all'estero*; tali disposizioni sono state abrogate ad opera del d.lgs. 101/2018 e la cosa è del tutto comprensibile dal momento che il regolamento europeo contiene già la disciplina specifica ed è *self executing*.

Fin qui il dato normativo, per quanto riguarda invece l'elaborazione giurisprudenziale che ne è conseguita, merita menzione il dibattito sorto sull'incerta definizione di "trasferimento di dati personali".

Sul punto è intervenuta la Corte di Giustizia[136], stabilendo che non può parlarsi di trasferimento di dati personali per il solo fatto che questi siano inseriti sulla pagina di un sito internet.

Vero è che in questo modo le informazioni ivi contenute sono potenzialmente accessibili dai più remoti angoli del pianeta, tuttavia la Corte non ritiene che sia questa la *ratio legis* sottesa alla disciplina sui trasferimenti transfrontalieri.

Infatti, ogni volta che is pubblicano dati su internet, quegli stessi dati divengono per giocoforza accessibili in ogni luogo del mondo nel quale vi siano le capacità tecniche per accedere alla rete; basta questo per dire che vi è stato un trasferimento? In effetti è vero che i dati sono accessibili anche fuori dai confini europei, ma non si tratta di un "trasferimento", quanto piuttosto di una messa a disposizione, revocabile in qualsiasi momento; chi accede ai dati in questo modo non ne detiene il possesso, a meno che non

[136] Corte di Giustizia dell'Unione europea, Sentenza nella Causa C-101/01 del 6 novembre 2003.

proceda a un *download* degli stessi o ad altre forme di archiviazione, facendoli in tal modo propri senza esserne tuttavia autorizzato[137].

Il trasferimento invece contempla un accordo fra coloro il soggetto che trasferisce e quello che riceve, il quale può disporre lecitamente di tali dati, nei termini dell'accordo con il quale è avvenuto il trasferimento. Così avviene soprattutto nell'ambito di accordi commerciali ed è questo che il legislatore ha voluto regolamentare.

Infatti, per quanto risulti evidente che il risultato finale sia comunque quello di mettere a disposizione dei dati anche al di fuori dei confini europei, un'interpretazione così omnicomprensiva del concetto di "trasferimento" avrebbe senza dubbio reso eccessivamente complicato il lavoro dei gestori dei siti internet, con significative ricadute sullo sviluppo del web.

In via generale, si deve constatare che, in assenza di una decisione di adeguatezza, gli strumenti più efficaci messi a disposizione dalla legislazione precedente al nuovo regolamento (peraltro trasposti nel nuovo impianto normativo) erano, e sono tuttora, le "clausole contrattuali tipo" (o *clausole contrattuali standard*), già previste *ex* art. 26, par. 4 della direttiva 95/46/CE, nonché le norme vincolanti d'impresa, altrimenti dette B.C.R. (*Binding Corporate Rules*).

2. Il trasferimento dei dati personali e il rapporto con gli USA: dalla sentenza C-362/14 al *Privacy Shield*

Parlando di trasferimento di dati personali al di fuori dello spazio europeo, una particolare attenzione deve essere posta sull'asse politico e commerciale con gli Stati Uniti d'America.

Per l'Europa il Paese americano rappresenta, storicamente parlando, il principale partner commerciale e politico e non c'è quindi da meravigliarsi se il flusso di informazioni e dati sia particolarmente intenso fra le due sponde dell'Atlantico.

Allo stesso tempo non deve stupire che Europa e Stati Uniti, pur avendo profonde radici in comune, abbiano nei secoli sviluppato approcci diversi alla vita culturale, sociale e

[137] Cfr. Piroddi P., *I trasferimenti di dati personali verso paesi terzi dopo la sentenza Schrems e nel nuovo regolamento generale sulla protezione dei dati*, in "Diritto dell'Informazione e dell'Informatica(Il)", fasc. 4-5, 2015, p. 827.

politica, e che quindi vi siano importanti differenze anche nell'elaborazione giuridica dei diritti della persona, cosa che appare in modo particolarmente chiaro quando si parla di privacy, come si è avuto modo di sottolineare nel corso del primo capitolo.

2.1. Il Safe Harbor

Il diritto americano, come noto, è un sistema di Common Law e come tale si fonda sulle pronunce dei giudici o, per dirla con un'espressione cara ai giuristi americani, sul *Law in the making*, il diritto che scaturisce dall'affronto delle problematiche concrete, contrapposto al *Law in the books* [138], il diritto delle norme generali e astratte, tipico dei Paesi di Civil Law.

Forse proprio a causa di questa caratteristica ontologica del sistema americano, il diritto teorizzato da Warren e Brandeis è stato a lungo meditato e approfondito dai giuristi, arrivando ad acquisire un'importanza sempre maggiore nella coscienza collettiva della società americana, soprattutto a partire dalla seconda metà del XX secolo, negli anni delle rivendicazioni dei basilari diritti civili da parte di interi gruppi sociali[139], senza tuttavia avere un univoco riconoscimento normativo.

Nonostante la nutrita articolazione dottrinale e giurisprudenziale infatti, ci volle uno scandalo, quello del "Watergate" nel 1970, per far superare l'*impasse* al governo americano e spingerlo all'approvazione di una legge in materia, il *Privacy Act*, che ha rappresentato per decenni il testo normativo di riferimento in materia di privacy.

Detta legge si occupava però di regolare i rapporti fra cittadini e istituzioni governative, mentre per quanto concerneva i rapporti fra privati, il modello americano si è sempre caratterizzato per la mancanza di una legislazione unitaria e generale, circostanza che ha favorito l'instaurarsi di un sistema di natura settoriale[140] ove i diritti relativi alla privacy

---

[138] Pagallo V. U., *La tutela dalla privacy negli Stati Uniti d'America e in Europa. Modelli giuridici a confronto*, Giuffrè Editore, Milano, 2008, pp. 66-70, cui si rimanda per un approfondimento sul tema della diversa lettura del diritto alla privacy in Europa e negli USA

[139] Merita una menzione la sentenza emessa dalla Corte Suprema USA nel caso rubricato al vol. 357 U.S. 449 (1958), nella quale la Corte, negando la legittimità della richiesta di una pubblica autorità che pretendeva di acquisire le liste degli iscritti ad un movimento di rivendicazione delle libertà civili, rilevò che la tutela della privacy è funzionale e indispensabile alla preservazione anche di altre libertà fondamentali garantite ai cittadini, quale il diritto di associazione.

[140] Sul punto si rimanda per approfondimenti a Miglietti L., *Profili storico-comparativi del diritto alla privacy*, in "Diritti Comparati", (http://www.diritticomparati.it/2014/12/profili-storico-comparativi-

vengono disciplinati nell'ambito dei diversi e specifici settori di attività, in particolare con riferimento al diritto dei consumatori.

Le differenze nell'approccio al tema della privacy non hanno però impedito ai governi degli Stati Uniti e dei paesi europei di negoziare, a cavallo del nuovo millennio, un accordo che regolasse modalità e condizioni per i trasferimenti internazionali di dati fra le due sponde dell'Atlantico.

Tale accordo, confluito poi nella decisione 2000/520/CE della Commissione del 26 luglio 2000, venne chiamato *Safe Harbor*, termine americano che significa "approdo sicuro".

Il suo fondamento era da rinvenirsi nella direttiva 95/46/CE, la quale all'art. 25, par. 1, permetteva il trasferimento di dati personali oltre i confini dell'Unione europea, pur nel rispetto della *condicio sine qua non* che il Paese di destinazione garantisse un livello di protezione adeguato ai dati stessi.

Per l'adesione da parte di un'azienda al regime del *Safe Harbor*, era necessario il rispetto dei principi[141] contenuti nell'allegato 1 cui si aggiungevano, nel secondo allegato, 15 *frequently asked questions and answers* (FAQs), il cui scopo era quello di assicurare un'interpretazione il più possibile omogenea dell'accordo, così da facilitarne il concreto recepimento da parte delle organizzazioni americane.

Il tentativo, nemmeno troppo celato, era quello di impostare gli scambi con gli Stati Uniti alla luce dei principi basilari che sovraintendono al trattamento dati personali nel diritto dei paesi europei.

---

del-diritto-alla-privacy.html), 4 dicembre 2014, ultima cons. 30 agosto 2018, di cui merita particolare attenzione la nota 25 che così si esprime: "Sono due i principali approcci alla regolamentazione in materia di privacy prevalenti negli Stati Uniti. Il primo si basa sulle cosiddette «fair information practies», che prevedono come elementi fondamentali l'informativa e la capacità di scelta dell'interessato. Si considera il processo che porta al trattamento dei dati esemplificato dal c.d. GLBA (Gramm-Leach-Bliley Act), ove sono contenute specifiche disposizioni che riguardano l'adozione di misure di sicurezza dei dati, l'obbligo di informare il cliente riguardo le policy di comunicazione dei suoi dati personali a terze persone e la sua possibilità di opporsi alla condivisione dei suoi dati finanziari con terze parti. Il secondo approccio è quello del cosiddetto «*permessible purpose*», che limita il trattamento dei dati a determinate finalità, previste dalla legge. Si tratta di un approccio che prende in considerazione il contesto in cui avviene il trattamento dei dati. Per maggiori approfondimenti si v. P.P. Swire, S. Bermann, *Information privacy*, IAPP Publication, 2007".

[141] I sette principi citati sono: Notifica, Scelta, Trasferimento successivo, Sicurezza, Integrità dei dati, Accesso, Garanzie di applicazione.

Sulla base di tale accordo lo scambio di dati da una sponda all'altra dell'atlantico è stato fluente per più di un decennio con vantaggi non solo economici ma anche per i più svariati ambiti della ricerca scientifica.

Questo libero scambio tuttavia, necessitava di sicurezza e garanzie circa l'effettiva tutela fornita ai dati utilizzati e nel tempo si è reso evidente come tali garanzie fossero tutt'altro che adeguate.

2.2. Il Datagate e la reazione delle istituzioni europee

Nel giugno 2013, a seguito delle rivelazioni di un *ex* dipendente della CIA, un quotidiano inglese iniziava la pubblicazione di alcuni documenti segreti, destinati a suscitare molto scalpore.

Stando a quanto ivi riportato, per iniziativa delle autorità americane, una compagnia di comunicazioni *leader* negli Stati Uniti avrebbe consegnato sistematicamente alle forze di *intelligence* informazioni circa dati e abitudini dei propri clienti.

Tutta questa vasta operazione sarebbe stata coordinata e diretta dalle agenzie di sicurezza americane, che avevano sì fra i propri compiti istituzionali il monitoraggio di potenziali terroristi ma non erano certamente legittimata a tenere sotto stretta sorveglianza le comunicazioni di intere popolazioni.

Lo scandalo, subito ribattezzato *Datagate*, si è andato successivamente allargando quando è emerso che anche alcune delle più importanti aziende del settore informatico erano coinvolte nelle attività di rapporti di sorveglianza, il che rendeva ancora più manifesta la violazione della privacy, data la capacità di queste ultime di accedere ad un'infinita varietà di dati degli utenti (non solo numeri e indirizzi ma anche foto, video, mail, ecc.) che pure sarebbero stati trasmessi alle forze di sicurezza americane.

È facile intuire come l'emergere di queste pratiche abbia messo seriamente in discussione alcuni capisaldi dei rapporti fra le due potenze internazionali.

Inoltre, lo scandalo ha instillato il germe del sospetto nei confronti della rete internet e in generale delle tecnologie di comunicazione, che da supremi veicoli della libertà di espressione e di scambi commerciali e culturali hanno iniziato ad essere guardati, all'opposto, come strumenti di controllo occulto.

La Commissione, in quella circostanza non mancò di sottolineare la sua preoccupazione[142] ma l'approccio adottato alla fine si rivelò meno drastico di quanto si inizialmente immaginato.

Infatti, pur riconoscendo il *vulnus* esistente nella tutela dei diritti degli europei per effetto dei trattamenti dati effettuati dagli americani, con una comunicazione *ad hoc* resa al Parlamento europeo, la Commissione ha voluto ricordare i grandi benefici che il regime del *Safe Harbor* aveva portato agli scambi commerciali e pertanto, ritenendo inopportuna una soluzione abrogativa dell'accordo, si è espressa per un rafforzamento dello stesso, da convenirsi con le autorità statunitensi, in modo che ne risultasse migliorata la "trasparenza delle politiche di tutela della sfera privata delle imprese certificate, e (...) garantite ai cittadini dell'UE la disponibilità e l'accessibilità di meccanismi di soluzione dei contenziosi"[143].

Ciò con l'ulteriore raccomandazione che l'eccezione alle tutele previste per motivi di sicurezza nazionale, clausola già prevista e sulla quale aveva fatto perno la difesa del governo americano per giustificare le proprie attività, venisse rivista e modulata secondo i principi di necessità e proporzionalità.

La politica di prudenza della Commissione a molti è apparsa dettata da ragioni politiche, che suggerivano di soprassedere a prese di posizioni più intransigenti, le quali trovavano invece sponda presso il Garante europeo per la protezione dei dati personali. Quest'ultimo, pur convenendo sulla necessità di recuperare quanto prima la fiducia, non ha esitato a sottolineare:

> "Le rivelazioni sulle attività di controllo da parte delle agenzie di intelligence statunitensi non soltanto intaccano la fiducia nei flussi di dati tra l'UE e gli USA, bensì si ripercuotono anche sui diritti esistenti ed esecutivi dei cittadini dell'UE al rispetto della vita privata e alla protezione dei loro dati personali. Tali diritti sono sanciti dal diritto primario e derivato sia dell'UE che del Consiglio d'Europa. Il GEPD deplora pertanto che la

[142] Cfr. in particolare: Comunicazione della Commissione al Parlamento europeo e al Consiglio, *Ripristinare un clima di fiducia negli scambi di dati fra l'UE e gli USA*, COM (2013) 846 final, Bruxelles, 27 novembre 2013.

[143] Ivi, punto 3.2.

> comunicazione sul ripristino della fiducia non abbia dedicato maggiore attenzione all'impatto sugli strumenti giuridici esistenti" [144].

Nello stesso documento, inoltre, si denunciava il fatto che nel contesto giuridico degli Stati Uniti, nonostante le affermazioni di principio, non vi fossero strumenti in grado di far valere concretamente i diritti vantati dai cittadini europei[145].

Insomma, la portata di quanto accaduto era tale che la regolamentazione pattuita anni prima con l'accordo *Safe Harbor* aveva perso di credibilità e si rendeva necessario un radicale ripensamento delle modalità di raccolta, trattamento, trasferimento, utilizzo di dati in movimento fra le due sponde dell'atlantico.

Tuttavia, la riluttanza delle istituzioni ad invalidare l'atto ha fatto sì che questo rimanesse operativo fino al 2015, allorquando si è arrivati per via giudiziaria laddove non si era ancora arrivati per volontà politica.

2.3. L'apporto della Corte di Giustizia

Negli anni immediatamente successivi allo scandalo *Datagate*, mentre la politica muoveva i propri passi, la giurisprudenza della Corte di Giustizia dell'Unione europea prendeva atto della necessità di intervenire in maniera più decisa rispetto al passato sulla tutela transazionale dei dati, anche al fine di risolvere problematiche pregresse che generavano situazioni di pericolo per i diritti dei cittadini europei.

Rilevanti in tal senso sono alcune sentenze che hanno di fatto delineato il tracciato entro il quale si è poi inserita prima la sentenza sul *Safe Harbor* e poi il nuovo regolamento europeo.

Va innanzitutto presa in considerazione la sentenza della Corte di Giustizia dell'Unione europea nella causa C-131/12 resa il 13 maggio 2014.

---

[144] Garante europeo per la protezione dei dati, *Sintesi del parere del Garante europeo della protezione dei dati sulla comunicazione della Commissione al Parlamento europeo e al Consiglio "Ripristinare un clima di fiducia negli scambi di dati fra l'UE e gli USA" e sulla comunicazione della Commissione al Parlamento europeo e al Consiglio sul funzionamento del regime "Approdo sicuro" dal punto di vista dei cittadini dell'UE e delle aziende ivi stabilite* (2014/C116/04), Bruxelles, 20.02.2014, IV, punto 79.

[145] Cfr. Ivi, I.4, punto 13.

Il caso giudiziario trae origine dal ricorso di un cittadino spagnolo che aveva richiesto l'eliminazione, dai risultati forniti da un motore di ricerca, di alcune informazioni risalenti nel tempo e a lui pregiudizievoli perché afferenti a vicende ormai conclusesi.
L'Autorità spagnola per la protezione dei dati decideva di ordinare alla società che gestiva il motore di ricerca la cancellazione dei dati in oggetto ma l'azienda in questione resisteva portando le proprie ragioni all'attenzione della *Audiencia Nacional*, che a sua volta ne investiva la Corte di Giustizia.
La sentenza ha assunto una particolare importanza perché ha riconosciuto il cosiddetto "diritto all'oblio", declinatosi in questo caso con l'obbligo per il motore di ricerca di rimuovere quelle informazioni che non si abbia più ragione di offrire agli utenti.
Ai fini che qui interessano però, ciò che preme rilevare è come la sentenza in questione abbia sciolto il nodo della legge applicabile al caso, interpretando in via estensiva l'art. 4, par. 1, lett. *a*) della direttiva.
La norma imponeva il ricorso ad una determinata legislazione nazionale qualora nel territorio di quel paese fosse radicato uno stabilimento che fra le sue attività effettuasse anche il trattamento di dati personali. Qualora poi uno stesso responsabile del trattamento fosse stabilito nel territorio di più Stati membri, esso doveva adoperarsi per fare in modo che ogni stabilimento rispettasse la normativa del Paese ospitante.
Premesso che la Corte ha precisato che l'attività svolta dalla società citata, concretantesi nel "trovare informazioni pubblicate o inserite da terzi su Internet, nell'indicizzarle in modo automatico, nel memorizzarle temporaneamente e, infine, nel metterle a disposizione degli utenti di Internet secondo un determinato ordine di preferenza" [146], presentasse tutte le caratteristiche proprie di un trattamento di dati personali, ciò che merita ulteriore attenzione è il ragionamento per cui, secondo i giudici, il termine stabilimento non indicava solo la sede primaria dell'azienda ma doveva essere così interpretato:

> "(...) un trattamento di dati personali viene effettuato nel contesto delle attività di uno stabilimento del responsabile di tale trattamento nel territorio di uno Stato membro, ai

[146] Corte di Giustizia dell'Unione europea, Sentenza del 13 maggio 2014, Causa C-131/12, punto 41.

> sensi della disposizione suddetta, qualora il gestore di un motore di ricerca apra in uno Stato membro una succursale o una filiale destinata alla promozione e alla vendita degli spazi pubblicitari proposti da tale motore di ricerca e l'attività della quale si dirige agli abitanti di detto Stato membro."[147].

Pertanto essendovi in Spagna un'articolazione territoriale della società, che effettuava attività di trattamento dati, era a tutti gli effetti da considerarsi quale *stabilimento* e si legittimava così l'intervento della legislazione e dell'Autorità di protezione dati del paese in cui era situata.

Si è trattato, evidentemente, di un passo chiarificatore, dimostrativo della volontà della Corte di Giustizia di spingere per una più ampia pervasività delle norme europee. Sullo stesso solco si collocherà, due anni più tardi, la sentenza del 1° ottobre 2015 sulla causa C-230/14, che trae origine dall'attività di una società slovacca che gestiva tramite il proprio sito internet alcuni annunci relativi a immobili situati in Ungheria.

La società in questione aveva permesso a clienti ungheresi la pubblicazione di inserzioni gratuite per un determinato periodo, alla scadenza del quale questi ultimi avevano chiesto la cancellazione dei propri annunci e dati personali forniti, richieste cui la società richiesta non ottemperava.

I clienti quindi si rivolgevano all'Autorità ungherese per la protezione dei dati, dalla quale ottenevano una risposta positiva.

Avverso tale decisione però la società ricorreva dapprima innanzi al *Fővárosi Közigazgatási és Munkaügyi Bíróság* (tribunale amministrativo e del lavoro di Budapest) e poi avanti alla *Kúria* (Corte Suprema ungherese).

Quest'ultima, a sua volta, investiva la Corte di Giustizia chiedendo lumi circa la possibilità di applicare il diritto ungherese in questa situazione e otteneva una risposta affermativa, assai rilevante perché in grado di fare luce sul concetto di *stabilimento* e di ampliarne la portata.

Nell'occasione infatti, i giudici europei hanno sostenuto che ciascuno Stato membro fosse chiamato ad applicare le norme nazionali adottate in forza della direttiva europea

[147] Ivi, punti 55, 56.

anche in mancanza di una vera e propria filiale, sede distaccata o ufficio, nel senso comune del termine.

Questo perché la *ratio* della direttiva, finalizzata al perseguimento della più ampia tutela possibile, portava a prendere in considerazione "qualsiasi attività reale ed effettiva, anche minima, esercitata tramite un'organizzazione a carattere permanente"[148] e pertanto la conclusione era che "la presenza di un unico rappresentante, in talune circostanze, può essere sufficiente a costituire un'organizzazione stabile se il medesimo opera con un grado di stabilità sufficiente con l'ausilio dei mezzi necessari per la fornitura dei servizi concreti di cui trattasi nello Stato membro in questione"[149].

Così argomentava la Corte, rilevando a quel punto che la società in questione aveva effettivamente nel territorio ungherese un rappresentante che fungeva da intermediario nei rapporti con gli inserzionisti e che aveva anche aperto un conto bancario.

Queste circostanze venivano quindi valorizzate e giudicate sufficienti per configurare la presenza di uno stabilimento nel territorio ungherese e, per l'effetto, la sua soggezione alla legge nazionale e ai poteri dell'Autorità di protezione dei dati locale.

Ora, entrambi i pronunciamenti citati sono rilevanti perché consentono di apprezzare lo sforzo interpretativo della Corte di Giustizia la quale, consapevole della dimensione transnazionale del mercato digitale e quindi delle conseguenti problematiche legate alla privacy, ha iniziato un'opera di progressivo affrancamento da una tutela che faceva perno sul principio di territorialità per abbracciare invece l'idea che la legislazione debba essere il più possibile vicina ai cittadini, che hanno il diritto di rivolgere le proprie istanze agli organi nazionali preposti e da essi ottenere risposte.

È probabile che questa sarebbe strada sarebbe comunque stata percorsa ma non è peregrino ritenere che le rivelazioni del *Datagate* abbiano contribuito non poco in questo senso.

---

[148] Corte di Giustizia dell'Unione europea, comunicato stampa n. 111/15, *La normativa di uno Stato membro sulla tutela dei dati può essere applicata a una società straniera che svolge, in tale Stato, tramite un'organizzazione stabile, un'attività reale ed effettiva* 1° ottobre 2015.

[149] Corte di Giustizia dell'Unione europea, sentenza del 1° ottobre 2015, causa C-230/14, punto 30.

2.4. L'invalidamento del Safe Harbor: la sentenza C-362-14

L'estrema rilevanza del trasferimento di dati fra USA e UE, che aveva spinto anche le istituzioni europee a muoversi con prudenza dopo i fatti del 2013, permette di comprendere l'agitazione che ha colto gli operatori allorquando la sentenza C-362-14 della Corte di Giustizia ha invalidato il *Safe Harbor* aprendo a tutti gli effetti una nuova fase nei rapporti di scambio e trattamento di dati personali fra Stati Uniti ed Unione europea.

La vicenda ha preso le mosse dagli studi di un giovane studente in legge austriaco il quale aveva svolto un'esperienza di studi nella Silicon Valley, che gli aveva lasciato diverse perplessità sul modo in cui i dati personali dei cittadini europei venivano tutelati negli U.S.A.

Nel 2011 lo studente decise di richiedere ad un noto social network copia di tutti i dati conservati nei suoi database che fossero inerenti alla propria persona.

Ciò fu reso possibile dal fatto che la società in questione, pur avendo base negli USA, aveva aperto una sede in Irlanda e pertanto era tenuta all'osservanza della normativa dell'Unione europea.

In tutta risposta, la società inviò al richiedente ben 1.200 pagine di documenti, comprendenti ogni operazione da egli compiuta, incluse dati che avrebbero dovuto essere già stati cancellati.

Aveva inizio quindi una campagna condotta sui grandi mezzi di comunicazione, volta sia ad informare l'opinione pubblica, sia a predisporre le opportune iniziative legali finalizzate ad ottenere il ristoro della privacy violata.

Un primo ricorso al *Data Protection Commissioner*, l'Autorità irlandese per la protezione dei dati personali, ebbe esito negativo.

Sosteneva infatti l'Autorità che non vi fosse prova del lamentato accesso illegittimo ai dati e che, inoltre, l'accordo vigente fra USA e UE, approvato dalla Commissione europea, impedisse qualsiasi intervento sulla questione da parte delle Autorità nazionali di protezione dei dati [150].

[150] Cfr. Corte di Giustizia dell'Unione europea, sentenza del 6 ottobre 2015, Causa C-362/14, punto 29.

Tutt'altro che scoraggiato, il ricorrente portò caparbiamente la questione all'attenzione della *High Court of Ireland*, la quale a sua vota ne investì la Corte di Giustizia dell'Unione europea.

La corte di Giustizia, conscia della particolare attenzione generatasi sul tema e dell'importanza della posta in gioco, decise in quell'occasione di intraprendere una strada di radicale rottura con il passato, invalidando il *Safe Harbor* con la sentenza C-362/14, resa dalla Grande Sezione il 6 ottobre 2015.

L'annullamento del *Safe Harbor* apriva la problematica concernente la regolamentazione degli enormi flussi di dati fra le due sponde dell'Atlantico.

Nel Comunicato stampa n. 117/15 del 6 ottobre 2015, veniva riepilogata la vicenda e le motivazioni che avevano spinto ad un così grave provvedimento, che si procede ora ad analizzare nei suoi punti salienti.

Preliminarmente, la Corte ha ritenuto opportuno ribadire il ruolo delle Autorità nazionali di controllo, deputate alla tutela e salvaguardia dei fondamentali diritti di riservatezza e privacy[151].

Tale ruolo non può quindi essere limitato, neppure dalle decisioni assunte dalla Commissione europea, perché anche le Autorità di controllo nazionali sono tenute alla sorveglianza dei trasferimenti di dati personali oggetto di una decisione della Commissione e, se investite di una domanda, devono poter esaminare in piena indipendenza se il trasferimento dati che ne costituisce oggetto rispetti o meno i requisiti stabiliti dalla direttiva.

Ciò premesso, i giudici europei sono passanti ad analizzare la questione sottesa al rinvio pregiudiziale, ossia la validità della decisione della Commissione del 26 luglio 2000, cd. *Safe Harbor*, chiamata in causa dal ricorso.

Nel merito, la Corte ha rigettato qualsiasi lettura formalistica, ribadendo che sarebbe stato compito della Commissione verificare se fattivamente gli Stati Uniti stessero garantendo un livello di protezione dei diritti fondamentali rispettoso degli accordi presi.

[151] Cfr. Ivi, punto 41

I giudici hanno dimostrato di ben comprendere il valore economico e commerciale di queste operazioni e la sottesa tensione fra libertà di impresa e tutela dei diritti fondamentali.

Infatti, è stato correttamente osservato che nel ragionamento della Corte emerge in modo lampante il principio secondo il quale il trasferimento internazionali di dati possono aver luogo se e solo se siano lo Stato di destinazione è in grado di garantire loro una tutela adeguata secondo le disposizioni della Direttiva 95/46/CE, perché in difetto si sacrificherebbe alle ragioni del commercio internazionale un fondamentale diritto della persona quale è quello alla privacy.

"La Corte però, sempre al punto 48, pone un paletto molto chiaro: i trasferimenti in questione non possono avere luogo se non in presenza di un livello di protezione adeguato. Così, le ragioni del commercio non possono mai prevalere su quelle della privacy, se non in presenza di requisiti particolari" [152].

Proprio in merito alla sussistenza di un livello di protezione adeguato, la Corte ha avuto buon gioco a constatare che la Commissione non aveva proceduto a una verifica puntuale in tal senso, ma si era limitata a esaminare il regime del *Safe Harbor* su un piano meramente formale.

Il massimo organo di giustizia dell'Unione ha quindi ritenuto del tutto inadeguato tale regime, non tanto per un'insufficienza normativa, quanto piuttosto per il fatto che esso fosse esclusivamente applicabile alle imprese americane che lo sottoscrivevano, di fatto non ponendo alcun vincolo alle autorità pubbliche degli Stati Uniti[153].

---

[152] Pollicino O., Bassini M., *La carta dei diritti fondamentali dell'Unione Europea nel reasoning dei giudici di Lussemburgo*, in *Il diritto dell'Informazione e dell'Informatica*, anno XXXI, n. 4/5, 2015, pp. 755-756; l'autore richiama in particolare il punto 48 della citata Sentenza sulla Causa C-362/14 che infatti così recita: "Riconoscendo al contempo, al suo considerando 56, che i trasferimenti di dati personali dagli Stati membri verso paesi terzi sono necessari allo sviluppo degli scambi internazionali, la direttiva 95/46 pone come principio, al suo articolo 25, paragrafo 1, che siffatti trasferimenti possano avere luogo soltanto se tali paesi terzi garantiscono un livello di protezione adeguato.".

[153] La sentenza lasciava poi alle Autorità garanti dei singoli stati membri pronunciarsi sulla decadenza dell'accordo, cosa che ha fatto anche il Garante per la protezione dei dati personali: Cfr. Comunicato del Garante per la protezione dei dati personali, *Trasferimento dati personali verso gli USA: caducazione provvedimento del Garante del 10 ottobre 2001 di riconoscimento dell'accordo sul c.d. "Safe Harbor"*, Roma, 22 ottobre 2015.

2.5. Il Privacy Shield

Alla sentenza C-362-14 hanno fatto seguito due anni di intensa attività diplomatica e negoziale, necessari per ricucire uno strappo che aveva messo seriamente in discussione i rapporti di fiducia fra Stati Uniti e Unione europea.

A tal fine la Commissione, già in una comunicazione del 27 novembre 2013 [154], aveva presentato delle proposte volte a superare la crisi creatasi intorno al *Safe Harbor*.

Le Linee guida dettate in quell'occasione implicavano tre direzioni di sviluppo: in primo luogo si sottolineava la necessità di una rapida approvazione del pacchetto di riforma europea in materia di protezione dei dati personali; in secondo luogo si raccomandava un rafforzamento delle garanzie in materia di protezione dei dati nel contesto della cooperazione fra Autorità di contrasto, prevedendo anche diritti individuali azionabili da parte dei cittadini dell'Unione e da ultimo si illustrava l'urgenza di mettere in pratica tredici raccomandazioni suggerite dalla Commissione stessa per migliorare il regime del *Safe Harbor*, specificate al punto 8 della Comunicazione e vertenti su: Trasparenza, Ricorsi, Applicazione e Accesso da parte delle autorità statunitensi [155].

Su queste premesse le parti in causa hanno collaborato per raggiungere un'intesa e il 2 febbraio del 2016 la Commissione ha annunciato con un comunicato stampa[156] il raggiungimento di un nuovo accordo fra Stati Uniti e Unione europea per la regolamentazione del flusso transatlantico dei dati, confluito poi nella decisione di adeguatezza del 12 luglio 2016 [157].

Tale accordo, ribattezzato *Privacy Shield* (scudo della privacy), sembra voler ribadire, anche nel nome, la priorità che si è voluta accordare alla protezione dei dati personali.

---

[154] Cfr. Commissione Europea, *Comunicazione della Commissione al Parlamento Europeo e al Consiglio sul funzionamento del regime "Approdo sicuro" dal punto di vista dei cittadini dell'UE e delle società ivi stabilite*, Bruxelles, COM(2013) 847 final, 27 Novembre 2013.

[155] Cfr. Junker J.C., *Un nuovo inizio per l'Europa Il mio programma per l'occupazione, la crescita, l'equità e il cambiamento democratico Orientamenti politici per la prossima Commissione europea*, Strasburgo, 15 luglio 2014, punto 9.

[156] Commissione europea – Comunicato stampa: *La Commissione europea e gli Stati Uniti concordano un nuovo quadro per i flussi transatlantici di dati: lo scudo UE-USA per la privacy*, Strasburgo, 2 febbraio 2016, IP/16/216.

[157] Cfr. Commissione europea, Comunicato stampa: *La Commissione europea lancia lo scudo UE-USA per la privacy: più tutele per i flussi transatlantici di dati*, IP/16/2461, Bruxelles, 12 luglio 2016.

Nelle intenzioni, infatti, il nuovo regime vuole fornire una regolamentazione rispettosa dei diritti dei cittadini europei, che non riguardi solo il settore commerciale ma anche l'utilizzo che dei dati trasferiti potranno fare le forze di *intelligence*.

Le imprese che vogliono importare dati personali dall'Europa avvalendosi del *Privacy Shield*, sono tenute a rispettare scrupolosamente le modalità di trattamento pattuite, rese sensibilmente più impegnative (tra le novità, particolarmente degne di nota è la limitazione dei c.d. trasferimenti successivi, ossia quei trasferimenti che avvengono in subcontratto e che coinvolgono soggetti non rientranti nell'accordo).

Viene poi ricordato che, nel caso in cui un'impresa tratti i dati degli europei nell'ambito delle risorse umane, dovrà in questa materia fare riferimento alle determinazioni delle Autorità di controllo europee.

Il Ministero del Commercio statunitense ha il compito di monitorare il comportamento delle imprese coinvolte nel *Privacy Shield* ed eventualmente depennare quelle che non ne rispettano le condizioni.

Qualora poi un cittadino europeo ritenga che il proprio diritto alla privacy sia stato leso da un uso improprio dei suoi dati personali da parte delle imprese americane, grazie al nuovo accordo egli può disporre di nuovi strumenti preposti alla salvaguardia dei suoi diritti.

Innanzitutto, è possibile proporre un reclamo direttamente all'impresa che si ritiene abbia agito in violazione dell'accordo, la quale deve rispondervi entro un termine prestabilito di 45 giorni.

Il reclamo può essere proposto anche dinanzi alle singole Autorità di controllo presenti nei paesi europei, che ne curano l'invio e ne seguono l'*iter* presso il Ministero del commercio e la Commissione federale per il commercio statunitensi, ottenendo così una velocizzazione e semplificazione del procedimento e una maggiore incisività dell'azione di indagine.

Al cittadino europeo è inoltre consentito il ricorso a meccanismi alternativi di risoluzione delle controversie (A.D.R.) che le imprese sono previamente tenute a indicare e grazie ai quali sarà possibile accertare il problema presentato e cercarvi una soluzione.

In ultima istanza, come *extrema ratio*, è possibile far valere i propri diritti in una procedura di arbitrato davanti a una giuria selezionata in maniera *bipartisan* dal Ministero del commercio americano e dalla Commissione europea, la cui decisione è vincolante per le imprese americane che aderiscono al *Privacy Shield*.

Per altro verso, qualora i propri dati vengano coinvolti nelle attività svolte dagli operatori della sicurezza nazionale, il cittadino europeo avrà diritto ad adire un mediatore indipendente, che sarà chiamato a gestire reclami e richieste di informazioni, al fine di valutare l'effettivo rispetto delle normative concordate.

Per evitare poi che si ripeta l'errore già commesso con il *Safe Harbor*, e cioè che il regime di protezione formalmente stabilito venga poi sistematicamente eluso nella sostanza, si è deciso di adottare un meccanismo annuale di riesame congiunto svolto per parte europea dalla Commissione e per parte statunitense dal Ministero del commercio ai quali si aggiungeranno esperti dell'*intelligence* nazionale statunitense e le Autorità europee di protezione dei dati.

Qualora dovessero emergere nuovamente gravi violazioni degli accordi, la Commissione sarà tenuta a prendere atto del venir meno della tutela fornita ai diritti dei cittadini europei e per l'effetto dovrà sospendere il *Privacy Shield*, conformemente a quanto stabilito nella sentenza C-362/14.

Il nuovo approccio, pertanto, si presenta di natura "dinamica" e d'altronde l'esperienza ha dimostrato che non si può fare affidamento sulle sole previsioni normative, soprattutto in un settore estremamente delicato e "magmatico" come quello della privacy, bensì è opportuno procedere a costanti verifiche delle condizioni pattuite, al fine di verificarne la sostanziale osservanza e, se del caso, procedere alle opportune "correzioni di rotta".

Invero, in fase di trattativa si erano levate voci critiche, prime fra tutte quella del Parlamento europeo che si è già mostrato non del tutto convinto dell'adeguatezza delle

nuove norme[158] e quella del "Gruppo di lavoro articolo 29", che aveva sollecitato modifiche al testo in fase di approvazione[159].

Il bilancio è per ora positivo; lo scambio di dati è ripreso con il nuovo accordo, in accordo con gli interessi delle aziende europee e statunitensi, tuttavia vi sono ancora forti tensioni, specie da quando, con il cambio di amministrazione ai vertici della Casa Bianca, le politiche in materia di sicurezza dei dati non hanno seguito una linea di aperta e piena collaborazione con le istituzioni europee, al punto che il Parlamento Europeo si è detto pronto a sospendere il *Privacy Shield*[160] a motivo della scarsa collaborazione riscontrata da parte delle autorità americane e della persistente incertezza circa i futuri sviluppi della tutela dei diritti dei cittadini europei in questo ambito da parte delle autorità americane

Un esito che vedesse nuovamente la caducazione dell'accordo raggiunto avrebbe conseguenze molto gravi e lo si deve considerare davvero come una *extrema ratio*, la quale è tuttavia improbabile ma non impossibile.

Il quadro appare in evoluzione e chiunque voglia affacciarsi nell'ambito della privacy dal punto di vista professionale dovrà seguirne gli sviluppi nei prossimi mesi perché qualunque realtà operante nel commercio, che non voglia limitarsi a raccogliere e conservare i dati secondo il regolamento ma intenda utilizzarli come fonte di business, dovrà necessariamente misurarsi con il tema dei trasferimenti internazionali di dati e, in particolari con quelli nei confronti degli Stati Uniti.

3. I principali richiami al trasferimento di dati personali verso Paesi terzi nelle disposizioni introduttive e nel testo del regolamento europeo 2016/679

Per quanto riguarda il profilo del trasferimento dati all'estero, numerosi sono gli aspetti che devono essere tenuti in considerazione da parte degli operatori, giacché il nuovo

---

[158] Cfr. Parlamento europeo, Comunicati stampa – Giustizia e affari interni/Relazioni esterne del 26 maggio 2016: *Trasferimento dati UE-USA: necessari miglioramenti al "Privacy Shield"*.

[159] Cfr. Gruppo di lavoro articolo 29, *Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision*, 13 aprile 2016.

[160] Cfr. Parlamento Europeo, *Risoluzione del Parlamento europeo del 5 luglio 2018 sull'adeguatezza della protezione offerta dallo scudo UE-USA per la privacy* (2018/2645(RSP), 5 luglio 2018.

regolamento, pur se riprende in buona parte l'impianto già presente nella direttiva del 1995, non manca di compiere una notevole opera di miglioramento e specificazione.
Il legislatore europeo dimostra consapevolezza circa l'importanza dei beni giuridici in discussione, il ruolo dell'evoluzione sociale e tecnologica e le conseguenze delle controverse vicende legate all'utilizzo dei dati degli europei al di fuori dei confini del vecchio continente.
Sin dalle prime battute del regolamento emerge quindi la volontà di superare quella frammentazione e complessità delle normative europee e nazionali che costituiva un "notevole ostacolo" [161] allo sviluppo dei traffici internazionali che si avvalgono anche del trasferimento dei dati personali.
Va tuttavia sottolineato che ad ogni concessione in tal senso il regolamento fa seguire una precisazione volta a scongiurare il rischio di interpretazione lassista.
Prova ne è il fatto che una delle più rilevanti novità previste dal regolamento è l'abbandono del principio dello stabilimento per come elaborato dalla direttiva 95/46/CE.
Infatti, seguendo un'evoluzione che, come si è avuto modo di vedere, era già iniziata con la sentenza nella causa C-131/12, la nuova normativa prevede che la propria applicazione debba aver luogo "indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione"; così si esprimono il considerando n. 22 e l'articolo 3, che nel tracciare l'ambito di applicazione del regolamento, ne stabilisce la precettività anche per i titolari e i responsabili del trattamento non stabiliti nell'Unione europea nei casi in cui il trattamento riguardi "dati personali di interessati che si trovano nell'Unione", in relazione a offerte di beni e servizi, siano esse gratuite o onerose ovvero il monitoraggio sul comportamento di persone fisiche che si trovano nell'Unione[162].

Il messaggio che se ne evince è chiaro: ogniqualvolta si dia luogo al trasferimento di dati personali di cittadini europei, occorre garantire il livello di tutela che il diritto dell'Unione impone per quella determinata situazione.

---

[161] Commissione Europea, *Proposta di regolamento del Parlamento europeo e del Consiglio, concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati, COM (2012) 11 final, 2012/0011 (COD)*, relazione introduttiva, Bruxelles, 25 gennaio 2012.
[162] art. 3 par.2 Regolamento (UE) 2016/679.

A ben pensarci non potrebbe darsi altra soluzione se si considera che il nuovo regolamento interviene a disciplinare un diritto di fondamentale importanza per le tradizioni giuridiche dei diversi paesi europei, la cui centralità è sancita anche dalla Carta di Nizza. È forse la prima volta che il diritto europeo avoca a sé una tutela così incisiva e determinante, perciò è comprensibile che il livello di prudenza sia elevato, così come non stupisce che vi sia l'intenzione di rendere precettive le nuove disposizioni anche al di fuori dei confini dell'Unione, dal momento che, in difetto, risulterebbe del tutto inconsistente l'effettività dei diritti vantati dai cittadini europei.

In quest'ottica si possono leggere le disposizioni introduttive.

Vale la pena soffermarsi sul considerando n. 6 che, prendendo atto delle richieste delle imprese, volte ad ottenere un regime più agevole per il trasferimento e gli scambi internazionali di dati, riconosce l'importanza di questa attività per lo sviluppo imprenditoriale e il ruolo svolto in questo senso dalle nuove tecnologie, che però devono anche essere sfruttate per garantire un elevato livello di protezione dei dati personali.

Pure si prende atto, al considerando n. 48, della necessità per i titolari del trattamento dati operanti nel medesimo gruppo imprenditoriale o in enti collegati a un organismo centrale di trasmettere dati personali all'interno del gruppo di appartenenza per fini amministrativi, necessità cui il regolamento si preoccupa di rispondere assicurando il rispetto dei principi generali della materia.

Ancora, il considerando n. 101, nel ribadire l'importanza dei flussi di dati personali per l'espansione del commercio e della cooperazione internazionale, si cura di precisare che il livello di tutela delle persone fisiche garantito all'interno dell'Unione europea non deve risultare compromesso anche nelle ipotesi di trasferimenti successivi di dati da un Paese terzo o organizzazione internazionale verso altro Paese terzo od organizzazione internazionale, ribadendo così il principio per cui un trasferimento può essere operato validamente solo se rispetta le condizioni del regolamento europeo.

Ciò si dice, avendo al contempo cura di precisare, nel successivo considerando n. 102, che la novella legislativa non pregiudica gli accordi già stipulati tra l'Unione e i paesi terzi in materia di trasferimento dati.

Il considerando n. 107 si preoccupa invece di ricordare il ruolo di monitoraggio e sorveglianza cui è tenuta la Commissione europea, affinché i Paesi terzi o le organizzazioni internazionali che sono stati riconosciuti sicuri per l'approdo dei dati personali dei cittadini UE garantiscano nei fatti il livello di tutela che si sono impegnati a osservare per mezzo degli accordi.

Un impegno, questo, tutt'altro che formale se si considera che, nel caso la Commissione dovesse riconoscere la non corrispondenza tra il livello di protezione pattuito e le prassi operative vigenti nei paesi di destinazione, essa sarà tenuta a prenderne atto e a vietare i trasferimenti insicuri per poi eventualmente rinegoziare gli accordi non rispettati.

Difficile non notare in questa disposizione la traccia lasciata dalla sentenza C-362/14 e da tutta la diatriba seguita all'invalidamento del *Safe Harbor*.

D'altronde, l'acquisita consapevolezza che non sia sufficiente una tutela nominale dei diritti legati alla privacy ma che occorra invece garantirne una sicurezza effettiva e continuamente aggiornata è uno dei fattori caratterizzanti il nuovo regolamento nel suo complesso e pertanto non stupisce vederlo ribadito in un campo sensibile come il trasferimento internazionale di dati.

Il considerando n. 111 specifica invece che è possibile prevedere, previo consenso dell'interessato, un trasferimento dati se questo è "occasionale e necessario in relazione a un contratto o un'azione legale, che sia in sede giudiziale, amministrativa o stragiudiziale, compresi i procedimenti dinanzi alle autorità di regolamentazione".

Stessa possibilità viene accordata nel caso in cui sussistano motivi di "rilevante interesse pubblico" ovvero "se i dati sono trasferiti da un registro stabilito per legge e destinato a essere consultato dal pubblico o dalle persone aventi un legittimo interesse", pur nel rispetto del principio di proporzionalità, per cui il trasferimento potrà aver luogo nei limiti di quanto necessario per soddisfare l'interesse in questione.

Il concetto viene ribadito anche dal considerando n. 112, che precisa come i trasferimenti in deroga al regime ordinario dovrebbero essere accordati solo in ragione di importanti motivi di interesse pubblico oltre che quando sia giustificato dalla necessità di "salvaguardare interessi vitali dell'interessato o di un'altra persona, quali la vita e integrità fisica".

In queste ipotesi, qualora non vi sia già una decisione di adeguatezza, sarà il diritto dell'Unione o degli Stati membri a fissare espressamente limiti al trasferimento di categorie specifiche di dati verso paesi terzi e organizzazioni internazionali e a darne tempestiva comunicazione alla Commissione.

Sulla stessa scia si inserisce il considerando n. 116 il quale, cogliendo il rischio che con i trasferimenti internazionali di dati aumentino sia la difficoltà per una persona fisica nell'esercitare i propri diritti, sia quella delle Autorità di controllo nello svolgimento delle proprie indagini e nell'utilizzo dei propri poteri oltrefrontiera, sottolinea l'importanza di una forte cooperazione tra le Autorità di controllo nazionali.

Queste, se vorranno dare efficacia alla propria azione, dovranno lavorare in concerto e scambiarsi ogni informazione utile non solo all'interno dei confini dell'Unione ma anche con le Autorità analoghe esistenti in altri paesi, sulla base del principio di reciprocità.

Quanto esposto nei vari considerando trova puntuale trasposizione negli articoli del regolamento, la cui analisi consente anzitutto di segnalare alcuni obblighi riguardanti il titolare del trattamento.

Gli articoli 13 e 14 infatti, descrivono quali siano le informazioni che egli è tenuto a fornire all'interessato nel momento in cui acquisisce i suoi dati personali, sia presso l'interessato stesso (art. 13) sia in tutte le altre ipotesi (art. 14).

È un adempimento, questo, di primaria importanza per la correttezza e regolarità della raccolta e del successivo trattamento dei dati.

Fra le informazioni che si è tenuti a rendere vi è anche, secondo l'art. 13, par. 1, lett. f) e l'art. 14, par. 1, lett. f), "l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso dei trasferimenti di cui all'articolo 46 o 47, o all'articolo 49, paragrafo 1, secondo comma, il riferimento alle garanzie appropriate o opportune e i mezzi per ottenere una copia di tali garanzie o il luogo dove sono state rese disponibili" [163].

[163] Si vedano l'art. 13, par. 1, lett. f) e l'art. 14 par. 1, lett. f), del regolamento UE 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, le parole fra parentesi sono aggiunte per la migliore comprensione dei lettori.

L'art. 15, par. 2, invece, nel disciplinare il diritto di accesso, si preoccupa di statuire che nel caso in cui i dati personali siano trasferiti a un Paese terzo o a un'organizzazione internazionale, l'interessato ha il diritto di essere informato sulla sussistenza in quel Paese o organizzazione di garanzie adeguate, in accordo con le prescrizioni di cui all'art. 46.

Importante segnalare anche la previsione di limitazioni alla piena operatività del regolamento.

Spicca a tal proposito l'ipotesi descritta all'articolo 23, secondo il quale il nucleo di diritti riconosciuti agli interessati può essere compresso in presenza di una serie di situazioni elencate al primo paragrafo, attinenti alla salvaguardia di interessi pubblici[164].

Tale limitazione non può avvenire di certo in maniera arbitraria, e a tal fine è posto il carattere tassativo delle ipotesi previste, che devono comunque garantire "l'essenza dei diritti e delle libertà fondamentali" e la proporzionalità rispetto allo scopo da raggiungere.

A tal fine l'art. 23, par. 2 specifica che le eventuali azioni legislative dovranno prevedere la regolamentazione di determinati aspetti, quali le categorie di dati coinvolte, la portata

[164] Così recita l'articolo 23, par. 1: "*Limitazioni* – 1. Il diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o il responsabile del trattamento può limitare, mediante misure legislative, la portata degli obblighi e dei diritti di cui agli articoli da 12 a 22 e 34, nonché all'articolo 5, nella misura in cui le disposizioni ivi contenute corrispondano ai diritti e agli obblighi di cui agli articoli da 12 a 22, qualora tale limitazione rispetti l'essenza dei diritti e delle libertà fondamentali e sia una misura necessaria e proporzionata in una società democratica per salvaguardare:
a) la sicurezza nazionale;
b) la difesa;
c) la sicurezza pubblica;
d) la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica;
e) altri importanti obiettivi di interesse pubblico generale dell'Unione o di uno Stato membro, in particolare un rilevante interesse economico o finanziario dell'Unione o di uno Stato membro, anche in materia monetaria, di bilancio e tributaria, di sanità pubblica e sicurezza sociale;
f) la salvaguardia dell'indipendenza della magistratura e dei procedimenti giudiziari;
g) le attività volte a prevenire, indagare, accertare e perseguire violazioni della deontologia delle professioni regolamentate;
h) una funzione di controllo, d'ispezione o di regolamentazione connessa, anche occasionalmente, all'esercizio di pubblici poteri nei casi di cui alle lettere da a), a e) e g);
i) la tutela dell'interessato o dei diritti e delle libertà altrui;
j) l'esecuzione delle azioni civili".

delle limitazioni introdotte, i rischi per i diritti e le libertà degli interessati e le garanzie atte ad impedire "abusi, accessi e trasferimenti illeciti" (art. 23, par. 2, lett. d).

3.1 Il Capo V

Ad ogni buon conto, dato atto di questi richiami diffusi nel regolamento, la disciplina specifica della materia è fornita dal Capo V, espressamente dedicato al trasferimento dei dati personali verso paesi terzi o organizzazioni internazionali.

3.1.1. Il principio generale

Il Capo si apre con il principio generale espresso dall'art. 44, a rigore del quale, per dar luogo a trasferimenti di dati personali vero un Paese terzo o organizzazione internazionale occorre fare riferimento alla normativa contenuta nello stesso Capo V.

Agire al di fuori della cornice descrittavi significherebbe infatti eludere la tutela prevista per i diritti fondamentali delle persone i cui dati sono trattati e andare incontro, di conseguenza, a pesanti sanzioni.

Per quanto di interesse degli operatori, sarà importante comprendere a quali condizioni possa considerarsi lecito un trasferimento di dati personali, ed è una domanda cui gli articoli successivi si occupano di dare risposta.

3.1.2. Il trasferimento in base a una decisione di adeguatezza

In via generale, era stato osservato già all'indomani della pubblicazione della proposta, che "il regolamento agevola i responsabili del trattamento mediante la previsione di varie «zone di sicurezza» (*safe harbours*) nella forma di decisioni di adeguatezza, di un sistema semplificato di norme vincolanti d'impresa per le multinazionali, di clausole contrattuali approvate e di approvazioni individuali da parte dell'autorità di protezione dei dati" [165].

Anzitutto quindi, a norma dell'articolo 45, il trasferimento può avvenire in base ad una decisione di adeguatezza.

[165] Gruppo di lavoro articolo 29 per la Protezione dei dati, *Parere 01/2012 sulle proposte di riforma in materia di protezione dei dati*, 23 marzo 2012, p. 24.

Può infatti darsi la circostanza per cui la Commissione europea decida che un determinato Paese o organizzazione internazionale disponga di un impianto normativo capace di fornire un'adeguata tutela ai dati personali che ivi sono trasferiti.
La decisione viene presa sulla base degli elementi descritti all'art. 45, par. 2:

> "a) lo stato di diritto, il rispetto dei diritti umani e delle libertà fondamentali, la pertinente legislazione generale e settoriale (anche in materia di sicurezza pubblica, difesa, sicurezza nazionale, diritto penale e accesso delle autorità pubbliche ai dati personali), così come l'attuazione di tale legislazione, le norme in materia di protezione dei dati, le norme professionali e le misure di sicurezza, comprese le norme per il trasferimento successivo dei dati personali verso un altro paese terzo o un'altra organizzazione internazionale osservate nel paese o dall'organizzazione internazionale in questione, la giurisprudenza nonché i diritti effettivi e azionabili degli interessati e un ricorso effettivo in sede amministrativa e giudiziaria per gli interessati i cui dati personali sono oggetto di trasferimento;
> b) l'esistenza e l'effettivo funzionamento di una o più autorità di controllo indipendenti nel paese terzo o cui è soggetta un'organizzazione internazionale, con competenza per garantire e controllare il rispetto delle norme in materia di protezione dei dati, comprensiva di adeguati poteri di esecuzione, per assistere e fornire consulenza agli interessati in merito all'esercizio dei loro diritti e cooperare con le autorità di controllo degli Stati membri;
> c) gli impegni internazionali assunti dal paese terzo o dall'organizzazione internazionale in questione o altri obblighi derivanti da convenzioni o strumenti giuridicamente vincolanti come pure dalla loro partecipazione a sistemi multilaterali o regionali, in particolare in relazione alla protezione dei dati personali".

Pertanto, la Commissione può prendere atto di questo stato di cose assumendo atti di esecuzione che consentano e disciplinino, senza necessità di ulteriori autorizzazioni, il trasferimento di dati verso quel Paese o suoi specifici territori oppure verso un'organizzazione internazionale.
Si tratta senza dubbio dell'ipotesi più immediata e agevole per chi intenda effettuare trasferimenti, perché in buona sostanza non vi è alcun particolare onere in capo ai

soggetti coinvolti. Infatti, essendo già state svolte "a monte" le necessarie verifiche da parte della Commissione, ad essi non rimane che aderire alle procedure stabilite.

L'adozione di un atto di esecuzione tuttavia non costituisce un punto di non ritorno per quel che riguarda gli scambi di dati fra Unione europea e Stati terzi o organizzazioni internazionali.

Il nuovo regolamento, facendo tesoro delle criticità emerse in passato, insiste sulla necessità di aggiornare continuamente il giudizio speso ed eventualmente revocarlo qualora si dovesse appurare che la tutela fornita non sia più adeguata, ipotesi estrema ma espressamente prevista e disciplinata. Trattasi senza dubbio di un approccio evolutivo, che propone un'idea di tutela che diffida da una lettura meramente formale della normativa, prediligendo una verifica in concreto della sicurezza accordata ai dati dei cittadini.

A tal fine l'art. 45, par. 3 prevede anche un meccanismo di riesame periodico che, almeno ogni quattro anni, permetta di stabilire se debbano perdurare le condizioni poste alla base di un trasferimento dei dati.

Sul punto torna anche l'art. 97, sancendo che entro il 25 maggio 2020 si avrà la prima relazione della Commissione al Parlamento sull'applicazione e sul funzionamento delle decisioni adottate.

Tale relazione coinvolgerà anche gli accordi per il trasferimento di dati già stipulati in costanza della precedente direttiva, i quali in nulla vengono inficiati dall'entrata in vigore delle nuove norme, come espressamente previsto dall'art. 96.

Nella stessa ottica si inserisce l'art. 45, par. 4, che impone alla Commissione un controllo continuativo sugli sviluppi della situazione nei paesi terzi e nelle organizzazioni internazionali che potrebbero incidere sul funzionamento delle decisioni adottate al punto da portare ad una loro revisione, ipotesi disciplinata dal successivo quinto paragrafo, il quale dispone che, qualora ricorra questa circostanza, la decisione precedentemente presa possa essere revocata, modificata o sospesa dalla Commissione sempre mediante atti di esecuzione, per poi giungere alla rinegoziazione degli accordi venuti meno (art. 45, par. 6) e fatta salva la possibilità di fare uso degli strumenti previsti dal regolamento ed elencati agli articoli successivi (art. 45, par. 7).

La procedura descritta dall'articolo 45 rappresenta senza dubbio la soluzione migliore per operare un trasferimento di dati a livello internazionale e tuttavia ad essa si può fare ricorso solo qualora il trasferimento avvenga nei confronti di quei paesi e organizzazioni internazionali di cui la Commissione abbia giudicato positivamente il livello di protezione fornito ai dati personali che vi approdano.

Sul concetto di adeguatezza, poi, si è inserito anche il Gruppo di lavoro articolo 29, con il documento "Criteri di riferimento per l'adeguatezza".

Nel testo si specifica ancora una volta che ai fini di un corretto trasferimento di dati nei paesi terzi, il livello di adeguatezza richiesta si realizza quando le tutele sono di fatto le medesime che si avrebbero in Europa, anche se, naturalmente, gli strumenti giuridici messi a disposizione dagli ordinamenti possono essere diversi; non sarebbe infatti realistico aspettarsi una riproduzione della legislazione europea in materia di protezione dei dati mentre è importante verificare in concreto se il quadro complessivo che se ne ricava è in grado di assicurare garanzie tali essere equiparabili a quelle previste dal regolamento[166].

Le ipotesi descritte di seguito devono quindi essere lette in ottica sussidiaria rispetto alla disposizione dell'articolo 45, essendo opportuno farvi ricorso in assenza di una decisione di adeguatezza, tuttavia esse sono assai frequenti dal momento che, ad oggi, non sono molti i paesi e le organizzazioni che hanno ricevuto un così ampio *placet* della Commissione [167].

3.1.3. Il trasferimento soggetto a garanzie adeguate

L'articolo 46 disciplina allora il trasferimento soggetto a garanzie adeguate, stabilendo che in mancanza di una decisione di adeguatezza *ex* articolo 45, par. 3, sia comunque possibile effettuare un trasferimento di dati, previa concessione di idonee garanzie e sal-

[166] Gruppo di lavoro articolo 29, *Criteri di riferimento per l'adeguatezza,* 18/IT WP 254 rev.01, adottati il 28 novembre 2017, versione emendata e adottata il 6 febbraio 2018, cap. 1.

[167] Per quanto riguarda i paesi per i quali la Commissione si è espressa con una decisione di adeguatezza, essi sono: Andorra, Argentina, Canada, Faer Oer, Guernsey, Isola di Man, Israele, Jersey, Nuova Zelanda, Svizzera, Uruguay, nonché Australia e USA per quanto riguarda i dati relativi al PNR (*Passenger Name Record*). Per gli Stati Uniti, a seguito dell'annullamento del *Safe Harbor*, il trasferimento dati si attua, come visto, in base all'accordo *Privacy Shield*.

vaguardando la possibilità per interessati di avvalersi di rimedi giurisdizionali effettivi a garanzia dei propri diritti.

Questa possibilità rappresenta una valida alternativa per gli operatori, pubblici o privati, soprattutto in considerazione di quanto riferisce il secondo paragrafo ossia, che nel caso in cui sussistano determinate condizioni, non vi è necessità di alcuna autorizzazione da parte dell'Autorità di controllo.

Certamente le ipotesi che il legislatore europeo prende in considerazione sono senz'altro impegnative e confermano la volontà di vincolare il trasferimento alla sussistenza di tutta una serie di premure volte garantire sicurezza e tracciabilità dei dati.

Viene infatti effettuato un riferimento ad altre ipotesi disciplinate dal regolamento e precisamente a:

> "a) uno strumento giuridicamente vincolante e avente efficacia esecutiva tra autorità pubbliche o organismi pubblici;
> b) le norme vincolanti d'impresa in conformità dell'articolo 47;
> c) le clausole tipo di protezione dei dati adottate dalla Commissione secondo la procedura d'esame di cui all'articolo 93, paragrafo 2;
> d) le clausole tipo di protezione dei dati adottate da un'autorità di controllo e approvate dalla Commissione secondo la procedura d'esame di cui all'articolo 93, paragrafo 2;
> e) un codice di condotta approvato a norma dell'articolo 40, unitamente all'impegno vincolante ed esecutivo da parte del titolare del trattamento o del responsabile del trattamento nel paese terzo ad applicare le garanzie adeguate, anche per quanto riguarda i diritti degli interessati;
> f) un meccanismo di certificazione approvato a norma dell'articolo 42, unitamente all'impegno vincolante ed esigibile da parte del titolare del trattamento o del responsabile del trattamento nel paese terzo ad applicare le garanzie adeguate, anche per quanto riguarda i diritti degli interessati".

Spicca in questo elenco l'ipotesi disciplinata alla lettera d), cioè quella delle "clausole contrattuali tipo" di cui si è parlato precedentemente.

Nella nuova formulazione la Commissione, nell'adozione della propria decisione circa la validità delle stesse, viene assistita da un Comitato, secondo una procedura disciplinata all'art. 93.

Per converso, vi sono altre due ipotesi, descritte dal terzo paragrafo dell'art 46, che necessitano di una preventiva autorizzazione da parte dell'Autorità di controllo; si tratta di:

> "a) le clausole contrattuali tra il titolare del trattamento o il responsabile del trattamento e il titolare del trattamento, il responsabile del trattamento o il destinatario dei dati personali nel paese terzo o nell'organizzazione internazionale;
> b) le disposizioni da inserire in accordi amministrativi tra autorità pubbliche o organismi pubblici che comprendono diritti effettivi e azionabili per gli interessati"[168].

La necessaria autorizzazione da parte di un'Autorità di controllo dovrà osservare quanto stabilito dal meccanismo di coerenza di cui all'art. 63.
Quest'ultimo si sostanzia in una procedura preposta all'adozione di soluzioni uniformi e condivise a più livelli, in virtù della quale le Autorità di controllo sono chiamate a cooperare tra di loro ed eventualmente con la Commissione, seguendo un *iter* che contempla anche l'intervento del comitato europeo per la protezione dei dati, cui vengono affidati compiti di composizione delle controversie.
L'art. 46, par. 5 si preoccupa invece di chiarire l'efficacia *ex nunc* di queste disposizioni. Si stabilisce infatti che le autorizzazioni già rilasciate da uno Stato membro o da un'Autorità di controllo così come le decisioni già adottate dalla Commissione in ossequio alla normativa europea previgente non vengono revocate *ipso iure* ma rimangono in vigore fino ad una loro eventuale modifica da effettuarsi in base alle nuove norme.

3.1.4. Le norme vincolanti di impresa

Una delle ipotesi previste in tema di garanzie adeguate *ex* art. 46, par. 2 è quella delle norme vincolanti d'impresa, che sono più dettagliatamente disciplinate all'articolo 47.
Si è già dato conto delle caratteristiche fondamentali dell'istituto, che consiste di fatto in una nutrita regolamentazione rivolta alle imprese, le quali sono chiamate a rispettarla se intendono trasferire dati al di fuori dello spazio europeo ma pur sempre all'interno della

[168] Art. 46, par. 3, Regolamento (UE) 2016/679.

propria struttura aziendale, circostanza che si verifica soprattutto nelle aziende multinazionali.

A tal fine, l'art. 47, par. 1 prevede che l'Autorità di controllo competente debba concedere la propria autorizzazione, osservando la procedura del meccanismo di coerenza *ex* art. 63 e previa verifica della sussistenza di alcune condizioni: *in primis* che tali norme siano considerate vincolanti per le imprese che intendano trasferire dati all'interno del proprio gruppo imprenditoriale o gruppo di imprese svolgenti attività economica comune; in secondo luogo, che agli interessati siano riconosciuti dei diritti azionabili relativamente ai dati che vengono trattati e da ultimo che sia garantito il rispetto di tutta una serie di prescrizioni, elencate al successivo paragrafo secondo.

Il regolamento delinea infatti, all'art. 47, par. 2, un articolato impianto prescrittivo, la cui *ratio* sta, ancora una volta, nell'insufficienza del ricorso a generiche rassicurazioni da parte delle imprese, che devono invece sottostare a una serie di procedure che consentano di ridurre al minimo i rischi di violazione dei dati trasferiti. Se, infatti, la lettera d) obbliga l'impresa in questione ad applicare i principi generali in materia di protezione dei dati, la lettera e) sottolinea il diritto dell'interessato a non essere sottoposto a profilazione e salvaguarda la possibilità di proporre reclamo alle Autorità di controllo competenti nonché ricorso alle Autorità giurisdizionali degli Stati membri *ex* articolo 79. L'interessato, inoltre, ha diritto ad essere previamente informato di quanto previsto dalle norme vincolanti d'impresa, come già visto agli articoli 13 e 14.

Merita particolare attenzione, poi, il gravoso regime di responsabilità previsto dalla lettera f), per cui il titolare o il responsabile del trattamento stabilito nel territorio di uno Stato membro deve rispondere anche delle violazioni commesse in spregio delle norme vincolanti d'impresa da un membro del gruppo al di fuori dell'Unione, salvo dimostri la non imputabilità della violazione al membro del gruppo in questione.

Importante è anche la prescritta adozione di meccanismi che consentano di verificare il rispetto delle norme vincolanti d'impresa all'interno dei gruppi di imprese o del gruppo imprenditoriale e di comunicare le eventuali modifiche delle norme pattuite alle Autorità di controllo, come previsto rispettivamente all'art. 47, par. 2, lett. j) e lett. k).

Proprio nei confronti delle Autorità di controllo, le imprese sono chiamate a sviluppare un vero e proprio meccanismo di cooperazione, finalizzato a garantire l'uniforme rispetto delle norme vincolanti da parte di tutti i membri del gruppo (art. 47, par. 2, lett. l ed m).

Da ultimo, si sottolinea la disposizione della lett. n), che sancisce l'obbligo di prevedere una "appropriata formazione" per coloro che saranno chiamati a gestire i dati trasferiti, avendovi un accesso regolare o permanente. Tale disposizione rende ancora più evidente, se mai ce ne fosse stato bisogno, l'importanza che viene ad assumere la formazione specifica all'interno delle imprese.

Sempre in tema di norme vincolanti d'impresa, l'art. 47, par. 3 lascia comunque alla Commissione la facoltà di "specificare il formato e le procedure per lo scambio di informazioni tra titolari del trattamento, responsabili del trattamento e autorità di controllo in merito alle norme vincolanti d'impresa ai sensi del presente articolo", facoltà che, se esercitata, rende senz'altro più agevole il lavoro degli addetti.

3.1.5. Trasferimento o comunicazione non autorizzati dal diritto dell'Unione

Quelle appena descritte sono le ipotesi più frequenti e ordinarie, cionondimeno possono verificarsi altre situazioni particolari.

Anzitutto può darsi il caso, disciplinato dall'articolo 48, per cui non sia un'azienda a voler disporre il trasferimento di dati personali al di fuori dei confini dell'Unione, ma una sentenza di un'Autorità giurisdizionale o le decisioni di un'Autorità amministrativa straniera.

Ebbene, nonostante le evidenti ragioni pubblicistiche insite nell'attività di un organo giurisdizionale o amministrativo, il nuovo regolamento vieta la trasmissione dei dati in questione, a meno che lo Stato da cui proviene la richiesta non abbia convenuto con l'Unione o un suo Stato membro un accordo internazionale in questo senso.

Ad ogni buon conto, anche nel caso di accoglimento della domanda, questo tipo di trasferimento dovrà pur sempre sottostare ai requisiti generali previsti nel capo V.

3.1.6. Le deroghe in specifiche situazioni

Al di là di questa ipotesi, possono più frequentemente verificarsi casi di deroga al regolamento in presenza delle specifiche situazioni delineate all'articolo 49.

Ivi si stabilisce che, in assenza dei presupposti di cui agli articoli 45 e 46, è comunque possibile il trasferimento di dati verso Paese terzo o organizzazione internazionale nel solo caso in cui ricorra una delle seguenti ipotesi:

> "a) l'interessato abbia esplicitamente acconsentito al trasferimento proposto, dopo essere stato informato dei possibili rischi di siffatti trasferimenti per l'interessato, dovuti alla mancanza di una decisione di adeguatezza e di garanzie adeguate;
> b) il trasferimento sia necessario all'esecuzione di un contratto concluso tra l'interessato e il titolare del trattamento ovvero all'esecuzione di misure precontrattuali adottate su istanza dell'interessato;
> c) il trasferimento sia necessario per la conclusione o l'esecuzione di un contratto stipulato tra il titolare del trattamento e un'altra persona fisica o giuridica a favore dell'interessato;
> d) il trasferimento sia necessario per importanti motivi di interesse pubblico;
> e) il trasferimento sia necessario per accertare, esercitare o difendere un diritto in sede giudiziaria;
> f) il trasferimento sia necessario per tutelare gli interessi vitali dell'interessato o di altre persone, qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
> g) il trasferimento sia effettuato a partire da un registro che, a norma del diritto dell'Unione o degli Stati membri, mira a fornire informazioni al pubblico e può esser consultato tanto dal pubblico in generale quanto da chiunque sia in grado di dimostrare un legittimo interesse, solo a condizione che sussistano i requisiti per la consultazione previsti dal diritto dell'Unione o degli Stati membri"[169].

L'art. 49 prevede inoltre una formula di salvaguardia che prevede che in tutti quei casi nei quali occorra procedere ad un trasferimento di dati pur non ricorrendo alcuno dei requisiti previsti dal capo V, sarà necessario quantomeno far sì che il trasferimento: riguardi un numero limitato di interessati, non sia ripetitivo, sia necessario per il

[169] art. 49, par. 1 Regolamento (UE) 2016/679.

perseguimento degli interessi legittimi cogenti del titolare del trattamento, su cui non prevalgano gli interessi o i diritti e le libertà dell'interessato[170].

Nel procedere in tale ipotesi, il titolare del trattamento deve valutare tutte le circostanze relative al trasferimento e sulla base di tale valutazione fornire garanzie adeguate sulla protezione dei dati personali.

Inoltre, in ossequio a quanto previsto dal sesto paragrafo, il titolare o il responsabile del trattamento devono attestare la suddetta valutazione e le garanzie previste nel registro di cui all'art. 30 (registro delle attività di trattamento), informare del trasferimento l'Autorità di controllo ed informare l'interessato del trasferimento e degli interessi legittimi cogenti perseguiti, in aggiunta alle informazioni già prescritte dagli articoli 13 e 14[171].

Rilevante è poi il chiarimento operato dal quarto paragrafo, per cui per interesse pubblico deve intendersi quello riconosciuto tale "dal diritto dell'Unione o dal diritto dello Stato membro cui è soggetto il titolare del trattamento".

Inoltre, al paragrafo quinto, si stabilisce che, laddove non vi sia una decisione di adeguatezza, il diritto dell'Unione o dei singoli Stati può limitare il trasferimento di determinate categorie di dati, qualora ricorrano "importanti motivi di ordine pubblico"[172].

È facile immaginare che sarà necessaria una particolare vigilanza su questa disposizione, perché se da un lato si comprende la necessità di prevedere una disciplina anche a situazioni impreviste che potrebbero verificarsi, all'altra occorrerà evitare che tale apertura si presti ad abusi ed elusioni.

Ad ogni buon conto, per evitare che la formulazione dall'articolo 49 sia interpretata in maniera disomogenea o eccessivamente estensiva, il 25 Maggio 2018 l'European Data Protection Board[173] (Comitato Europeo per la protezione dei dati) ha emanato le

---

[170] Ibidem.

[171] Ibidem.

[172] È d'uopo ricordare che per importanti motivi di interesse pubblico, il diritto dell'Unione o degli Stati membri possono imporre dei limiti relativi a determinate categorie di dati, ricorrendo in questa circostanza il dovere degli Stati membri di notificare tale decisione alla Commissione (Cfr. art. 49, par. 5).

[173] L'European Data Protection Board è stato creato dal Regolamento europeo n. 679/2016, ove è disciplinato alla sezione terza del capo VII (Artt. 68 e ss.), per sostituire il Gruppo di lavoro articolo 29.

Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, con una serie di indicazioni relative alle modalità di applicazione della normativa in questione. Si tratta di indicazioni importanti perché sono volte ad evitare che l'art. 49 diventi il "tallone d'Achille" della maglia di tutele su cui si innesta il lecito trasferimento di dati oltre i confini europei attraverso un'interpretazione lassa delle fattispecie rientranti nel concetto di "deroghe", motivo per il quale l'E.D.P.B. ha raccomandato il ricorso ad un test preventivo che determini l'effettiva necessità di fare ricorso all'art. 49[174].

3.2. La cooperazione internazionale per la protezione dei dati personali

Un cenno deve essere fatto anche in tema di cooperazione internazionale per la protezione dei dati personali, che il regolamento disciplina all'articolo 50.

Ivi è stabilito che la Commissione e le Autorità di controllo, al fine di facilitare un'applicazione il più possibile transnazionale della legislazione in materia di protezione dei dati personali, sono chiamate ad adottare tutte le misure che ritengono appropriate per sviluppare "meccanismi di cooperazione internazionale" (art. 50, lett. a), nonché a prestarsi reciprocamente assistenza e scambiarsi informazioni, documentazioni e prassi in materia, coinvolgendo le parti interessate nei processi decisionali (art. 50, par. 1, lettere b e c).

Si deve sottolineare che quello della cooperazione sarà senza dubbio un banco di prova cruciale per comprendere l'effettiva capacità del nuovo pacchetto di protezione dei dati a rispondere alle problematiche odierne.

È persino banale infatti constatare che le singole Autorità di controllo, pur se valorizzate nei loro poteri e nella loro indipendenza dall'impianto del nuovo regolamento, potranno fare ben poco senza un proficuo scambio di informazioni in un'ottica di piena e trasparente collaborazione reciproca fra di loro e con le altre istituzioni dell'Unione e degli Stati membri.

---

[174] European Data Protection Board, *Linee guida 2/2018 sulle deroghe di cui all'articolo 49 del regolamento 2016/679,* Adottate il 25 maggio 2018, p. 5)

Le dimensioni odierne del problema della privacy sono tali che questa appare l'unica via percorribile per giungere ad un livello di tutela credibile, senza dimenticare per questo le diverse tradizioni giuridiche e sensibilità che caratterizzano i soggetti in gioco.
Il meccanismo di coerenza disciplinato dagli articoli 63 e ss. rappresenta una buona base di partenza per generare prassi giuridiche e decisioni che siano comuni ma per un più efficace sviluppo della cooperazione internazionale sarà importante anche monitorare il recepimento della direttiva 680 del Parlamento europeo e del Consiglio del 27 aprile 2016, anch'essa facente parte del nuovo "pacchetto di protezione dei dati" che si spera riesca ad implementare la condivisione di informazioni ed esperienze. Non v'è infatti chi non ne veda l'importanza davanti alle sfide politiche, economiche, sociali e di sicurezza che ci aspettano nei prossimi anni.

CAPITOLO V

I RISCHI PER LA PRIVACY NEL CONTESTO INTERNAZIONALE: LA TUTELA PENALE E IL RUOLO DEL D.P.O.

1. Circolazione internazionale dei dati: la sfida della sicurezza - 1.1 Le fonti della tutela penale dei dati - 1.2. Gli interventi di matrice europea - 1.3. Il costo del crimine informatico - 1.4. La strategia dell'unione Europea in materia di cybersicurezza - 2. Il quadro sanzionatorio - 2.1 I reati attinenti alla privacy nel codice penale - 2.2. I reati previsti dal Codice privacy a seguito delle modifiche apportate dal d.lgs. n. 101 del 10 agosto 2018 - 3. Risk Based Approach e D.P.O. 3.1 D.P.O. e Data Protection Impact Assestment - 3.2. D.P.O. e Data Breach - 4. Considerazioni conclusive

1. Circolazione internazionale dei dati: la sfida della sicurezza

Nel precedente capitolo sono state descritte le modalità attraverso le quali può avvenire il trasferimento internazionale di dati, lecitamente e in conformità con quanto disposto dal nuovo regolamento (UE) 2016/679.

Si tratta di un aspetto che si ritiene di grande importanza per un D.P.O. che dovrà, nell'espletare le sue mansioni, essere molto attento a questo profilo così delicato per una corretta protezione dei dati.

È evidente infatti che, se già non è cosa semplice garantire la sicurezza dei dati in un ambiente "noto" quale il territorio nazionale o il territorio dell'Unione, al cui interno sono comunque previste le medesime garanzie in fatto di *data protection*, ancora più difficile deve essere ottenere ed esercitare un controllo effettivo quando i dati non sono più nella immediata disponibilità del titolare e delle autorità dell'Unione o dei suoi Stati membri. È logico che in questi casi le suddette autorità, per quanto possano continuare a godere di forme di verifica della liceità dei trattamenti svolti al di fuori dei confini europei, non potranno più avere la medesima capacità di intervento e sorveglianza che sarebbero in grado di svolgere all'interno dei propri confini di competenza.

Ciò a maggior ragione se si considerano le minacce che sono insite nella, sempre più indispensabile, dimensione internazionale della circolazione dei dati.

Infatti, lasciare che si traferiscano dati in paesi dove il livello di sicurezza è inadeguato rappresenterebbe un'inutile vanificazione del percorso di riforma europeo e delle tutele previste dal nuovo corpus normativo e quindi un maggior rischio di violazioni e utilizzi illeciti a danno degli interessati.

Come detto più volte, internet ha azzerato le distanze e ha reso gli attacchi della criminalità molto più subdoli e sfuggenti.

Ad esempio, nel contesto odierno un attacco proveniente da un paese dell'estremo oriente può colpire un server nel continente americano e di conseguenza violare dati personali di cittadini europei che erano stati lì trasferiti, rendendo estremamente difficile, se non impossibile, recuperare lo *status quo ante* l'intervento illecito, i cui esiti possono, nella maggior parte dei casi, solo essere arginati.

Gli scopi che muovono gli agenti criminali possono essere i più disparati e la casistica relativa a reati che possono essere compiuti per mezzo di dati personali è giocoforza aperta, potendo ricomprendere numerose tipologie di illeciti: dalla sostituzione di persona, reato p. e p. ex art. 494 c.p., alla diffamazione aggravata p. e p. ex art. 595, c. 3 c.p., fino alle varie fattispecie truffaldine e financo ipotesi di estorsione di cui all'art. 629 c.p.

Il vorticoso sviluppo tecnologico, d'altronde, fa sì che le reti di sicurezza predisposte per tutelare banche dati e informazioni riservate, debbano essere continuamente aggiornate per rispondere efficacemente agli assalti dei criminali informatici; a tal proposito si assiste a una continua rincorsa fra gli sviluppatori dei sistemi di sicurezza e le organizzazioni criminali.

In questo contesto, anche la risposta penale dovrebbe essere pensata in un'ottica transnazionale.

Beninteso, possono senz'altro avvenire, come in effetti avvengono, episodi criminosi in relazione ai dati personali che non implicano l'utilizzo di tecnologie informatiche o che comunque che non coinvolgono necessariamente soggetti situati in paesi e continenti diversi, tuttavia è innegabile che nell'attuale contesto operativo, qualsiasi tipo di

violazione, anche la più "banale", è suscettibile di essere moltiplicata esponenzialmente per mezzo delle tecnologie di comunicazione e quindi di rendere i dati violati accessibili praticamente in qualsiasi parte del mondo.
Inoltre, e soprattutto, la necessità di un approccio internazionale alla tutela dei dati si rende necessario perché, in prospettiva futura, è questo il fronte di maggiore sensibilità se si vuole assicurare una compiuta tutela delle persone e un'effettiva sicurezza sia dei singoli che delle collettività; è infatti da questo tipo di illeciti che discendono i danni più rilevanti a livello economico e sociale.

1.1 Le fonti della tutela penale dei dati

Il tema è senza dubbio di grande attualità ma non è certo nuovo nel panorama giuridico che già da tempo affronta la questione.
Il primo apporto normativo rilevante in Italia è rappresentato dalla l. n. 547 del 1993, non a caso introdotta negli stessi anni in cui si lavorava alla direttiva 95/46/CE; si era infatti nel periodo in cui la diffusione delle nuove tecnologie diveniva sempre più capillare e si iniziava ad avvertire l'esigenza di una difesa nei confronti delle azioni illecite compiute attraverso di esse.
La legge in commento ha avuto il merito di introdurre nel codice penale un corpus di reati caratterizzati dal fatto di essere tipicamente messi in atto attraverso strumenti informatici.
Invero, al quadro della disciplina italiana andrebbe aggiunta la l. 269/1998, *Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori, quali nuove forme di riduzione in schiavitù*, che allo scopo di tutelare i minori ha esteso il campo di applicazione della tutela penale anche alle attività svolte telematicamente, in particolare con riferimento all'art. 600-ter; sul punto sono intervenute successive modifiche, la più rilevante delle quali ad opera della l. n. 172 del 1 ottobre 2012, che ha ratificato la Convenzione di Lanzarote del 2007.
Si tratta, ad onor del vero, di ipotesi che ledono in primo luogo la dignità, la libertà e lo sviluppo del minore, tuttavia non si devono sottovalutare anche gli aspetti legati alla tutela dei dati in sé e per sé in quanto, per coloro che sono state vittime di queste condotte

particolarmente abiette, ristabilire e conservare la propria privacy, anche rimuovendo dalla rete e dagli altri canali di comunicazione qualsiasi dato che testimoni le violenze subite, costituisce parte integrante di una tutela completa e duratura nel tempo.

D'altronde questo ambito criminale è fra quelli che più si è giovato, purtroppo, dell'avvento delle tecnologie di comunicazione digitale, anche al fine di ampliare l'orizzonte delle condotte illecite in una dimensione sovranazionale.

Ad ogni buon conto, se si considera il quadro descritto, ben si coglie la preoccupazione del legislatore, che già negli anni '90 si trovava a confrontarsi con la vulnerabilità dei dati personali che venivano raccolti in sistemi dalle capacità sempre maggiori.

Si era ben consci del rischio che tali dati potessero sia costituire l'oggetto su cui ricadeva la condotta illecita, sia, qualora fossero caduti nelle mani sbagliate, diventare a loro volta strumenti per la realizzazione di ulteriori attività criminose; l'*appeal* che questo tipo di informazioni suscitava nei confronti dei malintenzionati era già notevole.

Certamente la normativa descritta dotava l'Italia di un valido apparato sanzionatorio per la prima metà degli anni '90, ma se si pensa che nel giro di una decade internet, dall'essere una novità nelle mani di pochi esperti è divenuto strumento ordinario e indispensabile utilizzato da chiunque, manifestando sin da subito la sua capacità di annullare il concetto tradizionale di "distanza" nel settore delle comunicazioni, si comprende facilmente il motivo per cui si è avvertita l'esigenza di un coordinamento fra i vari ordinamenti nazionali, chiamati a fronteggiare un fenomeno che poneva questioni sino ad allora inedite, soprattutto nel campo dell'individuazione e della repressione dei fenomeni criminali.

Tale esigenza è poi sfociata nella Convenzione di Budapest sul cybercrime del 21 novembre 2001, ratificata in Italia con legge n. 48 del 18 marzo 2008, che a sua volta ha introdotto il reato di cui all'art. 635-ter, *Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità* e all'art. 635-quater *Danneggiamento di sistemi informatici o telematici*, oltre ad aver apprestato modifiche rilevanti agli artt. 491-bis e 615-quinquies c.p.

La convenzione rappresenta un passo importante sotto molteplici aspetti perché, se da un lato ribadisce la centralità del principio di territorialità, dall'altra sottolinea la

necessità di individuare regole sovranazionali riconosciute unanimemente e una cooperazione fra polizia e autorità giurisdizionali dei diversi paesi.

Il crescente sviluppo e perfezionamento di prassi criminali rendeva infatti necessario organizzare modalità di investigazione e di repressione dei reati in un'ottica che andasse anche al di fuori dei confini dei singoli stati.

Da questo punto di vista, la Convenzione di Budapest è rilevante perché non ha coinvolto solo paesi europei ma anche da paesi che non sono membri del Consiglio d'Europa, fra cui Australia, Stati Uniti e Giappone.

Per contro, pur sottolineando l'importanza dei fini perseguiti, è stata criticata la genericità delle disposizioni[175] e il fatto che di essa non è stata data, ancora oggi, piena ratifica negli ordinamenti dei vari stati membri[176].

1.2. Gli interventi di matrice europea

Nel frattempo, anche le istituzioni della Comunità Europea si stavano muovendo sulla base delle stesse premesse[177], con una serie di iniziative che sfoceranno poi nella decisione quadro 2005/222/GAI del 24 febbraio 2005.

Si tratta di una decisione importante, che sin dai *considerando* introduttivi sottolinea l'esigenza di creare uno spazio di tutela di ampio respiro in Europa.

Vengono particolarmente in rilievo infatti l'obiettivo di "migliorare la cooperazione tra le autorità giudiziarie e le autorità competenti degli Stati membri"[178], la consapevolezza che "Il carattere transnazionale e senza frontiere dei moderni sistemi di informazione fa sì che gli attacchi contro tali sistemi siano spesso di natura transnazionale"[179] e quindi

---

[175] Cfr. Colombo E., *Una novità dall'unione europea per la lotta ai cybercrimes: una electronic evidence guide A Novelty from the European Union on the Fight against Cybercrimes: An Electronic Evidence Guide* in "Cassazione Penale", fasc.1, 2014, p. 377.

[176] L'elenco dei Paesi firmatari e di quelli che hanno ratificato la correzione è disponibile, continuamente aggiornato, alla pagina dedicata sul sito istituzionale del Consiglio d'Europa (https://www.coe.int/it/web/portal/home).

[177] Cfr. Commissione Europea, *Creare una società dell'informazione sicura migliorando la sicurezza delle infrastrutture dell'informazione e mediante la lotta alla criminalità informatica.* eEurope 2002 (COM(2000)890), 26 gennaio 2001.

[178] Consiglio dell'Unione Europea, *Decisione quadro 2005/222/GAI del Consiglio, del 24 febbraio 2005, relativa agli attacchi contro i sistemi di informazione*, 24 febbraio 2005, Considerando 1.

[179] Ivi, Considerando 5.

che "Le legislazioni penali nel settore degli attacchi ai danni di sistemi di informazione dovrebbero essere ravvicinate al fine di garantire la cooperazione giudiziaria e di polizia più ampia possibile"[180].

Presa consapevolezza che il fenomeno del cybercrime ha caratteristiche tali da rendere necessaria una tutela organizzata su scala internazionale, e che quindi vi è la necessità di addivenire a una tendenziale uniformità degli ordinamenti nazionali e alla cooperazione fra le varie forze di polizia, la decisione interviene in particolar modo sull'aspetto relativo ai criteri per stabilire la legislazione applicabile, enucleati nell'articolo 10. Ivi si stabilisce che, per individuare la competenza giurisdizionale, occorra considerare il luogo di commissione del reato, la cittadinanza dell'autore o la sede della persona giuridica che ha beneficiato dell'evento illecito.

Gli Stati, inoltre, avrebbero provveduto a disciplinare l'ipotesi in cui l'autore avesse commesso il reato nel territorio nazionale, indipendentemente dal fatto che anche il sistema oggetto di attacco fosse situato in quel territorio o ,per converso, il caso in cui il reato fosse commesso ai danni di un sistema sito all'interno del proprio territorio nazionale da un agente che si trovi al di fuori di esso[181].

In seguito, si è avuta l'adozione della Direttiva 2013/40/UE, attuata in Italia per mezzo di numerosi interventi legislativi[182]; tale direttiva ha sostituito la precedente decisione quadro, testè descritta.

Pur non rappresentando una rivoluzione, la direttiva ha ridefinito alcune fattispecie di reato, rendendone più rigida la disciplina[183].

Invero, nell'arco dello stesso anno, quel che più appare rilevante è l'istituzione del Centro europeo per la lotta alla criminalità informatica, operante all'interno

---

[180] Ivi, Considerando 8.

[181] Ivi, Considerando 10.

[182] L'elenco delle normative che hanno dato attuazione alla direttiva è disponibile nella pagina dedicata all'interno del sito https://eur-lex.europa.eu.

[183] Si pensi all'obbligo, per gli Stati di dare rilevo penale all'intercettazione illecita o alla previsione della reclusione per coloro che producono software strumentali alla commissione di reati informatici; sul punto Cfr. Conigliaro S. C., *La nuova tutela penale europea dei sistemi di informazione. Una prima lettura della direttiva 2013/40/UE del Parlamento europeo e del Consiglio*, in "Diritto penale contemporaneo", 30 ottobre 2013, (https://www.penalecontemporaneo.it/d/2588-la-nuova-tutela-penale-europea-dei-sistemi-di-informazione), ultima cons. 26.ottobre 2018.

dell'Europol. Si tratta di un'iniziativa che si inserisce nel solco della strategia di sicurezza che l'Unione aveva già iniziato nel 2010 e che individuava nell'infrastruttura informatica uno degli asset maggiormente esposti ad azioni illecite e dannose[184].

Il Centro è tutt'ora di fondamentale importanza nell'attività di contrasto alla criminalità informatica internazionale, svolge un'articolata attività di contrasto ai fenomeni illeciti della rete, riportata da un'importante attività di documentazione.

D'altronde, l'allerta nei confronti del fenomeno dei *computer crimes* è in continuo aumento e le tipologie di attacchi vanno articolandosi in varie direzioni.

Nella sua relazione *Relazione sulle possibili implicazioni e minacce per la sicurezza nazionale derivanti dallo spazio cibernetico* del 7 agosto 2010, il Co.pa.si.r. aveva già individuato alcune macrocategorie di attacchi cibernetici: "cyber-crime", "cyber terrorism", "cyber espionage", "cyber war"[185].

Si tratta della stessa classificazione che, qualche anno più tardi, sarà adottata anche nel *Quadro strategico nazionale per la sicurezza dello spazio cibernetico*[186] della Presidenza del Consiglio dei Ministri.

---

[184] Cfr. Commissione Europea, *Comunicazione della commissione al parlamento europeo e al consiglio La strategia di sicurezza interna dell'UE in azione: cinque tappe verso un'Europa più sicura*, Bruxelles, 22.11.2010 COM (2010) 673 definitivo, p. 4.

[185] La relazione, a p. 17, fornisce le seguenti definizioni:

"1) *cyber-crime*: ovvero l'insieme delle minacce poste da organizzazioni criminali nazionali o transnazionali, le quali sfruttano lo spazio cibernetico per reati quali la truffa, il furto d'identità, la sottrazione indebita di informazioni o di creazioni e proprietà intellettuali;

2) *cyber terrorism*: ovvero l'utilizzo della rete da parte delle organizzazioni terroristiche, a fini di propaganda, denigrazione o affiliazione. Particolarmente significativo è il caso della cyber-propaganda, ovvero della manipolazione delle informazioni veicolate nella rete a fini di denigrazione e delegittimazione politica, discriminazione sociale o personale. Nei casi estremi, si intende ipotizzare l'utilizzo sofisticato della rete internet o dei controlli telematici per mettere fuori uso, da parte di organizzazioni terroristiche, i gangli di trasmissione critica delle strutture o dei processi che attengono alla sicurezza nazionale;

3) *cyber espionage*: ovvero l'insieme delle attività volte a sfruttare le potenzialità della rete per sottrarre segreti industriali a fini di concorrenza sleale (se consumati nel mercato dei brevetti civili) o di superiorità strategica (nel caso di sottrazione di disegni e apparecchiature militari o dual-use);

4) *cyber war*: ovvero lo scenario relativo ad un vero e proprio conflitto tra Nazioni, combattuto attraverso il sistematico abbattimento delle barriere di protezione critica della sicurezza dell'avversario, ovvero attraverso il disturbo o lo «spegnimento» delle reti di comunicazione strategica, e l'integrazione di queste attività con quelle propriamente belliche.".

[186] Presidenza del consiglio dei Ministri, *Quadro strategico nazionale per la sicurezza dello spazio cibernetico*, Roma, Dicembre 2013, pp. 12-13.

Nell'ultimo decennio infatti, con l'aumentare non solo del fenomeno criminale sulla rete ma anche degli attacchi di tipo terroristico nell'ambiente online e del fenomeno diffuso dello spionaggio informatico, ogni paese ha avvertito in modo significativo la necessità di proteggere le proprie infrastrutture strategiche sia pubbliche che private dotate di rilevante valore per gli interessi nazionali, oltre ai propri asset industriali ed economici e quindi anche le aziende più importanti e rappresentative.

È evidente infatti che le modalità di condurre conflitti su scala mondiale oggi sono cambiate e possedere le capacità di difendere il proprio patrimonio di informazioni e di dati è giustamente considerato un modo di difendere la propria posizione all'interno del delicato equilibrio geopolitico del nuovo millennio.

Da questo punto di vista, nel nostro paese la situazione è resa più complessa dal fatto che il tessuto economico è costituito per la gran parte da piccole e medie imprese.

Sì e soliti pensare che bersaglio dei cyber attacchi siano le grandi aziende, le quali sicuramente ne subiscono in maniera significativa, tuttavia sarebbe sbagliato concentrarsi solo su di esse perché, in realtà, le imprese di ridotte dimensioni costituiscono comunque un deposito altrettanto importante ed appetibile di dati, visto il loro numero elevato e le difese generalmente assai meno sviluppate di cui dispongono. Non bisogna poi dimenticare che spesso è proprio grazie alla violazione dei sistemi di questo tipo che si riesce a inibire la sicurezza di aziende e strutture di grandi dimensioni[187]

In un mondo interconnesso sono interconnesse anche le informazioni e pertanto occorre sapere bene cosa si condivide, con chi e dove, proprio perché in molti casi basta un singolo punto debole per penetrare anche le difese più strutturate.

[187] A titolo di esempio, nel 2013 i clienti di una grande catena di supermercati degli Stati Uniti avevano subito la clonazione di 40 milioni di carte di credito; in quel caso la violazione del sistema di sicurezza era stata resa possibile per mezzo dei dati di un fornitore finiti in mano ai criminali, che li hanno usati per avere accesso alla banca dati della grande azienda. Cfr. Zappa F., *La criminalità informatica e i rischi per l'economia e le imprese a livello italiano ed europeo*, Progetto di ricerca per United Nations Interregional Crime and Justice Research Institute (UNICRI), 2014, (http://www.unicri.it/in_focus/files/Criminalita_informatica_def.pdf), p. 17.

Queste considerazioni portano a ribadire l'importanza di seguire scrupolosamente la normativa descritta dal regolamento, in particolare per quel che riguarda il trasferimento di dati all'estero.

Nel procedere a questo tipo di operazioni occorre infatti prestare attenzione a che siano veramente assicurate le garanzie previste dal regolamento, altrimenti il rischio che si corre è quello di generare un "anello debole" nella catena di sicurezza dei dati.

1.3. Il costo del crimine informatico

I costi del cybercrime sono molto pesanti per stati e aziende; secondo uno studio del Ponemon Institute[188] il costo medio del cybercrime dei principali paesi occidentali presi come riferimento[189] è stato di 11,7 milioni di dollari per il 2017, in esponenziale crescita rispetto ai 9,5 del 2016 e ai 7,7 del 2015.

Ancora, per avere un'idea dell'entità del fenomeno e delle sue ripercussioni sull'economia mondiale e sulla sicurezza dei dati basti pensare che, stando all'ultimo rapporto Clusit, il 2017 deve essere considerato quale *annus horribilis* per quel che riguarda i cyberattacchi[190] e più in generale, nel periodo 2011-2017, i costi sostenuti da soggetti pubblici e privati a causa di questo tipo di attività criminali è aumentato esponenzialmente, passando da 100 a 500 milioni di dollari circa[191].

Per quanto riguarda le cyberminacce, occorre tener presente che secondo i dati del C.N.A.I.P.I.C.[192], gli *alert* riguardanti "infrastrutture critiche nazionali" sono quasi quintuplicati rispetto all'anno 2016, attestandosi a quota 31.524[193], nello stesso periodo il centro ha gestito 1.032 attacchi contro siti internet istituzionali di enti pubblici.

---

[188] Cfr. Ponemon Institute, *Cost of cyber crime study 2017 insights on the security investments that make a difference*, Independently conducted by Ponemon Institute LLC and jointly developed by Accenture, Michigan, 2017, p. 12.

[189] Lo studio è stato condotto in relazione ad aziende di sette paesi: Australia, Francia, Germania, Italia, Giappone, Regno Unito e Stati Uniti.

[190] Cfr. Clusit – Associazione italiana per la sicurezza informatica, *Rapporto Clusit 2018 sulla sicurezza ICT in Italia, nuova edizione settembre 2018*, Milano, 2018, p. 10.

[191] Cfr. Ivi, p. 11.

[192] Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche

[193] Cfr. Clusit – Associazione italiana per la sicurezza informatica, *Rapporto Clusit 2018 sulla sicurezza ICT in Italia,* op.cit, p. 47.

Per quanto concerne invece il cybercrime di tipo finanziario, settore nel quale la criminalità si giova di tecniche sempre più raffinate, le forze di polizia sono riuscite a bloccare ben 20.839.576 euro sottratti indebitamente e pronti per essere destinati verso paesi rispetto ai quali sarebbe stato arduo qualsiasi tentativo di recupero[194].

1.4. La strategia dell'unione Europea in materia di cybersicurezza

Non sorprende allora che l'Unione Europea abbia avvertito la necessità, nel 2017, di dare luogo a una nuova riforma della cybersicurezza; si tratta in fin dei conti di un risvolto del nuovo pacchetto di protezione dati approvato nel 2016.

Al Consiglio d'Europa del 19 e 20 ottobre 2017 è emersa la necessità di implementare questo aspetto, partendo dalla consapevolezza che "il mondo digitale richiede fiducia, e questa può essere ottenuta solo se garantiamo una sicurezza maggiormente proattiva sin dalla progettazione in tutte le politiche digitali, forniamo adeguate certificazioni della sicurezza di prodotti e servizi e aumentiamo la nostra capacità di prevenire, dissuadere e individuare gli attacchi informatici e di rispondere ad essi"[195].

La nuova strategia delle istituzioni comunitarie si fonda su alcuni elementi fondamentali: deterrenza, cooperazione pubblico-privato, implemento della capacità di risposta della diplomazia, cooperazione esterna con i partner e le altre organizzazioni attive su questi temi[196], oltre alla previsione di una certificazione unica a livello europeo in tema di cybersicurezza[197], da realizzarsi con il sostegno dell'E.N.I.S.A.[198] che garantisca il rispetto di standard elevati ed uniformi in tutta l'Unione.

---

[194] Cfr. Ivi, p. 48.

[195] Consiglio Europeo, Conclusioni del Consiglio Europeo del 19.10.2017, (OR. en) EUCO 14/17 CO EUR 17 CONCL 5, Bruxelles, 19 ottobre 2017, p. 6.

[196] Cfr. Proli R., Valguarnera E., *Il Cybercrime e le strategie dell'Unione Europea*, in "Il diritto penale della globalizzazione", 28.08.2018, (http://www.dirittopenaleglobalizzazione.it/wp-content/uploads/2018/08/Il-Cybercrime-e-le-strategie-dell%E2%80%99Unione-Europea-1.pdf), ultima cons. 13.10.2018.

[197] Commissione Europea - Alto Rappresentante dell'Unione per gli affari esteri e la politica di sicurezza, JOIN (2017) 450 FINAL, *comunicazione congiunta al parlamento europeo e al consiglio Resilienza, deterrenza e difesa: verso una cibersicurezza forte per l'UE*, Bruxelles, 13.9.2017 par. 2.2.

[198] Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione.

Solo in questo modo, cioè attraverso l'instaurazione di una sicurezza unica, si potrà dar luogo all'obbiettivo finale delle istituzioni, che è quello è di creare un mercato unico[199] digitale in Europa.

In sintesi, ben si può dire che le esigenze di sicurezza vengono realizzate grazie a una protezione a più livelli: in primo luogo a livello internazionale, con trattati e strumenti di collaborazione fra le autorità investigative e in secondo luogo con le politiche condotte dalle istituzioni europee e nazionali.

Da questo punto di vista, un importante contributo viene dalla Direttiva 2016/680, recepita in Italia con d.lgs. n. 51/2018, che mira proprio a rafforzare la collaborazione in ambito europeo nell'attività di repressione dei reati.

Se ne evince che il ruolo delle istituzioni sia centrale, tuttavia il Regolamento UE 2016/679 sembra voler introdurre un ulteriore, fondamentale, livello di tutela diffusa.

La logica ivi descritta infatti sembra suggerire che buona parte del lavoro debba essere svolto alla base di questa piramide: nelle decine di migliaia di aziende, piccoli enti pubblici e studi professionali dove passano e vengono trattati, in buona sostanza, la gran parte dei dati.

È lì che è urgente generare prassi virtuose, che sappiano da un lato creare fiducia nei cittadini e dall'altro alimentare una nuova economia che si basi su di un utilizzo lecito e consapevole dei dati personali.

Ecco quindi che, in siffatto sistema, viene in auge la centralità della figura del Data Protection Officer quale soggetto capace di conoscere i rischi ma soprattutto di trovare la via per scongiurarli, essendo in grado di fornire la corretta lettura del rapporto fra la sicurezza dei dati e il loro utilizzo.

---

[199] Sul punto sono già attive impegnative politiche a livello europeo, quali l' abolizione delle tariffe di roaming nell'UE (Cfr. Council of the EU, Comunicato Stampa 360/17 *End of roaming charges in the EU: Joint statement by the European Parliament*, Bruxelles, 14 giugno 2017), la Portabilità dei servizi digitali (Cfr. Consiglio dell'Unione Europea, Comunicato stampa 332/17, *Portabilità dei servizi digitali nell'UE: il Consiglio adotta nuove norme*, Bruxelles, 8 Giugno 2017), il regolamento che rimuove gli ostacoli al commercio elettronico (il regolamento in questione è il Regolamento (UE) 2018/302; Cfr. Consiglio dell'Unione Europea, Comunicato stampa 95/18, *Blocchi geografici: il Consiglio adotta un regolamento che rimuove gli ostacoli al commercio elettronico*, Bruxelles, 27 febbraio 2018).

2. Il quadro sanzionatorio

Ad ogni buon conto, in attesa che si concretizzino ulteriori sviluppi a livello europeo, vale la pena ribadire brevemente quale sia, nell'attuale contesto normativo, il novero dei reati che sono connessi con la tutela dei dati e la loro sicurezza.

Vengono in rilievo *in primis* tutte quelle fattispecie presenti all'interno del codice penale che, pur se attengono alla tutela di beni giuridici diversi, sono strettamente connesse alla tutela dei dati personali.

Inoltre, devono essere menzionati i reati previsti e puniti proprio dal codice privacy, d. lgs. 196/2003, per come recentemente novellato dal d.lgs. n. 101/2018.

La conoscenza di questi aspetti relativi alla materia penale deve essere presente al D.P.O. perché, nello svolgere le proprie funzioni di consulenza, assistenza e sorveglianza, egli dovrà certamente prestare attenzione ai profili di rischio sui quali possono innestarsi le principali fattispecie di reato in ambito di privacy e, conseguentemente, rilevare e segnalare eventuali aspetti critici presenti nella struttura affidata alla sua attenzione.

Ciò soprattutto se si considera che, in attesa che si sviluppi una giurisprudenza chiarificatrice, il D.P.O. potrebbe non solo essere chiamato ad assistere il titolare da questo punto di vista ma addirittura venire coinvolto in eventuali illeciti in qualità di titolare di una posizione di garanzia.

2.1 I reati attinenti alla privacy nel codice penale

All'interno del Codice Penale i reati in questione sono contenuti prevalentemente, ma non esclusivamente, nel Libro II, titolo XII capo III sezione 4 e 5.

Non tutti, naturalmente, attengono alla dimensione *on-line*; non è così ad esempio per i reati previsti e puniti dagli articoli 614 e 615 c.p., che costituiscono il nucleo originario di tutela penale di quel diritto alla riservatezza che si sostanzia nello *ius excludendi alios*, a prescindere dal fatto che il soggetto escluso sia un privato o un pubblico potere.

A mezza via, per così dire, si pone l'articolo 615 bis c.p., *Interferenze illecite nella vita privata*, che punisce le condotte indiscrete volte a ottenere "notizie o immagini" relativi all'ambito domiciliare e la rivelazione o diffusione delle stesse al pubblico.

Da questo punto di vista è evidente che l'introduzione dell'articolo in questione, ad opera dell'art. 1 della l. n. 98/1974, sia andato a colmare un vuoto normativo dato dalla mancanza di una tutela penale della riservatezza domiciliare, che in quegli anni era stata già riconosciuta dall'ordinamento italiano a seguito della sentenza n. 2129 del 1975 della Cassazione e rispetto alla quale incontrano un limite altri diritti costituzionalmente garantiti[200].

Si intendeva così tutelare il contesto relazionale personale e la propria immagine nell'ambito privato; tale finalità è ancora pienamente attuale dato che i mezzi di comunicazione odierni hanno aumentato esponenzialmente la capacità di diffusione illecita che l'articolo in commento intende reprimere.

L'articolo 615 ter, *Accesso abusivo a un sistema informatico o telematico*, è invece figlio a pieno titolo dell'evoluzione del settore informatico; è stato introdotto dall'art. 4 della l. 547/1993 e rappresenta una delle fattispecie più complesse e pertinenti al tema della privacy, specie se affrontato in un'ottica internazionale, visto il fenomeno sempre più incisivo della pirateria informatica.

La norma incrimina chiunque si introduca illecitamente all'interno di un sistema, sia che la condotta avvenga "fisicamente" che a distanza, per mezzo di strumenti tecnologici, ed è ovvio che quest'ultima ipotesi sia quella più frequente in termini assoluti.

Dal punto di vista dell'interesse tutelato dal reato in commento, inizialmente si è ritenuto che non si trattasse d'altro che di una nuova declinazione del concetto tradizionale di domicilio.

Una soluzione del genere, tuttavia, è ben presto apparsa riduttiva, al punto che anche in giurisprudenza si è progressivamente affermata l'idea di una autonoma nozione di "domicilio informatico"[201], più ampia e capace di accogliere le diverse sfaccettature del

---

[200] Cfr. Monaco L., *sub 615 c.p.*, in Crespi A., Forti G., Zuccala G. *commentario breve al codice penale – complemento giurisprudenziale*, Wolters Kluwer, Cedam, Assago, Padova, 2014, p. 2512.

[201] Con riferimento alla nozione di "domicilio informatico", giova richiamare Cass. pen. sez. V, n. 42021/2012: che al punto 2 afferma: "l'art. 615 ter cod. pen. non si limita a tutelare solamente i contenuti personalissimi dei dati raccolti nei sistemi informatici protetti, ma offre una tutela più ampia che si concreta nello "jus excludendi alios", quale che sia il contenuto dei dati racchiusi in esso, purchè attinente alla sfera di pensiero o all'attività, lavorativa o non, dell'utente; con la conseguenza che la tutela della legge si estende anche agli aspetti economico-patrimoniali dei dati, sia che titolare dello "jus excludendi" sia persona fisica, persona giuridica, privata o pubblica, o altro ente (Sez. 6, n. 3067

problema, in particolare del mutato rapporto fra l'uomo e l'ambiente di cui si serve per esprimere e sviluppare la propria personalità ed esercitare i propri diritti.

Questa strumentalità, già valida in relazione al concetto di domicilio tradizionale, vale anche con riferimento al domicilio informatico, soprattutto se si prende in considerazione quanta parte della vita relazionale e professionale si svolge oggi nella dimensione *online*.

Ne discende che "nella fattispecie dell'accesso abusivo può considerarsi titolare dello *ius excludendi* colui che attualmente e legittimamente abbia scelto il sistema informatico come ambito all'interno del quale proiettare la propria personalità e trasferire i propri interessi e per questo abbia interesse all'integrità dello stesso, prescindendo dalla titolarità di eventuali diritti reali vantati sul sistema informatico."[202]

Con riferimento invece all'oggetto della tutela, va rilevato quanto recepito dalla Cassazione:

> "l'espressione 'sistema informatico' contiene in sè il concetto di una pluralità di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, attraverso l'utilizzazione (anche in parte) di tecnologie informatiche. Le linee telefoniche utilizzano, nell'epoca moderna, normalmente, tali tecnologie; la funzione di trasmissione delle comunicazioni si attua, invero, con la conversione (codificazione) dei segnali (nel caso, fonici) in forma di flusso continuo di cifre (bit) e nel loro trasporto in tale forma all'altro estremo, dove il segnale di origine viene ricostruito (decodificazione) e inoltrato, dopo essere stato registrato in apposite memorie. Si tratta, cioè, del flusso di comunicazioni relativo ai sistemi informatici di cui all' art. 266 bis c.p.p., introdotto dalla stessa l. n. 547 del 1993"[203].

---

del 4.10.1999, rv 214946)."; Cfr. anche Monaco L., *sub 615 ter c.p*, in *commentario breve al codice penale*, op. cit., p. 2515.

[202] Galdieri P. *Il domicilio informatico: l'interpretazione dell'articolo 615-ter c.p. tra ragioni di carattere sistematico e "forzature"* in "Diritto dell'informazione e dell'informatica", fasc.1, 2013, pag. 94-95.

[203] Cassazione penale, sez. VI, 04/10/1999, n. 3067, massima tratta da "Diritto dell'informazione e dell'informatica" 2001, fasc. 3, p. 485 (nota di: Lucente C. G.).

Vi è però chi ha ritenuto che la tutela debba essere accordata non già al sistema in sé considerato ma proprio ai dati che esso custodisce[204].

È una lettura, quest'ultima, che coglie sicuramente un aspetto decisivo della *ratio legis* sottesa alla norma incriminatrice, tuttavia si ritiene che il tenore letterale della norma stessa e il quadro sistematico in cui essa è inserita faccia propendere per una tutela più ampia accordata dal legislatore, che ha voluto espressamente riferirsi all'intero apparato tecnologico il quale è, nel suo complesso, di fondamentale importanza per lo sviluppo economico e per la tutela dei diritti e perciò meritevole *ex se* di tutela specifica.

Ciò non toglie naturalmente che si debba riconoscere una forte connessione fra la tutela dei sistemi informatici e la tutela dei dati contenuti al loro interno, perché è ovvio che l'apprensione in caso di intrusioni illecite riguardi nella maggior parte dei casi la sorte dei dati contenuti nei sistemi oggetto di attacco, tuttavia anche la semplice condotta consistente nell'attentare a un sistema, fosse anche privo di informazioni, è connotata da uno specifico disvalore, come lo sarebbe quella di entrare e intrattenersi in un'abitazione altrui senza permesso. In effetti, appare corretto ritenere che ad essere in pericolo sarebbe la sicurezza delle infrastrutture tecnologiche e il loro libero e funzionale utilizzo, che la norma intende invece tutelare.

Ulteriore fattispecie rilevante ai fini che qui interessano è l'articolo 615 quater, *Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici*.

Tale norma, in qualche modo, anticipa la tutela penale andando a punire una condotta che di fatto è prodromica sia all'ipotesi descritta dall'articolo 615 ter, sia alla realizzazione di altre fattispecie di reato.

Si vuole in questo caso reprimere a monte la possibilità di accessi abusivi e la sottrazione, la divulgazione o anche solo la semplice fruizione illecita di informazioni e servizi contenuti nei sistemi che sarebbero così violati.

D'altronde, per quanto elaborata possa essere una struttura di sicurezza informatica, a poco varrebbe nel caso in cui i codici che ne permettono l'accesso finissero nelle mani sbagliate.

---

[204] Cfr. Mantovani F., *Diritto Penale, parte speciale, I, Delitti contro la persona*, Cedam, Padova, 2011, pp. 545-546.

Altra fattispecie assai delicata è rappresentata dall'articolo 615 quinquies, *Diffusione di apparechiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico*, introdotto con la l. 48/2008, che ha ratificato la Convenzione di Budapest.

Si tratta di una delle fattispecie più pericolose e diffuse perché attraverso il ricorso a strumenti tecnici relativamente accessibili a chiunque, è possibile condurre attacchi su scala internazionale.

All'interno di questa categoria rientra una delle più tipiche tipologie di attacchi informatici, quella condotta attraverso i cd. *Ransomware*, che sono tipologie di malware capaci di interferire con il funzionamento di un sistema, fino a metterlo fuori uso nei casi più gravi, oltre ad essere in grado di carpire i dati contenuti al suo interno al fine di estorcere un riscatto al proprietario del sistema violato.

Numerose sono le tipologie di malware che rientrano in questa tipologia, fra cui il cd. *Wannacry*, che nel Maggio 2017 ha messo in seria difficoltà numerosi sistemi in tutto il mondo, compreso quello del servizio sanitario nazionale britannico.

In questa rassegna meritano menzione anche i *delitti contro la inviolabilità dei segreti*, in particolare le disposizioni che vanno dall'articolo 616 al 620 c.p., che sono volte a tutelare la libertà e la segretezza della corrispondenza e delle comunicazioni da eventuali alterazioni ed interferenze illecite.

Si tratta di fattispecie di origine risalente che tuttavia, nella loro evoluzione giurisprudenziale, rivelano la crescente attenzione per l'utilizzo assai spesso disinvolto di strumenti di riproduzione e diffusione di informazioni e immagini sempre più sofisticati e a buon mercato [205].

Altra fattispecie di importanza centrale con riferimento alle condotte lesive della privacy e alla dimensione internazionale di tale problema è quella descritta dall'art. 640 ter c.p. rubricato *Frode informatica*, che costituisce una declinazione della truffa semplice di cui all'art. 640 c.p.

[205] In particolare, gli articoli che vanno al 617 bis al 617 sexies sono stati introdotti con l. 98/1974 e l'art. 617 septies *Diffusione di riprese e registrazioni fraudolente*, con il d.lgs. n. 216 del 29 dicembre 2017.

Le modalità di realizzazione di questa fattispecie illecita sono purtroppo molteplici; si pensi alla falsificazione o clonazione di carte di pagamento effettuata acquisendo i dati tramite alterazioni dei sistemi di pagamento online o alla cd. "salami techniques", che consiste nella sottrazione illecita e protratta nel tempo di importi ridotti dal proprio conto, resa possibile da programmi creati *ad hoc*.

Sotto questa definizione rientra, tra le altre, una delle attività illecite più diffuse: il *phishing*[206].

Normalmente, questa tecnica viene realizzata attraverso l'invio di una e-mail che avvisa della necessità di fornire i propri dati, nella maggior parte dei casi dati bancari, per risolvere dei problemi che si sono verificati, per riscuotere dei premi o anche solo per la necessità di procedere a degli aggiornamenti. Tali avvisi si presentano come verosimili per lo stile grafico che adottano, che richiama quello di istituzioni pubbliche, banche, associazioni, ecc...

Il malcapitato destinatario, tratto in inganno, inserisce i dati richiesti che finiscono così nelle mani dei malviventi, i quali avranno poi gioco facile nel procedere al proprio piano criminoso, solitamente consistente nel prelievo di somme dai conti correnti di cui si sono acquisiti i codici di accesso e nel loro subitaneo dirottamento fuori dall'Unione Europea, in paesi nei quali il recupero sarà assai difficoltoso.

Ovviamente, visto anche l'allarme sociale che queste condotte generano, è solo una piccola percentuale di coloro che ricevono questi messaggi a cadere nel tranello, ma anche così la tecnica rimane molto redditizia.

Se fino a qualche anno fa la maggior parte dei tentativi di *phishing* avveniva con modalità grossolane e facilmente identificabili, negli ultimi anni la capacità delle organizzazioni criminali di creare le oggettive apparenze di una comunicazione ufficiale sono notevolmente migliorate, per cui banche, istituzioni e aziende che usano la rete come

[206] Cfr. Cajani F., Costabile G., Mazzaraco G., *Phishing e furto d'identità digitale. Indagini informatiche e sicurezza bancaria*, Giuffrè, Milano, 2008, p. 15 ss.

strumento di comunicazione devono tenerne conto e approntare prassi tali da garantire la sicurezza e impedire il più possibile situazioni di dubbio[207].

Altre fattispecie rilevanti sono quelle di cui agli articoli da 635 bis a 635 quinques, anch'essi introdotti dalla l. 48/2008 come declinazioni del reato di danneggiamento di cui all'art. 635.

L'elenco delle fattispecie in questo caso corre forse il rischio di essere ridondante e va a punire quelle condotte volte a rendere inservibile, a cancellare, alterare o deteriorare sistemi informatici sia privati che di pubblica utilità[208]; tali disposizioni, insieme a quella di cui terzo al comma dell'art. 392 c.p., *esercizio arbitrario delle proprie ragioni con violenza sulle cose*, ponendo una tutela penale sui sistemi sono finalizzate ad evitare il rischio di perdite o diffusioni di dati personali che deriverebbe dalle condotte in questione.

2.2. I reati previsti dal Codice privacy a seguito delle modifiche apportate dal d.lgs. n. 101 del 10 agosto 2018

Capitolo a parte è il discorso attinente ai reati appositamente dedicati alla tutela dei dati personali.

Si tratta di fattispecie che hanno sempre avuto la propria sede naturale all'interno del codice della Privacy e anche nel contesto legislativo post-riforma la situazione non è mutata giacchè il regolamento, essendo una fonte del diritto europeo, non poteva prevedere autonomamente la disciplina penale.

---

[207] Sul punto, la Sentenza del Tribunale di Milano, Sez. VI, 04.12.2014 ha statuito che "Nell'adempimento delle obbligazioni inerenti all'esercizio di un'attività professionale, la diligenza deve valutarsi con riguardo alla natura dell'attività esercitata, ai sensi dell'art. 1176, comma 2, c.c. In particolare, nel rapporto contrattuale di home banking, la banca ha la veste di contraente qualificato, che, non ignaro delle modalità di frode mediante phishing da tempo note nel settore, è tenuto ad adeguarsi all'evoluzione dei nuovi sistemi di sicurezza.", massima tratta da "Responsabilità Civile e Previdenza" (nota a cura di Frau R.), fasc. 3, anno 2015, p. 908. Tale orientamento sembra essere alla base della recente Cassazione civile, sez. VI, 12/04/2018, n. 9158 che ha stabilito l'obbligo risarcitorio sulla base del fatto che "in tema di responsabilità della banca in caso di operazioni effettuate a mezzo di strumenti elettronici, anche al fine di garantire la fiducia degli utenti nella sicurezza del sistema (il che rappresenta interesse degli stessi operatori), è del tutto ragionevole ricondurre nell'area del rischio professionale del prestatore dei servizi di pagamento, prevedibile ed evitabile con appropriate misure destinate a verificare la riconducibilità delle operazioni alla volontà del cliente, la possibilità di una utilizzazione dei codici di accesso al sistema da parte dei terzi, non attribuibile al dolo del titolare o a comportamenti talmente incauti da non poter essere fronteggiati in anticipo.".

[208] Cfr. Monaco L., *sub 635 bis e ss. c.p.*, in *commentario breve al codice penale* op, cit., p. 2636-2637.

In effetti in questi anni il dibattito sugli aspetti sanzionatori si è concentrato soprattutto sul profilo delle sanzioni amministrative previste dal Capo VIII del *General Data Protection Regulation*.

Si tratta in effetti di sanzioni estremamente pesanti; concepite con l'intento di fungere da sprone efficace nei confronti dei colossi del Web e dell'informatica ma che hanno finito per mandare in apprensione anche imprese di ridotte dimensioni.

Nondimeno, si è dovuto attendere a lungo per avere un intervento legislativo dello Stato che realizzasse un quadro definitivo dell'apparato sanzionatorio, organizzando anche la disciplina penale.

È d'altronde lo stesso regolamento che lascia dei margini per gli interventi legislativi dei singoli paesi membri, pur dovendo porre attenzione ad evitare rischi per la necessaria armonizzazione delle diverse legislazioni fra di esse e con la normativa europea[209].

Inizialmente quindi, attraverso l'art. 13 della legge delega n. 163/2017[210] era stata paventata l'ipotesi che il legislatore sarebbe intervenuto con un provvedimento normativo *ad hoc*, con il quale abrogare *in toto* il d.lgs. 196/2003.

---

[209] Cfr. Rubechi M., La transizione verso il nuovo sistema delle fonti europee di protezione dei dati personali, in Califano L., Colapietro c. (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati nel Regolamento UE 2016/679*, in "Università degli Studi Roma Tre - CRISPEL (collana)- Sezione di diritto pubblico italiano ed europeo – Collettanee", Editoriale scientifica, Napoli, 2017, p. 374-387.

[210] Così l'art. 13, l. n. 163/2017, "Delega al Governo per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonche' alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE":

" 1. Il Governo e' delegato ad adottare, entro sei mesi dalla data di entrata in vigore della presente legge, con le procedure di cui all'articolo 31 della legge 24 dicembre 2012, n. 234, acquisiti i pareri delle competenti Commissioni parlamentari e del Garante per la protezione dei dati personali, uno o piu' decreti legislativi al fine di adeguare il quadro normativo nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonche' alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE.

2. I decreti legislativi di cui al comma 1 sono adottati su proposta del Presidente del Consiglio dei ministri e del Ministro della giustizia, di concerto con i Ministri degli affari esteri e della cooperazione internazionale, dell'economia e delle finanze, dello sviluppo economico e per la semplificazione e la pubblica amministrazione.

3. Nell'esercizio della delega di cui al comma 1 il Governo e' tenuto a seguire, oltre ai principi e criteri direttivi generali di cui all'articolo 32 della legge 24 dicembre 2012, n. 234, anche i seguenti principi e criteri direttivi specifici:

Tale ipotesi non ha poi avuto seguito dal momento che avrebbe finito con l'eccedere rispetto a quanto richiesto dalla delega conferita al governo, la cui finalità era quella di riorganizzare il codice e non abrogarlo.

Inoltre, lo schema del decreto legislativo prevedeva la depenalizzazione *tout court* delle fattispecie penali previste nel d.lgs. 196/2003, seguendo un approccio per il quale l'apparato sanzionatorio avrebbe dovuto esaurirsi con l'aspetto amministrativo.

Un esito di questo genere non poteva dirsi in linea con la riforma europea, che se da un lato, effettivamente, non insiste in modo incisivo sugli aspetti penalistici, dall'altro però non avallava certo siffatte soluzioni.

La scelta del legislatore era stata stigmatizzata, fra gli altri, anche del Garante europeo per la protezione dei dati (E.D.P.S.), il quale non aveva mancato di sottolineare l'incompletezza della riforma senza le sanzioni in parola[211].

I rilievi mossi, insieme alla delicata fase di transizione politica avutasi nel passaggio fra la XVII e la XVIII legislatura hanno portato all'abbandono dello schema di decreto originario.

---

a) abrogare espressamente le disposizioni del codice in materia di trattamento dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196, incompatibili con le disposizioni contenute nel regolamento (UE) 2016/679;

b) modificare il codice di cui al decreto legislativo 30 giugno 2003, n. 196, limitatamente a quanto necessario per dare attuazione alle disposizioni non direttamente applicabili contenute nel regolamento (UE) 2016/679;

c) coordinare le disposizioni vigenti in materia di protezione dei dati personali con le disposizioni recate dal regolamento (UE) 2016/679;

d) prevedere, ove opportuno, il ricorso a specifici provvedimenti attuativi e integrativi adottati dal Garante per la protezione dei dati personali nell'ambito e per le finalita' previsti dal regolamento (UE) 2016/679;

e) adeguare, nell'ambito delle modifiche al codice di cui al decreto legislativo 30 giugno 2003, n. 196, il sistema sanzionatorio penale e amministrativo vigente alle disposizioni del regolamento (UE) 2016/679 con previsione di sanzioni penali e amministrative efficaci, dissuasive e proporzionate alla gravità della violazione delle disposizioni stesse.

4. Dall'attuazione del presente articolo non devono derivare nuovi o maggiori oneri a carico della finanza pubblica e ad essa si provvede con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente.".

[211] Cfr. Assonime – Associazione fra le società italiane per azioni, Rassegna Stampa 28 marzo 2018, disponibile sul sito internet dell'associazione, (http://www.assonime.it/_layouts/15/Assonime.CustomAction/GetPdfToUrl.aspx?PathPdf=http://www.assonime.it/assonime/area-stampa/comunicati/Documents/Rassegna%20stampa%2028%20marzo%202018.pdf), ultima cons. 14.10.2018.

Per l'effetto, alla data in cui il regolamento è entrato a pieno regime, non vi era ancora una normativa di raccordo con la legislazione italiana e il d.lgs. 196/2003 rimaneva operativo in tutte le sue parti andando a generare, come è logico, diversi problemi interpretativi nei primi mesi di vigenza della riforma.

Vero è che il quadro complessivo poteva essere ricostruito alla luce del principio di prevalenza del diritto europeo su quello nazionale ma altrettanto vero ed evidente è che questa operazione, in alcuni passaggi, si presentava ardua persino a soggetti esperti e che l'esegesi del testo che ne scaturiva era giocoforza aleatoria.

In effetti può dirsi che, visti i quesiti rimasti aperti, la data del 25 maggio 2018 abbia segnato sì un nuovo inizio nella legislazione in materia di privacy ma che questo inizio si stia realizzando per gradi, considerati gli interventi chiarificatori del Garante per la protezione dei dati, dell'European Data Protection Board e del European Data Protection Supervisor che si stanno susseguendo in questi mesi, proprio al fine di dettagliare gli aspetti ambigui della normativa.

Ad ogni buon conto, una tale situazione di incertezza non si sarebbe potuta protrarre a lungo.

L'iter del provvedimento è infatti ripartito il 15 maggio 2018, data in cui lo stesso è stato assegnato alla Commissione speciale per l'esame di atti del Governo sotto il nome di *Schema di decreto legislativo recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (22)*.

Abbandonata l'idea di un'abrogazione del d.lgs. 196/2003, la nuova proposta ha optato per una rivisitazione del testo, che eliminasse le disposizioni riferite ad aspetti già contenuti nel Regolamento (UE) 2016/679.

In tal modo si è pervenuti ad un drastico ridimensionamento del codice privacy, che pure ha conservato una rilevanza imprescindibile in alcuni settori, fra cui quello penale.

Nell'affrontare in particolare il tema delle fattispecie incriminatrici, la commissione ha sottolineato a più riprese la propria preoccupazione sulla necessità di evitare un'illegittima sovrapposizione fra le previsioni penali e quelle amministrative, in

considerazione del fatto che "le Corti internazionali più volte (anche molto di recente) hanno severamente censurato casi nei quali gli ordinamenti interni avevano previsto che le medesime violazioni risultassero sanzionate sia a livello amministrativo che sul piano penale ed il nostro sistema attualmente non dispone di norme generali di coordinamento in grado di scongiurare detto rischio."[212].

Invero, a leggere la relazione che ha accompagnato la presentazione del testo del decreto, si coglie la necessità di riformulare le previsioni penali in modo tale da renderle più aderenti alla nuova realtà normativa e di connotarle in modo da renderle effettivamente ed autonomamente applicabili.

Nel corso dei lavori è intervenuto anche il Garante privacy, che ne ha approvato i contenuti di fondo, pur presentando una nutrita serie di osservazioni[213].

La normativa che ne è uscita presenta quindi un nuovo impianto in materia di tutela penale della privacy, che porta a ritenere che il legislatore abbia voluto caratterizzare in modo più puntale le fattispecie meritevoli di sanzione penale.

Ne emerge infatti un quadro più ampio e dettagliato che appare maggiormente "al passo" con gli aspetti critici dei problemi odierni in materia di sicurezza dei dati, anche in campo internazionale, oltre che assai interessante per i profili di contatto che possono essere individuati rispetto alla figura del Data Protection Officer.

L'elenco dei reati inizia infatti con l'articolo 167, rubricato *Trattamento illecito di dati*[214].

---

[212] Ministero della Giustizia - ufficio legislativo, *Schema di decreto legislativo recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) - Analisi di Impatto della Regolamentazione (A.I.R.)*, p. 6.

[213] Garante per la protezione dei dati personali, *parere del Garante su uno schema di decreto legislativo recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679 dei Parlamento europeo e del Consiglio, del 27 aprile 2016*, Registro dei provvedimenti n. 312 del 22 maggio 2018.

[214] Così l'art. 167, d.lgs 196/2003, novellato dal d.lgs. 101/2018 e rubricato "Trattamento illecito di dati":

"1. Salvo che il fatto costituisca piu' grave reato, chiunque, al fine di trarre per sè o per altri profitto ovvero di arrecare danno all'interessato, operando in violazione di quanto disposto dagli articoli 123, 126 e 130 o dal provvedimento di cui all'articolo 129 arreca nocumento all'interessato, e' punito con la reclusione da sei mesi a un anno e sei mesi.

2. Salvo che il fatto costituisca piu' grave reato, chiunque, al fine di trarre per se' o per altri profitto ovvero di arrecare danno all'interessato, procedendo al trattamento dei dati personali di cui agli

Non vi è dubbio che ci sia una continuità con la precedente fattispecie che, tra l'altro, costituiva la principale fonte di responsabilità penale nel settore.

Permangono quindi gli elementi costitutivi del reato: anzitutto la necessità che vi sia un nocumento per gli interessati, e poi che la condotta sia posta in essere per generare un profitto per l'agente[215] o altri soggetti ovvero per arrecare un danno all'interessato, destinatario della condotta illecita. In ossequio al principio di offensività, occorrerà quindi dare la prova di una condotta lesiva che non si sia fermata alla mera irregolarità dal punto di vista amministrativo e gestionale ma che abbia provocato un danno apprezzabile alla persona offesa[216], voluto e perseguito dall'agente.

---

articoli 9 e 10 del Regolamento in violazione delle disposizioni di cui agli articoli 2-sexies e 2-octies, o delle misure di garanzia di cui all'articolo 2-septies ovvero operando in violazione delle misure adottate ai sensi dell'articolo 2quinquiesdecies arreca nocumento all'interessato, e' punito con la reclusione da uno a tre anni.

3. Salvo che il fatto costituisca piu' grave reato, la pena di cui al comma 2 si applica altresì a chiunque, al fine di trarre per sè o per altri profitto ovvero di arrecare danno all'interessato, procedendo al trasferimento dei dati personali verso un paese terzo o un'organizzazione internazionale al di fuori dei casi consentiti ai sensi degli articoli 45, 46 o 49 del Regolamento, arreca nocumento all'interessato.

4. Il Pubblico ministero, quando ha notizia dei reati di cui ai commi 1, 2 e 3, ne informa senza ritardo il Garante.

5. Il Garante trasmette al pubblico ministero, con una relazione motivata, la documentazione raccolta nello svolgimento dell'attivita' di accertamento nel caso in cui emergano elementi che facciano presumere la esistenza di un reato. La trasmissione degli atti al pubblico ministero avviene al piu' tardi al termine dell'attivita' di accertamento delle violazioni delle disposizioni di cui al presente decreto. 6. Quando per lo stesso fatto e' stata applicata a norma del presente codice o del Regolamento a carico dell'imputato o dell'ente una sanzione amministrativa pecuniaria dal Garante e questa è stata riscossa, la pena è diminuita".

[215] La giurisprudenza ha inteso in senso ampio la nozione di profitto, come si evince da Cassazione penale, sez. III, 16/07/2013, n. 7504: "Costituisce trattamento illecito dei dati personali relativi a minori, punibile ai sensi dell'art. 167, comma 2, del d.lg. 30 giugno 2003 n. 196, la pubblicazione non autorizzata, in un articolo di cronaca giornalistica, delle generalità e della fotografia di un minore rimasto vittima di un incidente stradale, quand'anche lo scopo perseguito sia stato quello di richiamare più efficacemente l'attenzione dell'opinione pubblica e delle competenti autorità sulla ritenuta necessità di interventi atti ad eliminare le condizioni di insicurezza presentate dal tratto stradale in cui l'incidente si era verificato, non presentandosi comunque, la detta pubblicazione, come connotata dal carattere dell'essenzialità ai fini della completezza dell'informazione, né potendosi escludere tanto la sussistenza del nocumento (ravvisabile anche con riferimento a soggetti terzi) quanto quella della quanto meno concorrente finalità di profitto, correlata al possibile incremento delle vendite del giornale.", massima tratta da "Rivista penale" fasc. n.4/2014, p. 409, Archivio della circolazione e dei sinistri 2014, 5, 400.

[216] Cfr., ex plurimis, Cass., sez. III pen., sent. 30134/2004.Più recente, sulla stessa linea interpretativa: Cass. pen., Sez. III, 18 dicembre 2014, n. 7504.

In tal modo, il "nocumento" costituisce condizione obiettiva di punibilità anche se parte minoritaria, ma persistente, della giurisprudenza seguita a valutarlo come elemento costitutivo del reato[217].

Le nuove disposizioni contengono anche ipotesi più dettagliate che prevedono la punizione nei confronti di coloro che operano "in violazione di quanto disposto dagli articoli 123, 126 e 130 o dal provvedimento di cui all'articolo 129"[218] o che procedono "al trattamento dei dati personali di cui agli articoli 9 e 10 del Regolamento in violazione delle disposizioni di cui agli articoli 2-sexies e 2-octies, o delle misure di garanzia di cui all'articolo 2-septies ovvero operando in violazione delle misure adottate ai sensi dell'articolo 2- quinquiesdecies"[219] o "al trasferimento dei dati personali verso un paese terzo o un'organizzazione internazionale al di fuori dei casi consentiti ai sensi degli articoli 45, 46 o 49 del Regolamento"[220].

Quest'ultima disposizione è di particolare importanza perché si riferisce proprio all'ipotesi in cui l'illecito trattamento sia avvenuto in violazione delle norme sul trasferimento di dati all'estero, a testimonianza dell'importanza che assume oggi una corretta circolazione internazionale dei dati, propedeutica a garantirne la sicurezza.

I commi 4 e 5 poi, si preoccupano di stabilire un circolo virtuoso di comunicazione e collaborazione fra Garante e Pubblico Ministero in ragione del quale ciascuno dovrà informare l'altro nel caso in cui emergano responsabilità di relativa competenza; è inoltre prevista una riduzione di pena qualora per il medesimo fatto sia applicata anche una sanzione amministrativa, secondo il disposto del sesto comma.

Proprio a partire da questa consapevolezza si può proseguire l'analisi con l'articolo 167 bis, *Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala*[221], che costituisce una nuova e rilevante fattispecie.

---

[217] Cfr. Cassazione penale, sez. III, n. 40103 del 5 febbraio 2015

[218] art. 167, c. 1, d.lgs. 196/2003, come modificato dal d.lgs. 101/2018; il richiamo agli articoli elencati è relativo alle prescrizioni, ivi descritte, in materia di comunicazione elettroniche.

[219] art. 167, c. 2, d.lgs. 196/2003, come modificato dal d.lgs. 101/2018.

[220] art. 167, c. 3, d.lgs. 196/2003, come modificato dal d.lgs. 101/2018.

[221] Così l'art. 167 bis, d.lgs. 196/2003, introdotto dal d.lgs. 101/2018 e rubricato "Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala":

Le condizioni concernenti la finalità di conseguire un profitto o arrecare un danno sono le medesime già descritte all'art. 167; in questo caso però la tutela penale è anticipata, in quanto non è necessario che si realizzi un nocumento per la vittima.

Oggetto della tutela è invece un "archivio automatizzato o parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala"; la nozione di "archivio automatizzato" è senz'altro singolare, perché non risulta una definizione di tal fatta nella legislazione di matrice europea o nazionale.

Sul punto però viene in soccorso anzitutto lo stesso regolamento europeo, che all'art. 4, par. 1, n. 6), stabilisce che archivio è "qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico".

La definizione data dal G.D.P.R. tuttavia non risulta esaustiva ed univoca poiché a seconda dei "criteri determinati" cui si fa riferimento, questa nozione può ampliarsi o restringersi, portando a difficoltà interpretative di non poco conto.

Il margine di indeterminatezza quindi permane e, in mancanza di un'univoca definizione di origine legislativa o giurisprudenziale, occorrerà far riferimento alle nozioni fornite da manuali tecnici di altre discipline e a concetti analoghi già contenuti nella legislazione vigente[222].

Anche in questo caso, comunque, non vi è dubbio che il legislatore si sia posto in un'ottica di tutela transnazionale, perché il concetto di "larga scala" tiene conto, come si

---

"1. Salvo che il fatto costituisca piu' grave reato, chiunque comunica o diffonde al fine di trarre profitto per se' o altri ovvero al fine di arrecare danno, un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala, in violazione degli articoli 2-ter, 2-sexies e 2-octies, è punito con la reclusione da uno a sei anni.

2. Salvo che il fatto costituisca piu' grave reato, chiunque, al fine trarne profitto per se' o altri ovvero di arrecare danno, comunica o diffonde, senza consenso, un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala, e' punito con la reclusione da uno a sei anni, quando il consenso dell'interessato è richiesto per le operazioni di comunicazione e di diffusione.

3. Per i reati di cui ai commi 1 e 2, si applicano i commi 4, 5 e 6 dell'articolo 167."

[222] Si pensi in particolare alla Direttiva 96/9/CE che al considerando 17 ha così definito il concetto di "Banca Dati": "raccolta di opere, siano esse letterarie, artistiche, musicali o di altro genere, oppure di materiale quali testi, suoni, immagini, numeri, fatti e dati; che deve trattarsi di raccolte di opere, di dati o di altri elementi indipendenti, disposti in maniera sistematica o metodica e individualmente accessibili"

è avuto modo di vedere, anche della "portata geografica"[223] del trattamento, oltre della mole di dati coinvolti.

Ad ogni modo, le condotte sanzionate dall'art 167 bis sono di due tipi: da una parte si punisce la comunicazione o diffusione che avviene "in violazione degli articoli 2-ter, 2-sexies e 2-octies" e dall'altra quelle che avvengono in casi in cui non vi era stato un preventivo consenso alla comunicazione o diffusione.

Speculare all'articolo 167 bis è l'articolo 167 ter, *Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala*[224].

Se la prima norma puniva la comunicazione e la diffusione degli archivi, in questo caso alle stesse condizioni ne viene sanzionata l'acquisizione.

Il presupposto è che, se da una parte c'è un soggetto che comunica o diffonde, dall'altra deve essercene un altro che riceve le informazioni illecitamente diffuse e le adopera a proprio vantaggio o altrui danno.

Per quanto concerne il rapporto fra queste fattispecie e il Data Protection Officer deve sottolinearsi che, *rebus sic stantibus*, le ipotesi di reato descritte coinvolgono tipologie di trattamenti per i quali è necessaria la nomina della nuova figura.

Ne deriva che, qualora la giurisprudenza intendesse accogliere la posizione, sostenuta dallo scrivente, che vede il suo possibile coinvolgimento in eventuali responsabilità penali egli, in caso di illeciti come quello in commento, potrebbe esserne chiamato a rispondere in relazione all'attività svolta nell'esercizio dei suoi compiti.

All'infuori dell'ipotesi di una responsabilità derivante da posizione di garanzia, va pur detto che, trattandosi di fattispecie che si presentano caratterizzate da dolo specifico, occorrerebbe un comportamento connotato da una particolare *intentio criminis* da parte dell'agente. D'altronde una condotta del genere difficilmente potrebbe venir posta in

---

[223] Cfr. Gruppo di lavoro articolo 29, *Linee guida sui responsabili della protezione dei dati*, op. cit., par. 2.1.3, p.10.

[224] Così l'art. 167 ter, introdotto dal d.lgs. 101/2018 e rubricato "Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala":
1. Salvo che il fatto costituisca piu' grave reato, chiunque, al fine trarne profitto per sè o altri ovvero di arrecare danno, acquisisce con mezzi fraudolenti un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala e' punito con la reclusione da uno a quattro anni. 2. Per il reato di cui al comma 1 si applicano i commi 4, 5 e 6 dell'articolo 167".

essere per un vantaggio diretto del D.P.O. o anche dello stesso titolare del trattamento, pur non potendo essere esclusa a priori; più facile invece immaginare che la condotta in questione potrebbe essere posta in essere a vantaggio dell'azienda o ente di appartenenza.

Novellato è anche l'art. 168, *Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante* [225], di cui sono stati riveduti il titolo e il testo.

Si punisce ora non solo la falsità nelle comunicazioni rese al Garante, ma anche l'ostacolo alla regolarità delle verifiche, delle ispezioni, dei procedimenti effettuati dal garante stesso, come si evince dal disposto di cui al comma secondo.

Ancor più che nel passato è evidente come la norma si ponga a presidio non solo della capacità sanzionatoria dell'autorità pubblica chiamata a svolgere un ruolo ispettivo ma anche, in subordine, della trasparenza che deve permeare tutte le operazioni che coinvolgono personali dei cittadini.

Questi infatti fanno affidamento su aziende ed enti pubblici nel momento in cui forniscono loro i propri dati, permettendogli di utilizzarli per le proprie finalità commerciali o istituzionali. Trattandosi di informazioni preziose, che mettono in discussione anche diritti fondamentali, i titolari sono chiamate ad esercitare una corrispondente responsabilità nel modo in cui gestiscono i dati e ne garantiscono la sicurezza nel rispetto della normativa vigente, cosa che si traduce anche nel dovere di esercitare trasparenza e di collaborare con le autorità.

Chi vuole permanere nel mercato dei dati infatti, deve contribuire alla costruzione di un clima di fiducia, incompatibile con condotte di falsità o comunque contrarie alla

---

[225] Così l'art. 168, d.lgs. 196/2003, novellato dal d.lgs. 101/2018 e rubricato "Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante":
1. Salvo che il fatto costituisca piu' grave reato, chiunque, in un procedimento o nel corso di accertamenti dinanzi al Garante, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi, e' punito con la reclusione da sei mesi a tre anni.
2. Fuori dei casi di cui al comma 1, e' punito con la reclusione sino ad un anno chiunque intenzionalmente cagiona un'interruzione o turba la regolarita' di un procedimento dinanzi al Garante o degli accertamenti dallo stesso svolti".

trasparenza e alla leale collaborazione che andrebbero inevitabilmente a minare tale fiducia, non solo nei confronti della specifica struttura che ha operato illecitamente, ma anche nei confronti di tutto il mercato, con grave danno all'economia generale.

Ecco perché è di fondamentale importanza la presenza di un collegamento diretto e leale fra le autorità di controllo e i titolari del trattamento.

Una comunicazione che viene esercitata in particolare dal D.P.O. che ha proprio il compito di fungere da punto di contatto con le autorità di controllo, specie in condizioni di pericolo per la sicurezza come i *data breach*.

La norma incriminatrice commentata rappresenta quindi un ulteriore profilo di responsabilità che può coinvolgere in prima persona il Data Protection Officer.

Pur non ritenendo corretto definirlo come un reato proprio del D.P.O., dal momento che pure altre figure potrebbero astrattamente incorrervi, è senz'altro un'ipotesi estremamente significativa per coloro che svolgono questo compito.

Per altro verso, è di fondamentale importanza anche il rispetto delle prescrizioni del Garante ed è proprio questo che è previsto dall'articolo 170, *Inosservanza di provvedimenti del Garante*[226].

Tale norma punisce quelle situazioni in cui non siano stati osservati "il provvedimento adottato dal Garante ai sensi degli articoli 58, paragrafo 2, lettera f) del Regolamento, dell'articolo 2-septies, comma 1, nonchè i provvedimenti generali di cui all'articolo 21, comma 1, del decreto legislativo di attuazione dell'articolo 13 della legge 25 ottobre 2017, n. 163".

Con riferimento a questa fattispecie delittuosa, occorre ribadire che, come si è detto, il Data Protection Office non ha poteri di gestione diretta, quindi ovviamente non potranno essere ipotizzate responsabilità da parte sua in caso di inosservanza *ex se* dei provvedimenti del Garante.

[226] Così l'art. 170, d.lgs. 1096/2003, novellato dal d.lgs. 101/2018:
"1. Chiunque, essendovi tenuto, non osserva il provvedimento adottato dal Garante ai sensi degli articoli 58, paragrafo 2, lettera f) del Regolamento, dell'articolo 2-septies, comma 1, nonchè i provvedimenti generali di cui all'articolo 21, comma 1, del decreto legislativo di attuazione dell'articolo 13 della legge 25 ottobre 2017, n. 163 e' punito con la reclusione da tre mesi a due anni."

Nondimeno, anche nel suo ruolo di "punto di contatto", egli dovrà dar conto al titolare o al responsabile di ogni iniziativa presa dal Garante che interessi la struttura in cui si trova ad operare come soggetto qualificato e specializzato, con conseguenza che una mancanza da questo punto di vista potrebbe esporlo a un concorso nel reato citato.

È stato abrogato, invece, il reato precedentemente previsto dall'articolo 169 del Codice Privacy, *Misure di sicurezza*.

La cosa in verità non deve stupire perché, pur essendoci nel regolamento la previsione di particolari misure di sicurezza al Capo IV, sezione II, queste non possono essere assimilate a quelle precedentemente enunciate dal codice privacy, in particolare nel suo allegato b), ora abrogato.

Infatti, in virtù del principio di accountability, si predilige un approccio sostanzialistico che non può essere ridotto all'osservanza di formule prestabilite e pertanto il disposto dell'articolo 169 non sarebbe stato coerente con la nuova impostazione del regolamento.

Pure deve essere citato l'art. 171, *Violazioni delle disposizioni in materia di controlli a distanza e indagini sulle opinioni dei lavoratori*[227].

Esso interviene sul codice privacy raccordandolo alla l. 300/70 e prevedendo una tutela penale nei confronti di quelle condotte di illecita installazione di impianti audiovisivi, finalizzata, fondamentalmente, a effettuare un controllo a distanza illegittimo sui lavoratori.

Ulteriore campo di applicazione della norma si riferisce a quelle condotte che, avvalendosi anche di sistemi tecnologici, sono finalizzate a indagare sulle opinioni personali, religiose, politiche dei lavoratori, in modo da esercitare un controllo del tutto inconferente con le finalità proprie del rapporto di lavoro.

Chi pratica il diritto del lavoro sa bene quanto sia complesso trovare nelle situazioni concrete il giusto compromesso fra tutela della libertà del lavoratore e potere di controllo da parte del datore e, soprattutto, quanto le nuove tecnologie abbiano esasperato questa

[227] Così l'art. 171 d.lgs. 196/2003, novellato dal d.lgs. 101/2018:
1. La violazione delle disposizioni di cui agli articoli 4, comma 1, e 8 della legge 20 maggio 1970, n. 300, e' punita con le sanzioni di cui all'articolo 38 della medesima legge

tensione, mettendo a disposizione strumenti che, in alcuni casi, sarebbero in grado di esercitare un controllo a distanza anche fra paesi diversi.

È quindi importante saper intervenire sul punto in modo equilibrato, competente e capace di mediazione, come dovrebbe saper fare un buon D.P.O.

Da ultimo va segnalato che l'articolo 172, *Pene accessorie*[228], prevede la pubblicazione dei provvedimenti di condanna, ai sensi del secondo e terzo comma dell'art. 36 c.p.[229]

Si tratta senz'altro di un ulteriore incentivo a evitare di incappare in sanzioni relative alla privacy, considerato che questo avrebbe un costo rilevante anche in termini di reputazione e di immagine.

Ora, le nuove norme penali sono sicuramente più dettagliate rispetto alle precedenti e distinguono varie tipologie di azioni illecite. Per la maggior parte, esse sono anticipate dall'introduzione "salvo che il fatto costituisca più grave reato".

In effetti nell'esperienza pre-riforma, i reati contenuti nel codice privacy venivano spesso identificati come condotte prodromiche alla realizzazione di altre fattispecie e da queste assorbite.

Sta quindi all'interprete valutare, caso per caso, se in relazione al bene giuridico messo in pericolo dalla condotta dell'agente e alle finalità della stessa, i reati previsti dal codice privacy debbano ritenersi assorbiti da fattispecie più gravi ovvero, pur se magari nell'ambito di un medesimo disegno criminoso ex articolo 81 c.p., possano essere tenuti distinti e quindi concorrere.

A tal proposito, c'è da immaginare che nel prossimo futuro il nuovo corpus di reati previsti dal Codice privacy sarà oggetto di particolare attenzione da parte della giurisprudenza in quanto, proponendo fattispecie più dettagliate e specifiche rispetto al

---

[228] Così l'art. 172 d.lgs. 196/2003, novellato dal d.lgs. 101/2018:
1. La condanna per uno dei delitti previsti dal presente codice importa la pubblicazione della sentenza ai sensi dell'articolo 36, secondo e terzo comma, del codice penale.

[229] I due commi in quesitone recitano:
"La sentenza di condanna è inoltre pubblicata nel sito internet del Ministero della giustizia. La durata della pubblicazione nel sito è stabilita dal giudice in misura non superiore a trenta giorni. In mancanza, la durata è di quindici giorni.
La pubblicazione è fatta per estratto, salvo che il giudice disponga la pubblicazione per intero; essa è eseguita d'ufficio e a spese del condannato."

passato, probabilmente vi sarà maggiore probabilità che emerga l'autonomia della nuova normativa rispetto ad altre figure delittuose.

Questa lettura, d'altronde, permetterebbe di valorizzare le disposizioni testè descritte nel contesto della tutela dei dati in ambito penale, dove finora sono state relegate ad una posizione "ancillare" rispetto ad altre fattispecie più complesse.

3. Risk Based Approach e D.P.O.

La disciplina descritta è importante anche perché consente di passare in rassegna le principali fattispecie di reato in cui si declinano i rischi per la protezione dei dati nell'attuale contesto operativo.

Tale elencazione, come già detto, non è certamente esaustiva, perché purtoppo i dati personali possono fungere da elemento necessario per la realizzazione di una molteplicità di condotte illecite.

Nondimeno, le ipotesi descritte costituiscono la maggior parte della casistica che i professionisti del settore affrontano nello svolgimento delle proprie mansioni.

I dati descritti dal Rapporto del Clusit e da altre ricerche, insieme alle tante notizie di cronaca che riportano violazioni, piani criminosi o comunque pratiche scorrette e lesive dei diritti afferenti alla privacy, contribuiscono a dare un'immagine non certo rassicurante dell'efficacia dei sistemi di tutela e, soprattutto, di una forte distanza fra i diritti riconosciuti agli interessati e la realtà concreta.

Non v'è azienda, in particolare fra quelle che operano nel campo dei servizi informatici e dell'elaborazione dei dati, che non spenda risorse importanti nel campo della sicurezza, cercando al contempo, legittimamente, di rassicurare i propri utenti sulla piena tutela fornita ai loro dati.

Occorre tuttavia prendere atto che la attuale situazione tecnologica e giuridica non consente, nemmeno laddove siano state dotate effettive misure di prevenzione e sicurezza, di ritenersi al riparo da qualsiasi tipo di rischio anzi, forse sarebbe opportuno impostare il rapporto fra titolari del trattamento da un parte e interessati dall'altro, sulla base di questa realistica consapevolezza e da qui cercare, ciascuno nei propri ambiti di

competenza, di mettere in atto misure e comportamenti in grado di evitare, situazioni di pericolo.

Non è un caso che il regolamento europeo fondi la propria strategia di sicurezza sul *risk-based-approach* (approccio basato sul rischio).

Si tratta di un connotato che caratterizza il regolamento, legandosi al principio di accountability e fungendo da corollario della privacy by design.

Esso prevede che, nell'organizzare un sistema di gestione della privacy che sia veramente conforme alla normativa (*privacy compliance*), sia necessario sviluppare le risposte della struttura a tutti i possibili fattori di rischio che potrebbero verificarsi e mettere a repentaglio l'integrità e la disponibilità dei dati.

In particolare, il risk based approach si evince dalle disposizioni in materia di "sicurezza dei dati" e da quelle relative a "valutazione di impatto sulla protezione dei dati e consultazione preventiva".

L'art. 32, *Sicurezza del trattamento*[230], indica una serie di misure da mettere in atto al fine di garantire un'adeguata tutela, in relazione alle caratteristiche intrinseche del trattamento e del contesto in cui viene effettuato.

---

[230] Articolo 32, Regolamento (UE) 2016/679:
"Sicurezza del trattamento:
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:
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

Tale indicazione però non è tassativa né esaustiva anzi, il regolamento stesso sembra incoraggiare il titolare o il responsabile a adottare ulteriori strumenti, in modo particolare la dotazione di un codice di condotta ex art. 40 o un meccanismo di certificazione ex art. 42 la cui individuazione è lasciata alla discrezionalità degli stessi.

Così, sempre nell'ottica di una minimizzazione del rischio e in ossequio a finalità di trasparenza, in caso di *data breach* spetta al titolare del trattamento il compito di notificare quanto avvenuto all'autorità di controllo[231] dando così inizio a un'attività di collaborazione volta a circoscrivere e risolvere il problema, oltre che, nei casi più gravi, darne comunicazione all'interessato[232].

Per altro verso, anche la D.P.I.A. ex art. 35 e la consultazione preventiva ex art. 36, altro non sono che dei risvolti di questa mentalità, risolvendosi di fatto in strumenti che cercano di individuare e neutralizzare i possibili problemi, secondo una prognosi *ex ante*. Si tratta di un approccio la cui responsabilità ultima ricade in capo al titolare, tuttavia è evidente che, trattandosi di attività che richiedono competenze peculiari, il ruolo del D.P.O. diviene decisivo nel momento in cui ci si appresta ad affrontare il gravoso impegno di strutturare un'organizzazione complessa in modo da assicurarne la *compliance*.

Parimenti evidente è che la rilevanza dell'apporto del D.P.O. a questo compito consenta di ipotizzare la sussistenza di responsabilità in capo allo stesso anche dal punto di vista penalistico, considerato che, ai sensi dell'art. 39, par. 2 del regolamento, egli è chiamato a tenere in debita considerazione i fattori di rischio che si possono presentare nell'espletamento dei suoi incarichi.

Ora, posto che, come in qualsiasi professione, episodi che diano origine a responsabilità di carattere civile o penale possono verificarsi nello svolgimento ordinario delle proprie mansioni, vi sono senza dubbio alcune situazioni particolarmente delicate, sulle quali è

---

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.

[231] Cfr. art. 33, Regolamento (UE) 2016/679, par. 1.

[232] Cfr. art. 34, Regolamento (UE) 2016/679.

bene focalizzare l'attenzione ai fini che interessano la presente ricerca, perché il D.P.O. ivi è chiamato ad esprimersi, ed esporsi, in modo significativo.

3.1 D.P.O. e Data Protection Impact Assestment

La *Data Protection Impact Assestment* (Valutazione d'impatto sulla protezione dei dati) rappresenta forse il più importante strumento di prevenzione dei pericoli per la sicurezza dei dati e costituisce una significativa novità introdotta dal regolamento europeo.

Essa viene disposta, in ossequio all'art. 35, par. 1 del regolamento, quando un determinato trattamento potrebbe, per le caratteristiche dei dati trattati o per le metodologie utilizzate, mettere a rischio "i diritti e le libertà" delle persone coinvolte[233].

Può trattarsi, ad esempio, di casi in cui vengono messe in campo tecnologie nuove e ancora non sperimentate per il trattamento e l'analisi dei dati ma anche casi in cui dati importanti vengano diffusi o comunicati in paesi all'infuori dell'area europea, per tutte le motivazioni già citate.

Pure in questo caso, l'onere di riconoscere la necessità di provvedere alla D.P.I.A.[234] e di farvi fronte efficacemente spetta al titolare, che però ha l'obbligo di consultarsi con il D.P.O., ai sensi del par. 2 dell'art. 35.

Non si tratta di una previsione di poco conto: nella D.P.I.A. il ruolo del Data Protection Officer e l'apporto delle sue competenze vengono valorizzarti in modo significativo.

Il compito di "sorvegliante" dell'osservanza del regolamento in questo caso si manifesta nella necessità di fornire un parere a richiesta del titolare.

---

[233] Va ricordato che secondo il par. 5 dell'art. 35 del regolamento, le autorità di controllo possono adottare degli elenchi di tipologie di trattamenti che possono costituire oggetto di valutazione di impatto; il 25 settembre 2018 l'European Data Protection Board ha inviato il proprio parere, negativo, in relazione all'elenco approntato dal Garante Privacy italiano, Cfr. European Data Protection Board, O*pinion 12/2018 on the draft list of the competent supervisory authority of Italy regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR)*, 25.09.2018.

[234] Sul punto, è utile fare ricorso a: Gruppo di lavoro articolo 29, *Linee-guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del regolamento 2016/679,* adottate il 4 aprile 2017 Versione successivamente emendata e adottata il 4 ottobre 2017.

Ai sensi delle linee guida elaborate dal gruppo di lavoro articolo 29, il parere deve vertere sia sull'*an* che sul *quomodo* della valutazione: a chi affidarla, come leggerne i risultati e quali conclusioni trarne circa gli aspetti di *compliance* e l'opportunità di procedere al trattamento e all'utilizzo di dati.[235]

È bene ricordare che il titolare non è vincolato a seguire le opinioni del Data Protection Officer e le soluzioni da questi proposte, tuttavia si intuisce facilmente che la conoscenza dettagliata della normativa posseduta dal D.P.O., costituisce il *quid pluris* che rende di fatto assai autorevole il parere e i consigli tecnici da questi forniti al punto che, qualora il titolare volesse smarcarsene, sarebbe tenuto a esporre i motivi per i quali ritiene che l'osservanza del regolamento sarebbe assicurata da soluzioni diverse rispetto a quelle prospettate dal D.P.O.

Costui, d'altro canto, è tenuto a svolgere le sue valutazioni tenendo bene in considerazione i possibili pericoli che deriverebbero dal trattamento e il suo giudizio deve mantenersi indipendente dalle ricadute di tipo economico che la struttura potrebbe subire a causa della decisione di non effettuare il trattamento o di effettuarlo solo a determinate condizioni.

Sul punto chiaramente è lecito attendersi che possano crearsi tensioni fra le aspettative dei titolari o comunque i vertici di un'organizzazione e i doveri del D.P.O., nonché fra le aspettative di sfruttamento economico dei dati e la prudenza che sempre deve accompagnare la valutazione giuridica.

Pur nel dialogo fra le diverse esigenze, il D.P.O. è chiamato a fare in modo che vengano rispettate le disposizioni e i diritti previsti nel Regolamento (UE) 2016/679 e nelle altre normative dell'Unione in materia di tutela dei dati personali.

Pertanto, qualora un determinato trattamento venga posto in essere mettendo in pericolo la sicurezza di tali diritti e disposizioni e da ciò derivino conseguenze tali da integrare una fattispecie di reato, si deve ritenere, sulla scorta della considerazioni svolte nel terzo capitolo, che per il D.P.O. il quale non abbia segnalato i fattori di rischio in fase di D.P.I.A., eventualmente indicando al titolare la contrarietà del trattamento alle

[235] Gruppo di lavoro art. 29, *Linee guida sui responsabili della protezione dei dati*, op. cit., p.23.

disposizioni normative ovvero suggerendo il ricorso alla consultazione preventiva ex art. 34 del regolamento ovvero ancora qualora egli abbia dato esplicitamente il suo avallo a soluzioni non conformi al regolamento, sia ipotizzabile una responsabilità penale, stante la configurabilità di una posizione di garanzia che gli impone non già di compiere azioni di gestione che, come detto, non gli competono, bensì di assicurarsi che il titolare sia reso consapevole di tutte quelle situazioni che costituiscono un *vulnus* alla corretta applicazione della normativa e quindi alla sicurezza e integrità dei dati.

3.2. D.P.O. e Data Breach

Altro aspetto di primaria importanza riguarda gli adempimenti da assolvere in caso di *data breach*; questi rappresentano l'altra faccia della medaglia rispetto alla D.P.I.A. in quanto, se quest'ultima mira a neutralizzare *ex ante* i rischi che possono derivare dal trattamento, la notifica da farsi in caso di violazione dei dati introduce la procedura di emergenza quando una violazione c'è stata e occorre attivarsi quanto prima per porvi rimedio.

Anche con riguardo a questo punto, il regolamento si affida a criteri alquanto valutativi visto che tale notifica va fatta, in linea di principio, in ogni situazione di *data breach*, salvo i casi in cui "sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche"[236].

La notifica apre un processo di confronto con l'autorità garante volto a ottimizzare le procedure per circoscrivere i danni causati dalla violazione e risolvere, per quanto possibile, il problema alla radice.

In alcuni casi, quando la violazione abbia caratteristiche tali da "presentare un rischio elevato per i diritti e le libertà delle persone fisiche" occorrerà procedere anche alla comunicazione all'interessato ex art. 34 Regolamento (UE) 2016/679, al fine di metterlo

[236] art. 33, par. 1 Regolamento (UE) 2016/679, che esplicita pure che la notifica va fatta "senza ingiustificato e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza". Il fattore temporale è infatti decisivo in queste ipotesi.

al corrente della situazione e di coinvolgerlo nelle operazioni di risoluzione del problema[237].

Il Data Protection Officer, anche in questo caso, riveste un ruolo importante perché in virtù della sua specializzazione, dovrà essere in grado di identificare quali siano quelle violazioni che rispondono ai criteri individuati dal regolamento come base normativa dell'obbligo di notifica all'autorità garante[238].

Pure in questa situazione, ci si deve aspettare che possano crearsi dei conflitti fra le esigenze di trasparenza e sicurezza imposte dal regolamento e la tentazione, da parte di aziende e enti, di tenere il più possibile nascosti eventuali violazioni subite[239].

In ogni caso, ciò che più rileva dal punto di vista del Data Protection Officer è il fatto che egli sia chiamato a fungere da punto di contatto fra l'autorità garante e la struttura per quel che riguarda la gestione della vicenda, come da articolo 33, par. 3 lett b) e 39, par. 1, lett. e) del regolamento, così come avviene, d'altro canto, in caso di consultazione preventiva; in entrambi i casi infatti, il titolare ha l'obbligo di comunicare nomi e dati di contatto del responsabile della protezione dei dati all'autorità di controllo[240].

---

[237] Va pur segnalato che, in forza dell'art. 34, par. 3:
"Non è richiesta la comunicazione all'interessato di cui al paragrafo 1 se è soddisfatta una delle seguenti condizioni: a) 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; b) 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; c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia."

[238] In questo sono aiutati dal documento del Gruppo di lavoro art. 29, *Linee guida sulla notifica delle violazioni dei dati personali ai sensi del regolamento (UE) 2016/679*, adottate il 3 ottobre 2017 ed emendate e adottate in data 6 febbraio 2018 che con riferimento alle pp. 11-13 forniscono una serie di esempi in merito.

[239] Invero, va detto che almeno nei primi quattro mesi di vigenza del regolamento, si è forse concretizzato il rischio opposto dal momento che le notificazioni sono aumentate significativamente, Cfr. Garante per la protezione dei dati personali, *Il bilancio dei primi quattro mesi di applicazione del GDPR*, 04.10.2018, (https://www.garanteprivacy.it/regolamentoue/regolamento-ue-2016/679-il-bilancio-dei-primi-4-mesi-di-applicazione), Ultima cons. 22.10.2018.

[240] Invero, sul ruolo del D.P.O. in questo frangente le citate *Linee guida sulla notifica delle violazioni dei dati personali ai sensi del regolamento (UE) 2016/679* non aggiungono particolari elementi di novità rispetto a quanto già previsto dal regolamento.

Ecco quindi che diviene fondamentale che da parte sua vi sia una piena e leale collaborazione con l'autorità garante, cui deve comunicare le azioni e le eventuali omissioni commesse all'interno della struttura in cui opera. Qualora si comportasse diversamente è ragionevole ritenere che incorrerebbe nelle novellate fattispecie di reato di cui agli artt. 168 e 170 del d.lgs. 196/2003.

Si ribadisce infatti come il regolamento abbia voluto circondare di una serie di attributi e tutele il Data Protection Officer proprio per avere un soggetto competente e indipendente con il quale interloquire nelle situazioni emergenziali e che sarebbe illogico e, soprattutto, non funzionale agli scopi perseguiti dal regolamento, pensare di lasciarlo indenne da qualsiasi tipo di responsabilità.

Peraltro, è del tutto coerente ritenere che egli possa essere considerato responsabile qualora venga meno alle prescrizioni del Garante o fornisca scientemente indicazioni false.

4. Considerazioni conclusive

In conclusione, si possono senz'altro trarre alcune riflessioni che saranno importanti nel prossimo futuro.

Alla luce del regime di competenze tecniche richieste e della delicatezza delle problematiche inerenti alla protezione dei dati, che coinvolge profili di tutela della persona assai rilevanti, la figura del Data Protection Officer pare destinata ad assumere una sempre maggiore importanza.

Infatti, al di là di quelli che possono essere i compiti affidatigli, appare chiaro che l'apporto di competenze necessario per organizzare una efficace tutela della privacy nel contesto odierno sarà garantito principalmente da questa figura, il che è particolarmente rilevante in un momento in cui, a seguito dell'entrata in vigore del regolamento, molti rappresentanti del mondo delle imprese lamentano una difficoltà nel passare dall'enunciazione dei giusti e condivisibili principi del regolamento alla loro traduzione pratica.

Il fatto che, confrontandosi con operatori economici e non solo, la domanda che più ci si sente rivolgere è: "quindi cosa dobbiamo fare?", esprime tutta la difficoltà che si

sperimenta in questo momento nell'entrare nel nuovo meccanismo delineato dal principio di accountability. Infatti, una risposta univoca e a priori a questa domanda non può essere data, rendendosi necessario verificare le situazioni caso per caso.

Se la figura del Data Protection Officer sarà sviluppata intelligentemente, essa potrà costituire proprio quel punto di confronto capace di tradurre in operazioni pratiche le indicazioni del regolamento.

Se invece si vorrà declinare questa figura come l'ennesimo orpello giuridico da inserire nell'organigramma aziendale solo per "essere a posto", si perderà un'occasione importante, in particolare dal punto di vista strategico, per rispondere alla sfida dell'aggiornamento e della competitività rispetto alle aziende straniere.

Le iniziative di riforma del settore della tutela dei dati, infatti, sono tutt'altro che esaurite dal regolamento e dalla direttiva; è in corso processo di rivisitazione generale della materia e nei prossimi mesi dovrebbe vedere la luce, tra l'altro, il cd. *regolamento e-Privacy*, relativo in particolare alla tutela della vita privata e delle comunicazioni elettroniche; per questo assicurarsi sin da ora competenze all'altezza della sfida costituisce non solo un elemento di maggiore sicurezza ed affidabilità nell'ottica di una riduzione dei rischi ma anche, soprattutto una marcia in più nella capacità di cogliere le opportunità che sono comunque consentite dalle nuove disposizioni normative.

È chiaro però che, allo stato attuale, questa situazione presenti il rischio che anche chi voglia mettersi pienamente in linea con i dettati del regolamento si trovi comunque in una situazione di incertezza perchè, di fatto, l'unico modo per essere davvero sicuri di aver rispettato le prescrizioni legali è il sentirselo dire da un giudice, cosa che chiunque vorrebbe evitare visto che per arrivare alla serenità di questa conferma, è prima necessario aver affrontato l'ansia che vi siano stati dei problemi che abbiano reso necessario l'instaurarsi di un giudizio.

Trattandosi di una materia che per effetto dell'innovazione tecnologica presenta quotidianamente connotati nuovi, sarà opportuno che, specie in ambito penale, la giurisprudenza che si trovi a vagliare la responsabilità di un titolare del trattamento, di un responsabile o di un Data protection Officer, si ponga in un'ottica che tenga conto delle rilevanti problematiche tecniche e della difficoltà che un operatore di diritto

incontra nel cercare di prendere le migliori decisioni in questo settore, pur senza avallare, naturalmente, orientamenti lassisti.

Un aiuto nel senso di inquadrare correttamente le ripartizioni di responsabilità all'interno di una struttura potrebbe venire dall' introduzione dei reati in materia di privacy all'interno del d.lgs. 231/2001, il cui art. 24 bis, introdotto dalla l. 48/2008, tradisce questa aspettativa sinora mancata.

Nulla toglie, ovviamente, che le aziende possano organizzarsi autonomamente in tal senso, anzi, ciò è auspicabile perché permetterebbe sia di definire maggiormente sia i diversi profili di responsabilità ricoperti dalle varie figure che si occupano del trattamento dei dati, sia, di conseguenza, di organizzare in modo più efficace la loro gestione, sicurezza e il lecito utilizzo.

BIBLIOGRAFIA

Adam R., Tizzano A., *Manuale di diritto dell'Unione Europea*, seconda edizione, Giappichelli Editore, Torino, 2017.

Allegrezza R., *La Responsabilità penale del RSPP*, in "Osservatorio per il monitoraggio permanente della legislazione e giurisprudenza sulla sicurezza del lavoro presso la Facoltà di Giurisprudenza dell'Università degli Studi di Urbino "Carlo Bo", consultabile in www.cpt.sr.it.

Allegri M. R., *Informazione e comunicazione nell'ordinamento giuridico italiano*, Giappichelli Editore, Torino, 2012.

Antolisei F., *Il rapporto di causalità nel diritto penale,* G. Giappichelli, Torino, 1934.

Assonime – Associazione fra le società italiane per azioni, rassegna stampa 28 marzo 2018, consultabile in: www.assonime.it.

Attanasio D., *La responsabilità concorsuale del professionista nell'esercizio dell'attività di consulenza fiscale: è necessaria la "serialità" della condotta per l'integrazione della nuova circostanza aggravante*, in "Diritto penale contemporaneo", fasc, 5/2018.

Basile E., *Consiglio tecnico e responsabilità penale - Il concorso del professionista tramite azioni neutrali*, in "Itinerari di Diritto Penale (collana)", Giappichelli Editore, Torino, 2018.

Cairo L., Roberto G. (a cura di), *Figure e ruoli (artt. 4; 24; 26-29; 37-39) Contitolare e ripartizione delle responsabilità (Artt. 4, 26, 82)*, in "In Pratica GDPR", Leggi D'Italia, Wolter Kluwer, 2018.

Cajani F., Costabile G., Mazzaraco G., *Phishing e furto d'identità digitale. Indagini informatiche e sicurezza bancaria*, Giuffrè, Milano, 2008.

Califano L., Colapietro c. (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati nel Regolamento UE 2016/679*, in "Università degli Studi Roma Tre - CRISPEL (collana)- Sezione di diritto pubblico italiano ed europeo – Collettanee", Editoriale scientifica, Napoli, 2017.

Calzolaio S., *Protezione dei dati personali*, in *Digesto delle Discipline Pubblicistiche - Aggiornamento* - diretto da Sacco R.; Bifulco R., Celotto A., Olivetti M. (a cura di), Utet Giuridica, Milano, 2017.

Cangiotti M., *Dalla sfera privata alla sfera del diritto alla privacy. Evoluzione o distorsione dello spazio pubblico?*, in Congiunti L., Ndreca A., Formica G. (a cura di), *Oltre l'individualismo. Relazioni e relazionalità per ripensare l'identità*, Urbaniana University Press, Città del Vaticano 2017.

Cartabia M., *I nuovi diritti*, in "Stato, Chiese e pluralismo confessionale" - Rivista telematica, febbraio 2011, in www.statoechiese.it.

Ciarlo P., *Democrazia, partecipazione popolare e populismo al tempo della rete* in "Rivista AIC", fasc. n. 2/2018.

Clusit – Associazione italiana per la sicurezza informatica, *Rapporto Clusit 2018 sulla sicurezza ICT in Italia, nuova edizione settembre 2018,* Milano, 2018.

Cocca A., *La distinzione tra reati ad evento naturalistico e reati di mera condotta in funzione di disciplina*, in "Giurisprudenza Penale Web", 2017, 5, reperibile in http://www.giurisprudenzapenale.com.

Colombo E., *Una novità dall'unione europea per la lotta ai cybercrimes: una electronic evidence guide A Novelty from the European Union on the Fight against Cybercrimes: An Electronic Evidence Guide* in "Cassazione Penale", fasc. 1, 2014.

Comellini S., *Il Responsabile per la protezione dei Dati (Data Protection Officer-DPO)*, Maggioli Editore, Santarcangelo di Romagna, 2018.

Conigliaro S. C., *La nuova tutela penale europea dei sistemi di informazione. Una prima lettura della direttiva 2013/40/UE del Parlamento europeo e del Consiglio*, in "Diritto penale contemporaneo", 30 ottobre 2013, reperibile in https://www.penalecontemporaneo.it/.

Fellman D., *The Defendant Rights Today*, The University of Wisconsin Press, Wisconsin, 1976.

Fiandaca G., Musco E., *Manuale di diritto penale, parte generale*, Zanichelli, Bologna, 2014.

Flor R., *Phishing, identity theft e identity abuse. Le prospettive applicative del diritto penale vigente*, in "Rivista italiana di diritto e procedura penale", fasc. 2-3, 2007.

Frau R., nota alla sentenza del Tribunale di Milano, Sez. VI, 04.12.2014, tratta da "Responsabilità Civile e Previdenza", fasc. 3, anno 2015.

Frosini T. E., *Internet e democrazia*, in "Diritto dell'Informazione e dell'Informatica (Il)", fasc. 4-5, 2017.

Gaeta M. C., *La protezione dei dati personali nell'internet of things: l'esempio dei veicoli autonomi* in "Diritto dell'Informazione e dell'Informatica (Il)", fasc. 1, 2018.

Galdieri P. *Il domicilio informatico: l'interpretazione dell'articolo 615-ter c.p. tra ragioni di carattere sistematico e "forzature"* in "Diritto dell'informazione e dell'informatica (Il)", fasc.1, 2013.

Junker J.C., *Un nuovo inizio per l'Europa Il mio programma per l'occupazione, la crescita, l'equità e il cambiamento democratico Orientamenti politici per la prossima Commissione europea*, Strasburgo, 15 luglio 2014.

Lucente C.G., nota alla sentenza Cassazione Penale sez. VI, 04 ottobre 1999, n. 3067, in "Diritto dell'informazione e dell'informatica (Il)" 2001, fasc. 3.

Maglio M., Tilli N., Polini M. (a cura di), *Manuale di diritto alla protezione dei dati personali*, in "Professionisti e imprese" (collana), Maggioli Editore, Santarcangelo di Romagna, 2017.

Mantovani F., *L'obbligo di garanzia ricostruito alla luce dei principi di legalità, solidarietà, di libertà e di responsabilità personale* in "Rivista Italiana di Diritto e Procedura Penale", Fasc. II, 2001.

Mantovani F., *Diritto Penale, parte speciale, I, Delitti contro la persona*, Cedam, Padova, 2011.

Marinucci G. – Dolcini E., *Manuale di diritto penale, parte generale*, Giuffré, Milano, 2003.

Miglietti L., *Profili storico-comparativi del diritto alla privacy*, in "Diritti Comparati", 4 dicembre 2014, reperibile in www.diritticomparati.it.

Modafferi F., *Lezioni di diritto alla protezione dei dati personali, alla riservatezza e all'identità personale*, Lulu.com, Roma, 2015.

Crespi A. , Forti G. , Zuccala G., *Commentario breve al codice penale – complemento giurisprudenziale*, Wolters Kluwer, Cedam, Assago, Padova, 2014.

Monteleone M., massima a Cassazione Sezione I Civile; 27 Maggio 1975, n. 2129 in "Il Foro Italiano", Vol. 99, 1976.

Niger S., *Le nuove dimensioni della privacy, dal diritto alla riservatezza alla protezione dei dati personali*, in *Contratto e Impresa*, serie diretta da Francesco Galgano, Cedam, 2006.

Pagallo V. U., *La tutela dalla privacy negli Stati Uniti d'America e in Europa. Modelli giuridici a confronto*, Giuffrè Editore, Milano, 2008.

Pascucci P. *La consulenza e la giurisprudenza*, Relazione presentata al Convegno regionale su "Il lavoro e la salute nelle Marche: le possibili strategie per un intervento comune", organizzato dal Comitato regionale di coordinamento per la salute e sicurezza nei luoghi di lavoro delle Marche, Jesi, 27 settembre 2010, reperibile in www.cpt.sr.it.

Pascucci P., *La tutela della salute e della sicurezza sul lavoro: il titolo I del d.lgs. n .81/2008 dopo il Jobs Act*, in "Quaderni di Olympus" (Collana), Fano, Aras Edizioni, 2017.

Patalano A (a cura di), *Reg. (CE) 27-04-2016, n. 2016/679/UE, Articolo 29 - Trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento*, in "In Pratica GDPR", Leggi D'Italia, Wolter Kluwer, 2018.

Pellos G.M. (a cura di), *Il Data Protection Officer. Il responsabile dei dati personali dopo il D. Lgs. 10 agosto 2018, n. 101*, in "in "Le nuove leggi del diritto" (collana)," Dike giuridica, Roma, 2018.

Pessoa F., *Se depois de eu morrer* (1913-1915), in *Poemas Inconjuntos*, in "Atena" n. 5, febbraio 1925.

Piazza M. *Un recente arresto della cassazione in tema di molestia o disturbo alle persone: alcuni spunti di riflessione* in "Diritto Penale Contemporaneo", 19 aprile 2012, reperibile in www.penalecontemporaneo.it.

Piroddi P., *I trasferimenti di dati personali verso paesi terzi dopo la sentenza Schrems e nel nuovo regolamento generale sulla protezione dei dati*, in "Diritto dell'Informazione e dell'Informatica (Il)", fasc. 4-5, 2015.

Pizzetti F. (a cura di), *La protezione dei dati personali e la sfida dell'intelligenza artificiale*, in "I diritti nella 'rete' della rete", collana diretta da Pizzetti F., Giappichelli Editore, Torino, 2018.

Pizzetti F., *Privacy e il diritto europeo alla protezione dei dati personali, il regolamento europeo 2016/679*, Giappichelli Editore, Torino, 2016.

Pollicino O., Bassini M., *La carta dei diritti fondamentali dell'Unione Europea nel reasoning dei giudici di Lussemburgo*, in *Il diritto dell'Informazione e dell'Informatica*, anno XXXI, fasc. n. 4/5, 2015.

Pollicino O., *Un Digital Right To Privacy Preso (Troppo) Sul Serio Dai Giudici Di Lussemburgo? Il Ruolo Degli Artt. 7 E 8 Della Carta Di Nizza Nel Reasoning Di Google Spain* in "Diritto dell'Informazione e dell'Informatica (Il)", fasc.4-5, 2014.

Ponemon Institute, *Cost of cyber crime study 2017 insights on the security investments that make a difference*, Independently conducted by Ponemon Institute LLC and jointly developed by Accenture, Michigan, 2017.

Proli R., Valguarnera E., *Il Cybercrime e le strategie dell'Unione Europea*, in "Il diritto penale della globalizzazione", 28 agosto 2018, reperibile in www.dirittopenaleglobalizzazione.it.

Rodotà S. *Intervista su Privacy e Libertà* (a cura di Conti P.), Leterza, Bari, 2005.

Rodotà S., *Repertorio di fine secolo*, Laterza, Roma-Bari, 1992.

Rossi E.A., *Il diritto alla Privacy nel quadro giuridico europeo ed internazionale alla luce delle recenti vicende sulla sorveglianza di massa*, in "Diritto comunitario e degli scambi internazionali", n. 3/2014.

Warren S., Brandeis L., *The Right to Privacy*, in "Harvard Law Review", Vol. IV, December 15, 1890, n. 5.

Zappa F., *La criminalità informatica e i rischi per l'economia e le imprese a livello italiano ed europeo*, Progetto di ricerca per United Nations Interregional Crime and Justice Research Institute (UNICRI), 2014 consultabile al sito: www.unicri.it.

DOCUMENTI

Agenzia delle Entrate, *Risoluzione n. 140/E*, 15 novembre 2017.

Comitato Economico e Sociale Europeo, *Parere del Comitato economico e sociale europeo in merito alla Proposta di regolamento del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (regolamento generale sulla protezione dei dati), COM(2012) 11 final – 2012/0011 (COD)*, Bruxelles, 23 maggio 2012.

Commissione Europea - Alto Rappresentante dell'Unione per gli affari esteri e la politica di sicurezza, JOIN (2017) 450 FINAL, *comunicazione congiunta al parlamento europeo e al consiglio Resilienza, deterrenza e difesa: verso una cibersicurezza forte per l'UE*, Bruxelles, 13 settembre 2017.

Commissione europea – Comunicato stampa: *La Commissione europea e gli Stati Uniti concordano un nuovo quadro per i flussi transatlantici di dati: lo scudo UE-USA per la privacy*, Strasburgo, 2 febbraio 2016, IP/16/216.

Commissione europea, Comunicato stampa: *La Commissione europea lancia lo scudo UE-USA per la privacy: più tutele per i flussi transatlantici di dati*, IP/16/2461, Bruxelles, 12 luglio 2016.

Commissione Europea, *Comunicazione della Commissione al Parlamento Europeo e al Consiglio Ripristinare un clima di fiducia negli scambi di dati fra l'UE e gli USA*, Bruxelles, COM (2013) 846 final, 27 novembre 2013.

Commissione Europea, *Comunicazione della Commissione al Parlamento Europeo e al Consiglio sul funzionamento del regime "Approdo sicuro" dal punto di vista dei cittadini dell'UE e delle società ivi stabilite*, Bruxelles, COM(2013) 847 final, 27 novembre 2013.

Commissione Europea, *Comunicazione della commissione al parlamento europeo e al consiglio La strategia di sicurezza interna dell'UE in azione: cinque tappe verso un'Europa più sicura*, Bruxelles, 22.11.2010 COM (2010) 673 definitivo.

Commissione Europea, *Creare una società dell'informazione sicura migliorando la sicurezza delle infrastrutture dell'informazione e mediante la lotta alla criminalità informatica*. eEurope 2002 (COM(2000)890), 26 gennaio 2001.

Commissione Europea**,** *Proposta di Regolamento Del Parlamento Europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (regolamento generale sulla protezione dei dati) /* COM/2012/011 final - 2012/0011 (COD) */*, 25 gennaio 2012.

Commissione Europea, *Proposta di regolamento del Parlamento europeo e del Consiglio, concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati, COM (2012) 11 final, 2012/0011 (COD)*, relazione introduttiva, Bruxelles, 25 gennaio 2012.

Comunicato del Garante per la protezione dei dati personali, *Trasferimento dati personali verso gli USA: caducazione provvedimento del Garante del 10 ottobre 2001 di riconoscimento dell'accordo sul c.d. "Safe Harbor"*, Roma, 22 ottobre 2015.

Comunicazione della Commissione al Parlamento europeo e al Consiglio, *Ripristinare un clima di fiducia negli scambi di dati fra l'UE e gli USA*, COM (2013) 846 final, Bruxelles, 27 novembre 2013.

Consiglio dell'Unione Europea, Comunicato stampa 332/17, Portabilità dei servizi digitali nell'UE: il Consiglio adotta nuove norme, Bruxelles, 8 giugno 2017.

Consiglio dell'Unione Europea, Comunicato stampa 95/18, *Blocchi geografici: il Consiglio adotta un regolamento che rimuove gli ostacoli al commercio elettronico*, Bruxelles, 27 febbraio 2018.

Consiglio Europeo, *Conclusioni del Consiglio Europeo* del 19.10.2017, (OR. en) EUCO 14/17 CO EUR 17 CONCL 5, Bruxelles, 19 ottobre 2017.

Corte di Giustizia dell'Unione europea, comunicato stampa n. 111/15, *La normativa di uno Stato membro sulla tutela dei dati può essere applicata a una società straniera che svolge, in tale Stato, tramite un'organizzazione stabile, un'attività reale ed effettiva*, 1 ottobre 2015.

Corte di Giustizia dell'Unione europea, Sentenza del 13 maggio 2014, Causa C-131/12.

Council of the EU, Comunicato Stampa 360/17 End of roaming charges in the EU: Joint statement by the European Parliament, Bruxelles, 14 giugno 2017.

Consiglio dell'Unione Europea, *Decisione quadro 2005/222/GAI del Consiglio, del 24 febbraio 2005, relativa agli attacchi contro i sistemi di informazione*, 24 febbraio 2005.

European Data Protection Board, *Linee guida 2/2018 sulle deroghe di cui all'articolo 49 del regolamento 2016/679,* adottate il 25 maggio 2018.

European Data Protection Board, O*pinion 12/2018 on the draft list of the competent supervisory authority of Italy regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR)*, 25 settembre2018.

Garante europeo per la protezione dei dati, *Sintesi del parere del Garante europeo della protezione dei dati sulla comunicazione della Commissione al Parlamento europeo e al Consiglio "Ripristinare un clima di fiducia negli scambi di dati fra l'UE e gli USA" e sulla comunicazione della Commissione al Parlamento europeo e al Consiglio sul funzionamento del regime "Approdo sicuro" dal punto di vista dei cittadini dell'UE e delle aziende ivi stabilite* (2014/C116/04), Bruxelles, 20 febbraio 2014.

Garante Europeo per la Protezione dei dati, *Sintesi esecutiva del parere del Garante europeo della protezione dei dati: «La risposta alle sfide dei megadati: richiesta di trasparenza, controllo da parte degli utilizzatori, protezione dei dati fin dalla progettazione e responsabilità»* , Bruxelles, 19 Novembre 2015.

Garante per la protezione dei dati personali, *Discorso del Presidente Antonello Soro, Relazione 2017, Proteggere i dati per governarne la complessità*, Roma, 10 luglio 2018, in www.garanteprivacy.it.

Garante per la protezione dei dati personali, *Nuove Faq sul Responsabile della Protezione dei Dati (RPD) in ambito pubblico.*

Garante per la protezione dei dati personali, *Nuove Faq sul Responsabile della Protezione dei Dati (RPD) in ambito privato.*

Garante per la protezione dei dati personali, *Parere del Garante su uno schema di decreto legislativo recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679 dei Parlamento europeo e del Consiglio, del 27 aprile 2016*, Registro dei provvedimenti n. 312 del 22 maggio 2018.

Garante per la Protezione dei Dati Personali, *Regolamento privacy: come scegliere il responsabile della protezione dei dati. Le prime indicazioni del garante: necessarie competenze specifiche non attestati formali,* in newsletter n.432 del 15 settembre 2017, consultabile al sito https://www.garanteprivacy.it.

Gruppo di lavoro articolo 29, *Linee guida sulla notifica delle violazioni dei dati personali ai sensi del regolamento (UE) 2016/679*, adottate il 3 ottobre 2017 ed emendate e adottate in data 6 febbraio 2018.

Gruppo di lavoro articolo 29 era intervenuto con il documento di lavoro *Trasferimento di dati personali verso paesi terzi: applicazione degli articoli 25 e 26 della direttiva europea sulla tutela dei dati* del 24 luglio 1998.

Gruppo di lavoro Articolo 29 per la protezione dei dati, *Linee guida sui responsabili della protezione dei dati adottate il 13 dicembre 2016*, emendate in data 5 aprile 2017.

Gruppo di lavoro articolo 29 per la Protezione dei dati, *Parere 01/2012 sulle proposte di riforma in materia di protezione dei dati*, 23 marzo 2012.

Gruppo di lavoro articolo 29, *Linee guida per l'individuazione dell'autorità di controllo capofila in relazione a uno specifico titolare del trattamento o responsabile del trattamento*, 13 dicembre 2016, emendate il 5 aprile 2017.

Gruppo di lavoro articolo 29, *Linee-guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del regolamento 2016/679,* adottate il 4 aprile 2017 Versione successivamente emendata e adottata il 4 ottobre 2017.

Gruppo di lavoro articolo 29, *Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision*, 13 aprile 2016.

Parlamento europeo, Comunicati stampa – Giustizia e affari interni/Relazioni esterne, *Trasferimento dati UE-USA: necessari miglioramenti al "Privacy Shield"*, 26 maggio 2016.

Parlamento Europeo, *Posizione del Parlamento europeo definita in prima lettura il 12 marzo 2014 in vista dell'adozione del regolamento (UE) n. .../2014 del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali*

e la libera circolazione di tali dati (regolamento generale sulla protezione dei dati), 12 marzo 2014.

Parlamento Europeo, *Risoluzione del Parlamento europeo del 5 luglio 2018 sull'adeguatezza della protezione offerta dallo scudo UE-USA per la privacy* (2018/2645(RSP), 5 Luglio 2018.

Presidenza del consiglio dei Ministri, *Quadro strategico nazionale per la sicurezza dello spazio cibernetico,* Roma, Dicembre 2013.

GIURISPRUDENZA

Corte di Cassazione, Sezione I Civile, Sentenza n. 4487 del 22 Dicembre 1956.

Corte di Cassazione Civile, sentenza n. 990 del 20 aprile 1963.

Corte di Cassazione, Sezione I civile, sentenza n. 2129 del 27 maggio 1975.

Cassazione Penale, Sez. VI, sentenza n. 3067 del 04 ottobre 1999.

Corte europea dei Diritti dell'Uomo, 28 gennaio 2003, sentenza nella causa n. 44647/98,

Corte di Giustizia dell'Unione Europea, 6 novembre 2003, sentenza nella Causa C-101/01.

Cassazione Penale, Sezioni Unite, sentenza n. 45276 del 24 novembre 2003.

Cassazione, Sezione III Penale, sentenza n. 30134 del 28 maggio-9 luglio 2004.

Corte Europea dei Diritti dell'Uomo, 3 aprile 2007, sentenza nella causa n. 62617/00.

Corte Europea dei Diritti dell'Uomo, Grande Camera (Strasburgo), ricorsi nn. 30562/04 e 30566/04.

Cassazione Penale, Sez. I, sentenza n. 10730 del 18 febbraio 2009.

Cassazione Penale, Sez. IV, sentenza n. 1834 del 15 gennaio 2010.

Cassazione Penale, Sez. IV, sentenza n. 2814 del 27 gennaio 2011.

Corte Europea dei Diritti dell'Uomo, 9 ottobre 2012, sentenza nella causa n. 42811/06.

Cassazione Penale, Sez. V, sentenza n. 42021 del 12 luglio-19 ottobre 2012.

Cassazione Penale, Sez. IV, sentenza n. 49031 del 17 dicembre 2012.

Cassazione Penale, Sez. IV, sentenza n. 11492 del 11 marzo 2013.

Cassazione Penale, Sez. III, sentenza n. 7504 del 16 luglio 2013.

Corte di Cassazione, Sez. VI penale, n. 36125 del 13 maggio 2014.

Cassazione Penale, Sezioni Unite, sentenza n. 38343 del 18 settembre 2014.

Sentenza del Tribunale di Milano, Sez. VI, 04 dicembre 2014.

Cassazione Penale, Sez. III, sentenza n. 7504 del 18 dicembre 2014.

Cassazione Penale, Sez. IV sentenza n. 12223 del 03 febbraio 2015.

Cassazione Penale, Sez. III, sentenza n. 40103 del 5 febbraio 2015.

Cassazione Penale, Sez. I, sentenza n. 7643 del 19 febbraio 2015.

Cassazione, Sez. IV, sentenza n. 14007 del 02 aprile 2015.

Cassazione, Sez. IV, sentenza n. 14142 del 08 aprile 2015.

Corte di Giustizia dell'Unione Europea, 1° ottobre 2015, sentenza nella causa C-230/14,.

Corte di Giustizia dell'Unione Europea, Grande Sezione, 6 ottobre 2015, sentenza nella Causa C-362/14.

Cassazione, Sez. IV, sentenza n. 2541 del 21 gennaio 2016.

Cassazione, Sez. IV, sentenza n. 19029, del 20 aprile 2017.

Cassazione Penale, sez. IV, sentenza n. 45853 del 13 settembre 2017.

Cassazione Penale, sez. IV, sentenza n. 45862 del 14 settembre 2017.

Cassazione civile, sez. III, sentenza n. 24073 del 13 ottobre 2017.

Cassazione, Sez. IV, sentenza n. 2354 del 21 dicembre 2017.

Cassazione, Sez. III Penale, sentenza n. 1999 del 18 gennaio 2018.

Cassazione Civile, Sez. VI, sentenza n. 9158 del 12 aprile 2018.

TAR Friuli Venezia Giulia, sentenza n. 287 del 13 settembre 2018.