"GDPR – EVOLUZIONE ed APPLICAZIONE della NORMATIVA EUROPEA sulla PRIVACY"

INDICE

"GDPR – EVOLUZIONE ed APPLICAZIONE della NORMATIVA EUROPEA sulla PRIVACY"

INTRODUZIONE

La discussione riguardante il diritto alla privacy oggi si afferma come un argomento sempre più presente nella vita quotidiana a livello globale: sebbene le sue origini non siano così recenti come si pensi, si tratta sicuramente di una delle grandi sfide della giurisprudenza contemporanea. Questo avviene per cause sia quantitative che qualitative: da un lato assistiamo alla crescita esponenziale della mole di dati che vengono raccolti, trattati e conservati grazie ad *internet* ed ai *social network*; dall'altro all'evoluzione dei mezzi di comunicazione stessi grazie alle nuove tecnologie. A questo proposito basti pensare che "*Nel 1986, le informazioni che venivano scambiate attraverso sistemi bidirezionali di telecomunicazioni […] era dell'ordine di 281 PB*[1]*. Questa quantità di dati è salita […] a 65000 PB nel 2017*"[2]. Per dare al lettore un'ulteriore prospettiva dell'enormità delle cifre in questione, basti pensare che, secondo un articolo apparso su Repubblica, il Salk Institute for Biological Studies della California ha rilevato che il cervello umano ha una capacità di circa 1 petabyte a disposizione per archiviare le informazioni riguardanti una vita intera.[3]

Si può facilmente intuire come regolare questi titanici movimenti di dati a livello legale sia un'impresa complicata, che richiede al legislatore continui aggiornamenti per rimanere al passo con le innovazioni tecnologiche. Allo stesso tempo una legislazione organica e quanto più completa possibile è fondamentale per garantire ai cittadini un trattamento consono ed appropriato delle informazioni che li riguardano.

L'Unione Europea ha cercato di dare una risposta a tutte queste esigenze mettendo a punto l'ormai famoso *Regolamento UE 2016/679 del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati",* più noto con l'acronimo inglese di GDPR – General Data Protection Regulation.

L'intento di questa tesi è proprio quello di analizzare il GDPR per comprenderne il metro di ragionamento. Poiché non è possibile comprendere le norme di dettaglio senza prima avere

---

[1]. Il *petabyte* è un'unità di misura che serve a valutare la quantità di dati. Corrisponde alla 10^{15} *bytes* di informazioni, per cui si tratta di un valore molto grande

[2] (A. BIASIOTTI, *Il nuovo regolamento europeo sulla protezione dei dati,* III edizione, Roma, 2018, pag. 149)

[3] E. RE GARBAGNATI, *Il tuo cervello è un super computer: può memorizzare 1 petabyte di dati*, in *Repubblica.it*, 24 gen 2016

un'idea di cosa si intenda per "diritto alla privacy", per prima cosa si introdurrà al lettore il punto di vista storico, in modo da comprendere quali siano le spinte che hanno portato all'inclusione di un nuovo diritto nella giurisprudenza occidentale. A partire dagli Stati Uniti, questa ulteriore fattispecie si è diffusa, non senza difficoltà, nel continente europeo, dove alcuni Stati hanno giocato il ruolo di alfiere, emanando leggi dedicate molto prima dell'intervento del legislatore europeo. Queste legislazioni nazionali saranno analizzate per comprendere i diversi approcci che i singoli Paesi hanno adottato, anche alla luce delle diverse situazioni storico-politiche. Con l'azione dell'Unione europea, il panorama cambia significativamente, in quanto tutti gli Stati membri sono obbligati a riconoscere questo diritto. Un grande passo avanti, che però come si vedrà è ancora lontano da una situazione di certezza normativa.

A questo punto l'Unione europea diventa la vera protagonista, sia nella realtà che in questa trattazione, in quanto sono le sue scelte a determinare il quadro che si va creando via via, non senza numerosi intralci. Sarà quindi presentato il processo di formazione del nuovo regolamento, per comprendere il percorso normativo "stratificato" avvenuto in seno all'UE, nel trattare il quale si darà particolare attenzione ai pareri degli organi tecnici intervenuti, oltre che a quelli più prettamente politici.

Solo alla fine di questo percorso al lettore sarà esposto il contenuto vero e proprio del regolamento, nelle sue parti più significative, proprio nell'intento di spiegare il meccanismo attuale tramite il quale i dati di ciascun cittadino all'interno dell'Unione europea sono protetti, insieme al corpo di diritti "derivati" dal diritto alla privacy, vale a dire tutte quelle azioni che il singolo stesso può porre in essere per proteggere autonomamente la propria sfera intima.

Infine ci si propone di spostare la lente d'ingrandimento sull'Italia, per studiare, con una logica molto simile a quella già usata per l'Unione Europea, l'evoluzione e l'applicazione della tutela della privatezza. In prospettiva storica, sarà presentato al lettore il ruolo cruciale assunto dalla giurisprudenza italiana, che è stata il vero motore nell'innovazione dell'ordinamento, con largo anticipo rispetto ai poteri legislativi ed esecutivi.

La tesi si concluderà quindi con uno sguardo pratico all'applicazione del GDPR nella realtà delle piccole e medie imprese in Italia, nonché per alcune particolari categorie di cittadini, per poter comprendere come la tutela della privacy possa impattare la vita quotidiana di ogni singolo cittadino nei modi più disparati.

CAPITOLO 1 – Prospettiva storico-comparata

1.1 La nascita del diritto alla privacy: "Right to Privacy" di Warren e Brandeis

Norberto Bobbio sostiene che i diritti umani *"sono diritti storici, cioè nati in certe circostanze [...] gradualmente, non tutti in una volta e non una volta per sempre"*[4]. Non stupisce, quindi, che la prima definizione del diritto alla privacy risalga alla fine del XIX sec., in quanto la diffusione dei primi apparecchi fotografici e delle prime testate scandalistiche, poneva appunto un problema di tutela dell'immagine e della reputazione dei soggetti, che venivano posti sotto l'occhio del pubblico e che tale definizione sia stata coniata negli Stati Uniti, Paese all'avanguardia nel dibattito giuridico dell'epoca.

Ciò che invece potrebbe stupire è il fatto che la definizione che qui si analizza non nasca da una sentenza o da una proposta di legge, quanto piuttosto da un *gossip*. Ebbene sì, pare che una delle motivazioni che spinse Samuel D. Warren a scrivere un articolo in difesa del diritto alla *privacy*, insieme al suo socio e futuro giudice della Corte Suprema, Louis D. Brandeis, fu l'essere costantemente bersagliato dai giornali scandalistici di Boston a causa delle numerose e manifeste infedeltà della moglie.

Un articolo avente ad oggetto proprio il diritto alla privacy apparve per la prima volta il 15 dicembre 1890 sulla prestigiosa Harvard Law Review ed ebbe una portata rivoluzionaria[5]. Il grande merito di Warren e Brandeis fu il definire la privacy come un diritto autonomo, separato ed indipendente da altri istituti, che riguardavano, comunque, la reputazione delle persone come la calunnia e la diffamazione ("*slander and libel*" che secondo il saggio stesso possono essere già rintracciati nel XIV sec.) o ancora dai diritti di proprietà intellettuale ("*works of literature and art, goodwill, trade secrets and trade marks*").[6]

Il diritto alla privacy è riassunto nella fortunata espressione *"the right to be let alone"* ovvero il "diritto di essere lasciati in pace", configurandosi quindi come un diritto "negativo" di tipico stampo liberale. Nell'Ottocento infatti dal liberismo economico era nato il liberalismo a livello politico: una dottrina basata sui diritti individuali, concepiti come prerogativa naturale dell'uomo. In quest'ottica, l'autorità pubblica esisteva in funzione delle garanzie che essa poteva dare all'individuo. Pertanto non si trattava di uno Stato obbligato a "fare" per garantire il welfare dei cittadini, quanto piuttosto uno Stato che doveva "non fare" limitandosi a proteggere la libertà dei cittadini, senza ulteriori interferenze. Infatti per Warren e Brandeis, la privacy è un diritto da

[4] N. BOBBIO, L'età dei diritti, Torino, 1990, p. 13-14
[5] Si tratta di "Right to privacy" di Samuel D. Warren e Louis D, Brandeis.
[6] S.D. WARREN, L.D. BRANDEIS, Right to privacy, in Harvard Law Review, 1890, p. 194-195

difendere e proteggere contro le invasioni esterne: la protezione statale deve fermarsi a questa soglia e non può in alcun modo interferire sulla sfera interna, di cui il cittadino è l'unico titolare.

Il saggio denuncia l'inadeguatezza degli strumenti legali fino ad allora utilizzati, lontani sia per premesse che per finalità dal *"right to be let alone*" che è prerogativa dell'individuo. L'intuizione principale è quella che distingue il raggio d'azione dei diritti della persona ancora una volta in chiave liberale. Seguendo una concezione prettamente mercantilistica, Warren e Brandeis osservano che la legge contro la calunnia protegge la persona nelle sue relazioni esterne, configurandosi di fatto come un'estensione del diritto di proprietà. Infatti la reputazione di un uomo è monetizzabile esattamente quanto quella di un marchio: una buona reputazione implica fiducia in tutte le transazioni umane. Ma se la legge protegge solo la reputazione esterna, si rende anche necessaria una legge che protegga la sfera interna dell'individuo: la natura dei reati riconosciuti dalla legge dello *slander and libel* è materiale e non spirituale, perciò non si riconosce alcuna riparazione per i danni arrecati ai sentimenti dell'offeso.[7]

I due avvocati passano poi ad un'analisi accurata di svariati provvedimenti giudiziari estrapolati dalla *common law* a sostegno della propria tesi. Fra questi merita una menzione la sentenza Millar v. Taylor del 1769, in cui già si individua il diritto a non rendere pubblici i propri pensieri (oltre ovviamente al caso di testimonianza in un processo). Naturale corollario di questa affermazione è il fatto che i pensieri siano protetti dalla privacy, indipendentemente dal mezzo materiale a cui sono affidati, sia esso un diario o un saggio.[8] Pertanto il diritto alla privacy si configura come qualcosa di altro anche rispetto ai diritti di copyright, in quanto questi proteggono l'autore nel momento in cui decide di pubblicare i propri lavori, mentre il nuovo diritto di Warren e Brandeis si arresta appunto alle soglie della pubblicazione, dopo la quale ragionevolmente cessa la sua protezione. È questa una concezione decisamente moderna, da cui di fatto scaturirà il principio del consenso: è l'interessato che decide liberamente e consapevolmente di mettere a disposizione di altri informazioni relative alla sua sfera professionale.

Giova ribadire che il limite oltre cui non si applica il diritto alla privacy è il pubblicare e non l'intenzione di farlo. La medesima protezione è ragionevolmente accordata all'autore di qualsiasi scritto, indipendentemente dalla pubblicabilità e monetizzabilità dello stesso. In pratica

---

[7] "*In short, the wrongs and correlative rights recognized by the law of slender and libel are in their nature material rather than spritual. That branch of the law simply extends the protection surrounding phisical property* […] *On the other hand, our law recognizes no principle upon which compensation can be granted for mere injury tot he feelings."* (S.D. WARREN, L.D. BRANDEIS, *Right to privacy*, in *Harvard Law Review*, 1890, p. 197)

[8] "*The same protection is accorded to a casual letter or an entry in a diary and to the most valuable poem or essay* […] *In every such case the individual is entitled to decide whether that which is his, shall be given to the public"* (S.D. WARREN, L.D. BRANDEIS, *Right to privacy*, in *Harvard Law Review*, 1890, p. 199)

l'intrusione concreta nella vita di un cittadino non è più l'unico presupposto per ottenere delle garanzie: il diritto alla privacy non protegge un bene oggettivamente misurabile, ma il valore che l'interessato attribuisce alla propria sfera privata.

Questa visione moderna del diritto, che mette al centro la persona e le proprie prerogative rispetto al valore giuridico-commerciale, è sopravvissuta ed è tornata alla ribalta in anni recenti. Ad oggi non vi sono dubbi sul fatto che siano i singoli a disporre liberamente dei propri dati e che questo diritto superi la ragion di mercato. Basti pensare a quanto è stata progressivamente ridotta la sfera di controllo sulla profilazione a fini commerciali: oggi l'individuo può attivare i propri diritti di accesso e di oblio quando vuole, senza bisogno di giustificazioni, a scapito delle imprese che utilizzano quei dati a scopi di marketing. La logica di Warren e Brandeis si configura quindi come quanto mai attuale, diventando una componente fondamentale della nostra vita di tutti i giorni.

1.*1.2 William Prosser e il dibattito negli Stati Uniti*

Uno dei critici più noti delle teorie di Warren e Brandeis è William Prosser, che nel suo saggio "Privacy", pubblicato nel 1960 sulla California Law Review, divide le fattispecie di violazione della privacy in quattro casi, ossia (i) intrusione negli affari privati dell'interessato; (ii) divulgazione pubblica di fatti privati o "delicati" riguardanti l'interessato; (iii) notorietà che pone l'interessato in cattiva luce agli occhi del pubblico; (iv) appropriazione dell'identità e/o delle sembianze dell'interessato a proprio vantaggio.

La prima cosa che salta agli occhi è che, per affermazione dello stesso Prosser, si tratta di categorie "*loosely related"*[9], specie se contrapposte al principio unitario che avrebbe dovuto caratterizzare la privacy secondo Warren e Brandeis. Ciononostante, fra le due teorie, fu proprio lo schema di Prosser ad avere maggior successo nelle aule di tribunale: già nel 1964, ben prima della prima legge federale sulla privacy, il suo "quadrilatero" era comunemente utilizzato nella *common law* di trentadue Stati, nei codici di altri quattro, oltre ad essere in via di approvazione in quattro ulteriori Stati.[10] Richards e Solove sintetizzano magistralmente il suo contributo alla legge americana, affermando che prima di Prosser i tribunali consideravano se i casi rientrassero o meno nell'ampio "diritto di essere lasciati in pace", mentre dopo Prosser tutti i casi dovevano essere divisi nei suoi quattro illeciti.[11]

---

[9] Debolmente collegate fra loro

[10] Fu lo stesso Prosser ad annunciare questi successi nel capitolo dedicato alla privacy della terza edizione del suo "HANDBOOK OF THE LAW OF TORTS" del 1964.

[11] *"Before Prosser, courts looked to Warren and Brandeis's article and examined whether particular harms fell under the very broad principle of the "right to be let alone". After Prosser, courts looked to whether a particular harm fi tinto one of Prosser's four categories"* (N. M. RICHARDS, D.J. SOLOVE,

Un'altra differenza sostanziale fra l'approccio di Warren e Brandeis e quello di Prosser sta nel rapporto con la common law: se i primi ne criticano l'inadeguatezza, premendo per una sua evoluzione in senso estensivo, Prosser fa esattamente il contrario. Il suo metodo infatti trova nella common law il proprio punto di partenza e la propria legittimazione finale. Il lavoro di Prosser si divide infatti in tre fasi principali: (i) categorizzazione dei casi giuridici per "estrarre" la fattispecie; (ii) adozione delle sue categorie da parte delle Corti; (iii) citazione delle sentenze di queste Corti a riprova dell'efficacia della categorizzazione applicata.

Prosser intende quindi mettere ordine in ciò che già esiste di fatto nella legge americana, senza creare nulla di nuovo. Non a caso egli stesso preferisce definirsi un "catalogatore" piuttosto che un inventore. Egli non intende rivoluzionare il mondo della privacy, quanto piuttosto riordinarlo e renderlo più facilmente fruibile agli attori della legge.

Proprio per questo, nonostante l'indubbio merito di aver portato ordine nel caos delle sentenze riguardanti la privacy germogliate nel cinquantennio seguente all'affermazione del cd. "Right to Privacy", oggi ci si chiede se la divisione di Prosser non abbia posto un freno allo sviluppo della materia. Una categorizzazione così stretta e rigida, pur provvedendo un'utile chiave di lettura delle sentenze in materia di privacy, sembra inibire ulteriori e imprevisti sviluppi delle garanzie che il diritto alla privacy dovrebbe dare nell'Information Era. Come sostengono Neil M. Richards e Daniel J. Solove, nel categorizzare quattro tipi di violazione della privacy, Prosser ha dato una statura ufficiale e una legittimazione giuridica alla materia, rendendola però rigida e difficilmente adattabile a eventuali sviluppi tecnologici e sociali.[12]

1.1.3 Il quadro federale e il Privacy Act del 1974

Dopo aver analizzato i due principali filoni teorici che caratterizzano l'approccio alla privacy nello Stato che ne vide i natali, è naturale domandarsi quali siano stati gli effetti giuridici concreti di un dibattito tanto acceso. Fino ad ora infatti tutti i processi o gli atti normativi nominati riguardano i singoli Stati americani, senza coinvolgere il livello federale. Questo perché, fino agli

Prosser's Privacy Law: A Mixed Legacy, in *GW Law Publications & Other Works*, 2010, Vol. 98:1887 pag. 1915)

[12] *"Although Prosser gave tort privacy order and legitimacy, he also stunted its development in ways that have limited its ability to adapt to the problems of the Information Age* […] *Prosser thus greatly increased tort privacy's stature at the cost of making it harder for privacy law to adapt to new circumstances in the future*." (N. M. RICHARDS, D.J. SOLOVE, *Prosser's Privacy Law: A Mixed Legacy,* in *GW Law Publications & Other Works*, 2010, Vol. 98:1887 pag. 1890)

anni Sessanta, le cause riguardanti la privacy venivano ascritte al livello privato e perciò non venivano sottoposte a scrutinio di costituzionalità.

Tuttavia risulta evidente come il diritto alla privacy andasse necessariamente bilanciato da uno dei pilastri della Costituzione americana, più precisamente si tratta del primo Emendamento, che garantisce la libertà religiosa, di culto, di parola e di stampa, oltre al diritto di riunirsi pacificamente e di appellarsi alla legge per la compensazione dei torti.[13] La prima soluzione pratica applicata dalle Corti statunitensi fu quella di soppesare i due interessi: da un lato i diritti del querelante e dall'altro il primo Emendamento.[14]

A livello federale fu la Corte Suprema a dare una svolta a questa situazione di incertezza: nel caso *New York Times Co v. Sullivan* del 1964[15], venne dichiarato che le garanzie alla libertà di parola presenti nel I Emendamento potevano restringere la possibilità di un pubblico ufficiale (o di un cittadino che concorresse per diventarlo) di sporgere denuncia per diffamazione. Senza addentrarsi nello specifico della sentenza, il principio che qui interessa sottolineare è che le leggi statali sulla privacy avrebbero dovuto garantire un livello minimo di protezione alla libertà di parola e di stampa, pena l'essere dichiarate incostituzionali sulla base del I Emendamento.

La tanto attesa legge federale in materia di privacy arrivò solo nel 1974 (ben 84 anni dopo l'articolo di Warren e Brandeis) con il nome di Privacy Act. Secondo il sito del Dipartimento di Giustizia statunitense, gli obiettivi primari di questo atto erano da un lato una regolamentazione dei comportamenti delle agenzie governative, che dovevano limitare in più possibile la divulgazione di informazioni riguardanti persone identificabili e sottostare a un più stringente codice comportamentale; dall'altro l'aumento delle garanzie accordate agli individui, che si sarebbe tradotto in un più ampio diritto di accesso e rettifica nei confronti dei propri dati.

---

[13] *"Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances"* (I UNITED STATES CONGRESS, *United States Bill of Rights* 15 dic 1791, New York)

[14] "*In torts such as defamation or the disclosure of private facts, the First Amendment interests were weighed against the plaintiff's interests in her reputation or the emotional injury that would result from publication*" (N. M. RICHARDS, D.J. SOLOVE, Prosser's Privacy Law: A Mixed Legacy, in GW Law Publications & Other Works, 2010, Vol. 98:1887 pag. 1902).

[15] New York Times Co. v. Sullivan, 376 U.S. 254 (1964) fu una sentenza rivoluzionaria nella storia americana. Il caso però ebbe inizio nel 1960, durante la lotta per i diritti civili. In una pagina pubblicitaria finanziata da sostenitori di Martin Luther King comparvero informazioni che ponevano in cattiva luce il dipartimento di polizia di Montgomery (Alabama). Parte delle notizie inoltre era inaccurata o inesatta, per cui il commissario L.P. Sullivan portò il Times davanti alla Corte della contea per diffamazione. Il primo processo si risolse in una condanna per il Times, confermata anche in appello dalla Corte Suprema dell'Alabama con l'argomentazione che l'inesattezza delle notizie pubblicate costituiva reato di per sé. Il processo ebbe una svolta con l'appello alla Corte Suprema degli Stati Uniti, la quale con un verdetto di 9 favorevoli e 0 contrari rovesciò la sentenza, affermando che le decisioni precedenti violavano il I Emendamento.

Poiché l'obiettivo di questa tesi non è l'analisi del Privacy Act, ci si limiterà a considerare gli elementi principali di questa disposizione. Per prima cosa viene introdotto il principio secondo cui nessuna informazione personale può essere comunicata a terzi dalle agenzie federali senza il consenso dell'"interessato" (mi si perdoni questa nomenclatura tipicamente europea). [16]

A questo principio generale sono date però alcune eccezioni, quali scopi storico-statistici di enti pubblici o comunque usi necessari alle agenzie federali o ancora indagini condotte dal Congresso e rispetto delle leggi.

Sempre nell'ottica di un maggiore controllo dei propri dati da parte dell'individuo, sono stati introdotti il diritto di accesso e quello di emendamento. Il primo stabilisce il diritto in capo all'individuo di visionare i dati che lo riguardano contenuti nei database federali, nonché di farne una copia, mentre tramite il secondo l'individuo può richiedere la "correzione" dei propri dati conservati da un'agenzia federale.

È importante aggiungere che questo provvedimento nel tempo è stato integrato da altri atti "modernizzatori" e complementari. Il primo in ordine cronologico è il Computer Matching and Privacy Protection Act del 1988, riguardante ciò che venne definito come la comparazione computerizzata di sistemi di archiviazione federali.[17]

Il secondo è l'E-Government Act del 2002, introdotto allo scopo di migliorare e regolare i servizi elettronici governativi. Una delle novità di questo provvedimento fu l'introduzione di un Chief Information Officer nominato dal Presidente stesso presso l'Office of Management and budget, che nulla ha a che vedere con la figura del Garante in Unione Europea. Il Chief Information Officer infatti agisce più come un amministratore che come una figura di controllo: decide le spese e le politiche riguardanti le tecnologie informatiche, nonché gli investimenti federali in questo campo.

Infine troviamo il Judicial Redress Act del 2015 (Public Law 114–126114th Congress) che estende le possibilità di ricorso giudiziario già previste dal Privacy Act alle persone fisiche provenienti da 28 Paesi od organizzazioni regionali.

La novità è che l'Unione Europea rientra proprio in queste ultime, ed infatti nel 2016 viene firmato il Data Protection and Privacy Agreement, che garantisce collaborazione fra le parti con il

[16] "*No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains...*" (The Privacy Act of 1974, UNITED STATES DEPARTMENT OF JUSTICE).

[17] " *(i) two or more automated systems of records with a set of non-Federal records (ii) two or more automated Federal personnel or payroll systems of records or a system of Federal personnel or payroll records with a set of non-Federal records*" (Computer Matching and Privacy Protection Act of 1988, Pub. L. 100-503)

proposito di "prevenire, individuare, investigare o perseguire atti criminali" (sito department of justice). L'articolo 19 in particolare prevede l'obbligo per gli ordinamenti dei "covered countries" di garantire possibilità di ricorso reciproche.

1.2 Pionieri in Europa: le legislazioni in materia di privacy in Germania, Francia e Regno Unito

Poiché lo scopo di questo capitolo è un'analisi storico-comparata dell'evoluzione delle tutele della privacy, non è necessario soffermarsi sul contenuto specifico di ciascun atto, quanto piuttosto considerare le diverse circostanze storiche che hanno portato questi Paesi ad adottare legislazioni in materia di privacy prima del legislatore europeo. [18]

1.2.1 Il Bundesdatenschutzgesetz e la Guerra Fredda

Cronologicamente, la prima legge sulla protezione dei dati del mondo fu adottata nella Repubblica Federale Tedesca (o Germania Ovest) dallo Stato federale dell'Assia nel 1970. Da questa legge statale l'anno seguente scaturì un progetto di legge federale che, dopo varie peripezie, diede alla luce il *Bundesdatenschutzgesetz* (BDSG), entrato in vigore il 1 gennaio 1978. L'obiettivo della legge era stabilire norme precise sulla gestione dei dati, sia che fossero processati manualmente che attraverso *software*. Il passo successivo si ebbe nel 1983, anno in cui era previsto il primo censimento automatizzato dei cittadini tedeschi, che reagirono con centinaia di petizioni e ricorsi contro questo provvedimento, forse troppo "orientale" per i cittadini della *Bundesrepublik Deutschlands* (BRD) Si giunse ad un verdetto della Bundesverfassungsgericht, l'organo di controllo costituzionale tedesco, che diede al diritto alla privacy rango costituzionale, sotto la protezione degli articoli 1 e 2 della Legge Fondamentale della BRD, riguardanti le libertà e la protezione della dignità umana.[19] A questo punto non restava che adottare una nuova legge in materia di protezione dei dati a livello federale, che arrivò nel 1990.

---

[18] Ci si riferisce in particolare alla Direttiva 95/46/CE del Parlamento Europeo e del Consiglio, del 24 ottobre 1995 "*relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati",* che qui si considera come "direttiva madre" in quanto per la prima volta sorse l'obbligo in capo a tutti i Paesi membri di adottare un atto adeguato alla protezione della privacy. Naturalmente il legislatore europeo aveva già da tempo provveduto ad inserire simili tutele nei propri atti fondamentali, ma di questo argomento ci si occuperà nel capitolo seguente.

[19] *"Articolo 1 [Protezione della dignità umana]*
(1) La dignità dell'uomo è intangibile. È dovere di ogni potere statale rispettarla e proteggerla. (2) Il popolo tedesco riconosce gli inviolabili e inalienabili diritti dell'uomo come fondamento di ogni comunità umana, della pace e della giustizia nel mondo. (3) I seguenti diritti fondamentali vincolano la legislazione, il potere esecutivo e la giurisdizione come diritti direttamente applicabili.
Articolo 2 [Diritti di libertà]
(1) Ognuno ha diritto al libero sviluppo della propria personalità, in quanto non violi i diritti degli altri e non trasgredisca l'ordinamento costituzionale o la legge morale. (2) Ognuno ha diritto alla vita e all'integrità fisica. La libertà della persona è inviolabile. Solo la legge può limitare questi diritti."(E. PALICI DI SUNI PRAT, F. CASSELLA, M. COMBA, *Le Costituzioni dei Paesi dell'Unione Europea*, Padova, CEDAM, 1998)

Non sfuggirà al lettore che tutto il processo sopra descritto ebbe origine nella sola Germania Ovest. Vale la pena quindi domandarsi cosa stesse accadendo negli stessi anni dall'altra parte della cortina di ferro, ovvero nella Repubblica Democratica Tedesca. Nei primi anni Settanta la DDR[20] era retta dal Consiglio di Stato capeggiato da Walter Ulbricht e dai rappresentanti del suo partito, la SED[21], che continuava a mantenere saldamente in pugno lo Stato attraverso l'applicazione del modello socialista diffuso in tutto il blocco sovietico. Si era quindi molto lontani dal clima di riavvicinamento fra le due Germanie che si sarebbe instaurato in seguito, anzi Ulbricht si rese protagonista di una politica di rafforzamento dei legami con i Paesi del Patto di Varsavia e quindi, come diretta conseguenza, di allontanamento dall'Occidente. In questo modo il leader della SED sperava di fare pressione sulla Repubblica Federale Tedesca e sugli altri Paesi europei affichè riconoscessero ufficialmente la DDR.

La storia della Repubblica Democratica Tedesca è tristemente segnata dalle vicende riguardanti la Stasi[22], la temuta polizia politica al servizio (almeno in teoria) del Consiglio dei Ministri. Di fatto questo organismo, oltre ad occuparsi dello spionaggio estero, esercitava un ossessivo e capillare controllo della vita dei cittadini della DDR: "*Attraverso metodi non sempre ortodossi essa poteva garantire l'eliminazione politica, se non addirittura fisica, di chiunque tentasse di porre in dubbio l'egemonia della SED, ossia del Partito Socialista Unificato. In realtà, fu soprattutto a partire dal 1957, anno della nomina a direttore di Erich Mielke, che la Stasi iniziò a trasformarsi in una vera e propria macchina di sorveglianza*."[23] Con un agente circa ogni 83 abitanti, la Stasi era quindi il più efficiente e impressionante apparato statale di controllo ed elaborazione di informazioni in Europa, più efficiente dello stesso KGB sovietico. Letta all'inverso, la Stasi era la responsabile della violazione sistematica della privacy verosimilmente di ogni cittadino sotto la propria giurisdizione, non disdegnando metodi quali le intercettazioni segrete, il controllo della corrispondenza privata o l'installazione di microfoni nelle abitazioni.
È chiaro quindi che la leadership della Germania Ovest avesse tutto l'interesse ad elevarsi a difensore della sfera privata dei propri cittadini, in netto contrasto con la propria metà orientale.

Naturalmente la nascita del BDSG ha anche origine nella diffusione dei primi procedimenti automatizzati e computerizzati, ma non è certo un caso che sia stata proprio la Germania ad

[20] Acronimo di *Deutsche Demokratische Republik*, ovvero Repubblica Democratica Tedesca.
[21] Acronimo di *Sozialistische Einheitspartei Deutschlands*, ovvero Partito di Unità Socialista tedesco, egemone indiscusso della DDR per tutta la sua storia (dal 1949 fino al 1990).
[22] Abbreviazione di *Ministerium für Staatssicherheit*, ovvero il nome del Ministero per la Sicurezza di Stato, da cui questo organismo dipendeva.
[23] (A. GOGGIO, *Controllori Controllati: Le Finestre Della Stasi*. in Altre Modernità 1 (2015): 181–195. Web.)

affrontare per prima questa rivoluzione nello scenario europeo. Bisogna infatti ricordare che la Guerra Fredda fu in gran parte una contrapposizione fra stili di vita: se a livello consumistico la bandiera dell'Occidente fu la diffusione dei beni di consumo su larga scala, a livello giuridico il secondo dopoguerra si caratterizza per l'ampliarsi dei diritti umani e della persona. All'equazione capitalismo/liberismo contro socialismo/comunismo non è poi così strano aggiungere l'antitesi fra invasione e rispetto della sfera privata del singolo.

1.2.2 Il progetto Safari e la Loi Informatique et Libertes

Nello stesso anno in cui BRD dava alla luce il *Bundesdatenschutzgesetz*, in Francia entrava in vigore la legge 78/17 del 6 gennaio 1978, nota anche con il nome francese di "*Loi Informatique et Libertes"*. Nel caso francese però si giunse alla stesura della legge dopo un forte tumulto mediatico che giunse a coinvolgere l'allora Ministro dell'Interno Jacques Chirac. Tutto ebbe inizio il 21 marzo 1974, quando sul noto quotidiano francese Le Monde venne pubblicato un articolo intitolato "*SAFARI ou la chasse aux Français"*[24] in cui si svelava l'esistenza di un progetto, dal nome esteso di "Système Sutomatisé pour les Fichiers Administratifs et le Répertoire des Individus" con lo scopo creare un database nazionale che avrebbe consentito l'identificazione di ciascun cittadino francese da parte di svariati uffici governativi. Nonostante la smentita di Chirac stesso, apparsa sul quotidiano il giorno successivo, la notizia scatenò un'ondata di sdegno verso il Governo da parte del pubblico che non voleva essere "schedato". [25]

Questo spinse il Governo francese a dare una maggiore regolamentazione all'ambito del trattamento dei dati personali con la Loi Informatique et Libertés, il cui primo articolo infatti afferma il principio secondo cui l'informazione è al servizio del cittadino e perciò non può ledere la sua identità, la sua libertà o il suo diritto alla vita privata.[26]

L'altra intuizione del legislatore francese fu quella di creare una Commissione incaricata di sorvegliare lo sviluppo informatico dello Stato e garantire che questo si svolgesse nel pieno rispetto dei diritti dei propri cittadini, *in primis* quello alla privacy. Con l'articolo 8 della legge 78/17 nasceva così il CNIL – Commission Nationale de l'Informatique et des Libertés, un'autorità

[24] Traducibile con "SAFARI o la caccia ai Francesi"

[25] Si noti che il predecessore di Chirac, Raymond Marcellin, era stato costretto a dimettersi per un altro scandalo riguardante la privacy. Egli aveva infatti messo sotto controllo i telefoni del giornale "La Canarde Enchainè".

[26] "*L'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques*." (Loi Informatique et Libertes, Act n. 78-17 du 6 Janvier 1978 relative à l'informatique, aux fichiers et aux libertés)

amministrativa indipendente dal Governo centrale e per questo libera di scegliere il proprio corso d'azione nei limiti delle funzioni assegnatele dalla legge stessa, che sopravvive ancora oggi.
La soluzione francese mostra l'importanza dell'inquadramento giuridico delle norme in materia di privacy nella creazione di fiducia tra i cittadini e le istituzioni: una volta che la raccolta dei dati viene inquadrata in un preciso schema di diritti e doveri, questa non viene più percepita come un'attività lesiva della sfera personale dell'individuo, quanto piuttosto come un'attività naturale e necessaria al funzionamento dei servizi pubblici, ma al contempo rispettosa di diritti e interessi degli individui.

1.2.3 L'approccio della common law e il DPA del 1984

Il processo di formazione del Data Protection Act inglese mostra spiccate differenze con i cugini tedesco e francese. Infatti in questo caso la necessità di dare una regolamentazione organica in materia di privacy non nasce da nessun tipo di rivendicazione popolare nei confronti dell'esecutivo, bensì da una volontà dello stesso di anticipare le necessità che le nuove tecnologie stavano creando.
Fu proprio in questo spirito, tipico della common law, che il governo Heath commissionò il primo di due rapporti fondamentali: lo *Younger Committee's Report on Privacy* del 1972. Questo rapporto conteneva una serie di raccomandazioni circa l'adeguamento della legislazione britannica ad un'ottica di maggiore protezione della privacy. Di fatto secondo le raccomandazioni la ricetta vincente per assicurare una maggiore protezione ai cittadini doveva comprendere innovazioni legislative, controllo amministrativo e autodisciplina degli organismi pubblici.[27]
Particolarmente interessante è l'approccio alle eventuali modifiche della legge civile: il Comitato si esprime contro la creazione di una fattispecie generale a cui appellarsi per "*qualsiasi violazione sostanziale e irragionevole"* del diritto alla privacy, preferendo una divisione "di stampo prosseriano" in tre illeciti: (i) *Unlawful surveillance* in riferimento ai "Big Brothers", i dispositivi di sorveglianza automatici; (ii) *Disclosure or other use of information unlawfully acquired* in riferimento alle informazioni "rubate"; (iii) *Breach of confidence* o "violazione della fiducia".

Questo primo rapporto portò ad una proposta di legge nel 1975, intitolata "Computers and Privacy", ma soprattutto ebbe il merito di attirare l'attenzione sia dell'esecutivo che del legislativo sulla questione del diritto alla privatezza.

Il secondo rapporto risale al 1978 ed è noto come *Lindop Report on Data Protection*. Questa volta il Comitato si concentrò maggiormente sulla questione dei sistemi computerizzati di raccolta dei

[27] "*Its recommendations fell into three categories: protection by changes in the law; protection by the creation of administrative control; and protection by persuading some organizations to exercise greater self-discipline*" (G. DWORKIN, The Younger Committee Report on Privacy. 1973, The Modern Law Review, 36(4), 399-406.)

dati, sia pubblici che privati. Questo documento considera anche le soluzioni offerte dagli altri Paesi europei e non solo: proprio in quel periodo infatti Svezia, Germania Ovest, Francia, Norvegia, Danimarca e Stati Uniti avevano già varato le proprie leggi, mentre in Austria, Belgio e Lussemburgo vi erano bozze in attesa di approvazione. Vale la pena notare come – bizzarramente – questo documento lasci fuori il trattamento manuale dei dati, occupandosi solo del trattamento computerizzato. In ogni caso, la conclusione fondamentale a cui arrivano i membri del Comitato è quella di creare uno *white paper* riguardante unicamente il diritto di privacy individuale, lasciando gruppi ed associazioni ad altri rami della legge. Questo paper avrebbe dovuto contenere anche un embrione di Data Protection Authority, presumibilmente sul modello francese, il quale sarebbe poi diventato l'attore responsabile dell'implementazione delle future norme.

Il Rapporto Lindop ebbe maggior fortuna del precedente: nel 1982 venne stesa la bozza definitiva, che avrebbe incontrato l'approvazione di Sua Maestà due anni più tardi, il 12 luglio 1984, con il nome di *Data Protection Act*.

1.3 Lo scenario europeo

Fin dai primi passi del processo di integrazione europea, le nascenti istituzioni si sono mostrate molto attente al tema dei diritti umani, in cui rientra anche la protezione della privacy. Alcuni riferimenti si possono già trovare nella *"Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali"* firmata a Roma il il 4 novembre 1950, che con un ventennio di anticipo sul resto del mondo occidentale all'articolo 8 recita:

"1. Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza.

2. Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui".[28]

L'Unione Europea ha fatto proprio questo articolo con la proclamazione della Carta dei Diritti Fondamentali dell'Unione Europea nel 2000, che è stata elevata a rango di diritto primario dell'Ue

[28] Non a caso questo documento della Corte di Strasburgo è integralmente riconosciuto dall'Unione Europea, per mezzo dell'articolo 6 del TUE – Trattato sull'Unione Europea. In particolare il TUE si riferisce alla versione più recente della Carta, ovvero quella adattata il 12 dicembre 2007 a Strasburgo, che ha lo stesso valore giuridico dei Trattati.

con il Trattato di Lisbona del 2009. La privacy è quindi diventata un diritto fondamentale protetto dall'Unione attraverso un sistema articolato di fonti, che verrà analizzato nel capitolo successivo.

1.3.1 La direttiva 94/46/CE

Sebbene negli anni Novanta fosse già chiaro come il rispetto dei diritti fondamentali, fra cui il diritto alla privacy, fosse una bandiera dell'Unione Europea, mancavano ancora disposizioni armoniche per tutti gli Stati membri in materia di trattamento di dati personali e affini. L'esistenza di un articolato sistema di principi fondamentali riguardanti la protezione della privacy permise al legislatore europeo di non perdere tempo: a soli due anni dalla sua nascita, l'Unione Europea si dotava della direttiva 94/46/CE relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, entrata in vigore nel 1995. Questa era rivolta a tutti i Paesi membri, i quali avrebbero dovuto dotarsi di legislazioni conformi entro il 31 dicembre 1996.[29]

Per sua stessa natura, "*la direttiva vincola lo stato membro cui è rivolta per quanto riguarda il risultato da raggiungere, salva restando la competenza degli organi nazionali in merito alla forma e ai mezzi"*[30]. In particolare, gli obiettivi fondamentali di questa direttiva erano due: la salvaguardia del diritto alla protezione dei dati personali e la libera circolazione dei dati personali fra gli Stati membri dell'Unione Europea, ovvero il cosiddetto *"free flow of data"*.

In virtù del secondo obiettivo, questa direttiva ebbe l'indubbio merito di "aprire" maggiormente i confini all'interno non solo dell'Unione Europea, ma anche dello Spazio Economico Europeo, in ossequio ai dettami della Convenzione di Shengen, il cui obiettivo è appunto quello di una maggiore integrazione territoriale volta all'implementazione del mercato unico. Il suo rapporto con questa Convenzione, però, la rese agli occhi di molti un mero strumento del mercato interno, trasformando il trattamento dei dati in un rapporto economico e la salvaguardia degli stessi in una tutela della proprietà privata.

Nonostante le critiche, gran parte del sistema creato da questa direttiva permane ancora oggi: fondamentale in particolare il ruolo del consenso e delle informative, pietra angolare del trattamento dei dati personali ancora oggi.

Particolarmente interessante è il rapporto che la direttiva aveva con i Paesi al di fuori dello Spazio Economico Europeo: partendo da una concezione poco internazionalista rispetto alla normale

[29] In Italia venne recepita con la legge 675/96 proprio nell'ultimo giorno utile, il 31 dicembre 1996.
[30] Trattato sul funzionamento dell'Unione Europea del 13 dicembre 2007, versione consolidata della Gazzetta ufficiale n. C 326 del 26/10/2012

vocazione europea, essa vietava il trasferimento di dati in Stati ove non fosse garantito un livello di protezione adeguato alle disposizioni della stessa.

La vigilanza sull'applicazione e l'interpretazione spettava naturalmente alla Corte di Giustizia dell'Unione Europea, ma dall'oggetto della direttiva rimanevano escluse le questioni di sicurezza pubblica e giustizia penale, nonché il trattamento di dati personali effettuato da privati a fini esclusivamente personali, che venivano demandati ai singoli Stati membri secondo l'art. 3.2.

Nonostante gli indubbi meriti, la direttiva si rivelò molto presto obsoleta, anche a causa della velocità di sviluppo delle nuove tecnologie. Per questo venne integrata dal regolamento CE n. 45/2001 e poi abrogata dal regolamento UE 2016/679.[31]

1.3.2 Il regolamento delle istituzioni europee sulla protezione dei dati CE 45/2001: nasce il Garante Europeo

Mentre avveniva la graduale attuazione della direttiva 94/46/CE da parte dei vari Stati membri, l'Unione Europea decise di fare un passo avanti fondamentale: l'unificazione in un solo regolamento delle norme relative al trattamento dei dati personali da parte delle varie istituzioni europee. Da questa decisione scaturì il regolamento in questione, il cui nome per esteso è "*Regolamento (CE) n. 45/2001 del Parlamento Europeo e del Consiglio, del 18 dicembre 2000, concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati*"

Oltre l'indubbio impatto di un'autoregolamentazione da parte dell'Unione Europea nel sottolineare l'importanza del diritto alla privacy, una novità fondamentale fu l'introduzione di una nuova figura, il Garante Europeo della protezione dei dati, noto con l'acronimo inglese EDPS – European data protection supervisor. Questa figura di sorveglianza indipendente vigila sul rispetto del diritto alla vita privata delle persone fisiche nel trattamento dei dati personali da parte degli organi dell'UE. Questi ultimi infatti non possono trattare dati personali relative ad orientamento politico, sessuale, religioso, filosofico o sindacale, tranne naturalmente alcune necessarie eccezioni.

Il Garante Europeo è nominato dal Parlamento e dal Consiglio per un mandato rinnovabile di 5 anni. I suoi poteri sono divisibili in tre filoni, dei quali il primo è un generale potere di controllo

[31] Regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio, del 18 dicembre 2000, concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati, Gazzetta ufficiale del 12/01/2001
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, Gazzetta ufficiale del 04/05/2016

e supervisione: il Garante esamina il protocollo di trattamento dei dati di ciascun organismo europeo ed emette un parere in materia di controllo preventivo, la cui attuazione è poi a sua volta oggetto di verifica e controllo.

Questo potere porta anche il Garante ad essere una sorta di autorità di ricorso per le materie di cui si occupa: egli infatti esamina le denunce presentate da chiunque ritenga che la sua o altrui privacy sia stata violata da organismi europei.[32] In questo campo egli può inoltre commissionare indagini.

Il Garante ha anche un potere consultivo: nelle materie di sua competenza, egli consiglia la Commissione, il Parlamento ed il Consiglio dell'Unione Europea in svariati campi. Può inoltre intervenire in qualità di esperto in casi giudiziari pendenti dinanzi alla Corte di Giustizia dell'Unione Europea. Naturalmente consiglia anche le varie autorità nazionali e studia l'evoluzione delle nuove tecnologie nel proprio settore.

Infine il Garante ha delle mansioni che potremmo definire cooperative: in virtù delle proprie competenze in materia di trattamento dei dati personali, egli collabora con le altre istituzioni per dare un'attuazione coerente ed uniforme ai principi del regolamento.

Il Garante Europeo inoltre partecipa all'*European Data Protection Board*, ovvero il Comitato Europeo per la protezione dei dati, insieme alle autorità Garante nazionali e a vari organi di controllo.

1.4 Verso il GDPR

Per analizzare le motivazioni che hanno spinto la Commissione Europea a proporre un nuovo regolamento in materia di trattamento dei dati personali, è utile ricordare innanzitutto che la legge europea più recente risale al 1995 (naturalmente escludendo il sopracitato regolamento 45/2001 in quanto riguarda solo le istituzioni dell'UE). Si trattava quindi di disposizione obsolete, specie considerando la velocità e l'ampiezza della diffusione dei nuovi mezzi digitali di informazione. Oltre a ciò, in questa legge mancava del tutto una legislazione riguardante i dati trattati a fini investigativi e giudiziari. Infine, il fatto che il quadro normativo fosse retto da una direttiva aveva portato ad una frammentazione statale delle varie disposizioni, che erano interpretate ed applicate in modo diverso in ogni Paese.

Di fronte a questo quadro incompleto e caotico, la Commissione Europea decise di reagire con una proposta di regolamento, datata 25 gennaio 2012, che avrebbe dovuto sostituire l'ormai anziana direttiva 95/46/CE. Nel fare questo, la Commissione cita anche motivazioni di carattere

[32] Qualora il ricorrente non fosse d'accordo con la decisione del Garante, in ultima istanza può ricorrere alla Corte di Giustizia.

economico, come la creazione di fiducia per favorire il commercio on-line, in piena compatibilità con quanto previsto dall'Agenda digitale Europea e dalla Strategia Europa 2026.

1.4.1 Il procedimento legislativo

Poiché si tratta di un regolamento, il GDPR è stato adottato seguendo la cosiddetta procedura legislativa ordinaria (o procedura di codecisione) ex. art. 289 del TFUE, che vede la concorrenza del Parlamento e del Consiglio Europeo nell'elaborazione di una norma proposta dalla Commissione Europea, che ricordo essere il principale organo a detenere il potere di proporre una legge, salvo che i Trattati dispongano diversamente.

La procedura legislativa ordinaria si compone normalmente di almeno due fasi: in una prima lettura il Parlamento adotta la propria "posizione" in merito alla proposta di legge, che viene trasmessa al Consiglio. Se il questo approva la posizione del Parlamento, l'atto è adottato. In caso contrario, il Consiglio adotta a sua volta la propria posizione in prima lettura.

La seconda lettura è una fase di tre mesi in cui il Consiglio può approvare la posizione del Parlamento o decidere di non deliberare, nel qual caso l'atto si considera adottato. Il Consiglio potrebbe anche scegliere di respingere la posizione del Parlamento o di proporre emendamenti. Nel primo caso la procedura si ferma e l'atto non è adottato, mentre nel secondo è necessario un nuovo intervento della Commissione, che emette un parere sugli emendamenti. Se il Consiglio approva tutti gli emendamenti (all'unanimità quelli con parere contrario della Commissione), l'atto è adottato. Se invece il Consiglio non approva tutti gli emendamenti, interviene il Comitato di Conciliazione che ha sei settimane di tempo per pervenire ad un nuovo progetto. Qualora questo progetto venga approvato in terza lettura, l'atto è adottato. Se invece il Comitato non riesce a stilare il progetto o questo viene respinto, la procedura si arresta e l'atto non è adottato.

Nel caso del GDPR, la Commissione ha promulgato la proposta di regolamento nel gennaio del 2012. Proprio come accadrebbe in Italia, la proposta è stata esaminata da una specifica Commissione in seno al Parlamento, in questo caso la Commissione LIBE – Commissione per le libertà e la giustizia. Il referente Jan Philip Albrecht ed il suo team hanno quindi analizzato la bozza e proposto gli eventuali emendamenti, fra cui fondamentale l'introduzione della figura del *data producer* o la creazione dei dati pseudoanonimi, di cui ci si occuperà in seguito.

Nel 2013 le proposte definitive di modifica sono state sottoposte alla Commissione LIBE, la quale si è rivolta ad altre Commissioni specifiche competenti nel tema, quali: la Commissione JURI per le questioni giuridiche, la Commissione EMPL per l'impiego e gli affari sociali, la Commissione IMCO per il mercato interno e la protezione dei consumatori IMCO ed infine la Commissione ITRE per l'industria, la ricerca e l'energia.

Nello stesso periodo, la bozza è stata posta al vaglio dal Consiglio dell'Unione Europea, tramite la Commissione DAPIX – Data Protection and Information Exchange. Il 31 maggio 2013 anche questo organo è pervenuto ad un parere, concentrato principalmente sul ruolo di riferimento per i cittadini esercitato dall'autorità Garante, anche a livello nazionale. Secondo la proposta del Consiglio, la figura di riferimento dovrebbe essere il Garante del Paese in cui il titolare od il responsabile del trattamento hanno la sede principale.[33]

Nel 2014 è stato adottato in prima lettura dal Parlamento il regolamento generale 7427/14. L'anno seguente il Consiglio ha coniugato i propri pareri in un orientamento generale (9565/15) e affidato al Presidente il mandato per aprire negoziati a tre[34] con il Parlamento. Da questi colloqui è scaturito un accordo sul testo definitivo, datato 15 dicembre 2015.

L'ultimo passo del procedimento è stata la conferma del testo da parte della Commissione per le libertà civili, la giustizia e gli affari interni del Parlamento europeo (Commissione LIBE) e del Comitato dei Rappresentanti Permanenti del Consiglio dell'Unione europea (Coreper). A questo punto, rispettivamente il 6 e il 15 aprile 2016 il Consiglio ed il Parlamento hanno dato la propria approvazione definitiva al regolamento, che è stato pubblicato sulla Gazzetta Ufficiale il 4 maggio del 2016.

1.4.2 Alcuni pareri fondamentali in corso d'opera

Oltre alle autorità e commissioni precedentemente citate, la bozza del regolamento è stata esaminata da una moltitudine di altri gruppi di esperti, commissioni ed autorità indipendenti. Per ragioni di brevità qui saranno analizzati soltanto la ricerca condotta da Eurobarometer, l'opinione dell'Agenzia dei diritti fondamentali dell'Unione europea e quella del consulente London Economics. Ciascuno di questi pareri si concentra su un aspetto diverso del regolamento e dei suoi presupposti.

Per necessità sia logiche che cronologiche la scelta obbligata è quella di iniziare con la ricerca n. 359 di Eurobarometer, risalente al giugno 2011. Al lettore non sfuggirà che la data precede l'inizio dei lavori di stesura del GDPR. Infatti la ricerca si concentra sulla percezione del diritto alla privacy da parte dell'utente medio all'interno dell'Unione, evidenziando alcune preoccupanti lacune nei metodi precedentemente utilizzati. Si può quindi dire che questa ricerca ha provveduto a dare degli spunti di miglioramento, oltre ad un impulso all'intervento del legislatore. Eurobarometer parte dal presupposto che il primo soggetto a dover tutelare l'utente è proprio

[33] In ossequio al principio del *"one stop shop"* che consiste nel garantire un punto di contatto univoco, il Garante nazionale appunto, per tutti i trattamenti effettuati in più di uno Stato membro.
[34] I cosiddetti *triloghi*

l'utente stesso, attraverso un'attenta lettura e comprensione delle informative, oltre ad una serie di comportamenti cautelari.

In quest'ottica, il primo dato che salta agli occhi è la disinformazione dell'utente: riguardo la lettura dell'informativa sulla privacy, il 58% afferma di leggerla, ma scomponendo la cifra si nota come solo il 34% affermi di capirla interamente, mentre il 24% legge senza comprendere.

A questi si aggiunge un 25% che non la legge affatto, un 8% che afferma di ignorarla deliberatamente e un 5% che non riesce a trovare l'informativa nel sito.

Fra coloro che non leggono l'informativa, al 41% basta sapere che il sito abbia una privacy policy, il 27% pensa che la legge interverrà in ogni caso a tutelarli, mentre il restante 24% pensa addirittura che il sito non rispetterebbe la sua privacy in ogni caso, denotando un'incredibile sfiducia nella protezione fornita dalle leggi sulla privacy.

Un dato più incoraggiante riguarda la domanda circa la modifica del proprio comportamento dopo la lettura dell'informativa: ben 7 utenti su 10 adottano comportamenti diversi rispetto a prima, sottolineando quindi l'effettiva efficacia ed importanza di un'informativa chiara e comprensibile.

Non a caso, nella sezione "*Regulations and remedies"* che conclude la ricerca, Eurobarometer sottolinea da un lato come gli utenti chiedano espressamente di avere maggior controllo sui propri dati[35] e dall'altro la necessità di uniformare le norme in materia di trattamento dei dati personali all'interno dell'Unione.

L'approccio adottato dalla FRA – Agenzia dei diritti fondamentali dell'Unione europea, a differenza di Eurobarometer, non è statistico, ma si concentra sull'interpretazione estensiva dei diritti fondamentali riconosciuti dalla giurisprudenza comunitaria. Per questo motivo l'Agenzia propone principalmente tre modifiche in tal senso: in primo luogo maggiori garanzie riguardo al trasferimento di dati a Paesi terzi, che devono dimostrare di garantire lo stesso rispetto dei diritti fondamentali dell'UE. L'Agenzia infatti si dichiara scettica sulla mancanza di una disposizione in tal senso nella bozza del regolamento.

In secondo luogo si dovrebbe migliorare il bilanciamento tra diritto alla privacy e libertà di informazione ed espressione: alcune prescrizioni del regolamento possono essere annullate "per

[35] *"The interviewees were asked to name the first actor that should be responsible for the safe handling of personal data [..] half of the respondents point to themselves (49%), while one-third point to the social networking or sharing sites (33%). Even fewer identify the public authorities (16%)."* (SPECIAL EUROBAROMETER 359, *Attitudes on Data Protection and Electronic Identity in the European Union*, june 2011)

finalità giornalistiche", mentre la FRA preferirebbe sostituire questa espressione con "per salvaguardare il diritto alla libertà di espressione ed informazione".

Infine la FRA si preoccupa di facilitare il più possibile il procedimento di accesso alla giustizia da parte degli interessati.

Vale la pena di menzionare anche lo studio commissionato dal Garante britannico[36] ad un gruppo di consulenti della London Economics si concentra maggiormente sul punto di vista dei soggetti coinvolti nel trattamento e nella protezione dei dati, anziché sugli interessati. Lo scopo di questo studio è dare voce in capitolo alle imprese sottoposte al nuovo regolamento, concentrandosi su tematiche come costi economici e burocratici.

London Economics ha rilevato che, benché molte aziende di fatto adempissero già ai dettami del futuro regolamento, i soggetti da esse scelti mancassero di una formazione adeguata. In parole povere, la maggior parte delle aziende con oltre 250 dipendenti aveva già del personale incaricato del trattamento e della protezione dei dati, per cui l'applicazione del nuovo GDPR non avrebbe dovuto generare costi aggiuntivi. Piuttosto, ulteriori costi avrebbero potuto essere attribuiti alla formazione specifica di questo personale, il cui standard veniva innalzato dal nuovo regolamento.

L'altro grande punto interrogativo delle aziende esaminate sembra riguardare la burocrazia e i suoi vari adempimenti. Ad esempio il limite di 24 ore di tempo entro cui notificare all'interessato una violazione dei dati[37] o le richieste di accesso degli interessati sembrano destare notevoli preoccupazioni agli imprenditori.

A conclusione di questo studio, il Garante inglese dà una valutazione generalmente positiva della situazione, considerando anche alcune soluzioni di rimedio. Ad esempio, sebbene il 40% delle aziende inglesi non ha un'idea chiara degli adempimenti introdotti dal nuovo regolamento, queste sembrano tenere in gran conto le indicazioni del proprio Garante nazionale: circa il 20% delle aziende partecipanti allo studio si era già rivolta in passato all'ICO. A livello prettamente economico, la conclusione è assai interessante: sebbene alcune aziende specializzate dovranno probabilmente sostenere costi più elevati, la creazione di fiducia e stabilità nel sistema potrebbe portare a dei benefici per l'intera economia, risultando quindi in un guadagno netto.

Di fronte a questa conclusione, non si può far altro che sperare che pervengano ad essa più Stati possibili, in modo che il risultato netto sia un miglioramento delle condizioni di privacy della società civile, seppur dettato da ragioni economiche e non culturali come ci si auspicherebbe.

[36] ICO – Information Commissioner's Office
[37] Non a caso questo limite temporale è stato esteso a 72 ore.

CAPITOLO 2 – Aspetti fondamentali del Regolamento Generale sulla Protezione dei Dati

2.1 Regolamento o direttiva?

Al lettore non sfuggirà certo il cambiamento nello strumento legislativo adottato dall'Unione europea per disciplinare il settore della privacy. Infatti inizialmente il legislatore aveva optato per una direttiva[38], mentre nel 2016 con il GDPR è stato attivato un regolamento. Ma qual è il motivo di questa evoluzione?

In realtà si tratta di ragione piuttosto semplice: per sua stessa natura, la direttiva non garantisce uniformità nell'applicazione dei principi dettati dal legislatore europeo, mentre il regolamento sì. Per comprendere meglio questa affermazione, è necessario confrontare questi due strumenti legislativi, che si differenziano per portata, obblighi ed applicabilità.

Sotto il profilo della portata, si è soliti affermare che la direttiva abbia portata individuale, ovvero abbia dei destinatari definiti, che possono consistere di uno o più Stati membri, mentre il regolamento ha portata generale, ovvero è automaticamente vincolante su tutto il territorio dell'Unione Europea. Nella realtà dei fatti la direttiva 94/46/CE era una direttiva generale, ovvero rivolta a tutti gli Stati membri, per cui la portata era la stessa del regolamento 2016/679.

È negli obblighi che si rileva la differenza sostanziale fra direttiva e regolamento: mentre la direttiva vincola gli Stati nel risultato, lasciando libertà di adattamento all'ordinamento interno, il regolamento è direttamente applicabile in tutti gli Stati nel modo e nel momento in cui entra in vigore nell'ordinamento d'origine (ovvero l'Unione europea). In pratica la direttiva ha una normazione in due fasi: alla stesura degli obiettivi nell'ordinamento di origine segue un atto di recepimento da parte dello Stato membro che attua con strumenti normativi dettagliati gli obiettivi generali. Il regolamento invece è già uno strumento completo e dettagliato, che non necessita di questa seconda fase ed è valido nello stesso modo in tutto il territorio dell'Unione.

Questo ci porta al profilo della diretta applicabilità, di cui solo il regolamento gode, in quanto l'adattamento del regolamento avviene direttamente, ovvero automaticamente e immediatamente, senza alcun intervento da parte degli Stati membri. Il regolamento è in grado di produrre effetti diretti all'interno degli ordinamenti statali, mentre nel caso della direttiva sono i provvedimenti di recepimento a produrre un effetto nell'ordinamento.

Proprio gli ultimi due profili sono fondamentali per comprendere la scelta del legislatore europeo. Per prima cosa, grazie all'uso di un regolamento, viene snellito il processo di

[38] Ci si riferisce alla direttiva 94/46/CE del 24 ottobre 1995 relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

implementazione eliminando una fase, quella del recepimento. Questo ha evitato infatti casi limite come quello italiano, dove la legge di adattamento alla direttiva del 1995 era stata emanata l'ultimo giorno disponibile, risultando in una disposizione frettolosa ed incompleta.

Inoltre, la direttiva 94/46/CE aveva creato uno scenario frammentato e disomogeneo, dove ciascuno Stato aveva dato una diversa applicazione agli obiettivi stabiliti dall'Unione. Questa disarmonia legislativa si era naturalmente tradotta in incertezza pratica, specie nel trasferimento di dati da uno Stato all'altro: basti pensare che per ogni confine vi era un tempo diverso per la conservazione dei dati su supporti cartacei e non.

Con l'implementazione di un regolamento, tutte queste problematiche vengono superate a favore di uno scenario più ordinato, in cui gli stessi diritti siano garantiti a tutti nelle stesse modalità, per accordare maggior certezza ed efficacia in tutti gli Stati dell'Unione.

2.2 Le fonti giuridiche

Per comprendere nel dettaglio il contenuto del Regolamento Generale per la protezione dei dati è necessario risalire alle sue fonti giuridiche, ovvero a quei principi fondamentali tutelati nell'ordinamento europeo che costituiscono i diritti originari da cui vengono derivate le norme applicative di dettaglio. Per quanto riguarda il diritto alla privacy, il sistema di fonti si articola come segue.

2.2.1 Articolo 8 CEDU – il rispetto della "vita privata e familiare"

Per quanto la Convenzione Europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali non sia un documento elaborato in seno all'Unione Europea[39], essa occupa indubbiamente una posizione privilegiata in quanto documento di riferimento ed ispirazione per la tutela dei diritti fondamentali all'interno di quest'ultima. Per questo motivo ed anche perché è il primo documento approvato in ordine cronologico fra quelli proposti[40], ritengo sia doveroso analizzare l'articolo 8 di questa Convenzione, che introduce per primo il diritto alla privatezza.

Il testo dell'articolo recita:

1. *"Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza.*
2. *Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al*

[39] La CEDU fu redatta dal Consiglio d'Europa, organizzazione internazionale fondata nel 1949 ed indipendente dall'Unione Europea.
[40] La Convenzione Internazionale per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali fu firmata a Roma il 4 novembre 1950.

benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute e della morale, o alla protezione dei diritti e delle libertà altrui."

Lo scopo principale della disposizione è difendere la privacy dell'individuo dalle ingerenze del potere pubblico, sebbene il secondo comma introduca alcune necessarie eccezioni riguardanti l'interesse pubblico. Proprio per questo motivo il rispetto della vita privata e personale non si configura come un diritto assoluto, ma deve essere necessariamente bilanciato e soppesato con altri interessi concorrenti. Per la Corte Europea dei Diritti dell'Uomo[41] deve sussistere *"un principio di proporzionalità tra la misura [contestata] e lo scopo perseguito".*[42]

È interessante notare come l'articolo 8 costituisca un'apertura nei confronti dei diritti positivi: se da un lato sorge un obbligo passivo di non intromissione in capo allo Stato, dall'altro è possibile ipotizzare un parallelo dovere attivo nella protezione della privacy dei propri cittadini.

Il lettore noterà subito che la CEDU non parla di diritto alla privacy, ma di rispetto della vita privata. Qual è dunque la definizione di vita privata secondo la Corte di Strasburgo?

Osservando la giurisprudenza della Corte si può dedurre che essa dia un'interpretazione decisamente ampia di questa espressione: nel proteggere la vita privata dei cittadini si intende salvaguardare la loro integrità fisica ma anche morale, nonché i diritti di immagine. Infatti, riprendendo una concezione che si può far risalire fino a Warren e Brandeis, rientrano sotto la protezione dell'articolo 8 anche quelle informazioni che un individuo può legittimamente aspettarsi che non vengano divulgate senza il suo consenso.[43]

Sempre con una giurisprudenza decisamente moderna e innovatrice, la Corte di Strasburgo ha ritenuto attinenti alla vita privata oltre al nome[44] o alle fotografie[45], anche elementi quali il diritto di filiazione[46] ed i diritti ad esso connessi, attraverso l'introduzione della parte riguardante la vita familiare.

2.2.2 Articolo 16 TFUE – la protezione dei dati di carattere personale

All'articolo 16 del Trattato sul funzionamento dell'Unione europea, come modificato dal Trattato di Lisbona del 13 dicembre 2007, troviamo un altro fondamentale riferimento al diritto alla

[41] Anche nota come Corte EDU o Corte di Strasburgo, essa sovrintende al rispetto e all'applicazione della Convenzione.
[42] Sentenza del 3 ottobre 2014, *Jeunesse contro Paesi Bassi*.
[43] Sentenza del 6 aprile 2010, IV sez., *FLinkkila and Others contro Finlandia*,§75.
[44] Sentenza del 5 dicembre 2013, V sez., *Henry Kismoun contro Francia*, in tema di cambiamento del cognome e del nome delle persone fisiche.
[45] Sentenza del 7 febbraio 2012, Grande Camera, *Von Hannover contro Germania*, § 95.
[46] Sentenza del 26 giugno 2014, *Mennesson contro Francia*.

privacy[47]. In realtà l'odierno articolo 16 del TUE ricalca fedelmente l'articolo 287 del Trattato che adotta una Costituzione per l'Europa, meglio noto come TCE, redatto già nel 2003 dalla Convenzione europea. Questo Trattato, come suggerisce il nome stesso, sarebbe dovuto diventare la legge fondamentale dell'Unione europea, elevando perciò grazie all'articolo 287 il diritto alla privacy al rango più alto delle tutele possibili in quanto principio fondamentale dell'Unione.

È chiara quindi la volontà di riorganizzare e dare maggior peso alle norme relative al settore della privacy, che prima di questo intervento rimanevano suddivise fra il primo pilastro, dove si trattava della protezione dei dati a scopo economico-commerciale, ed il terzo pilastro, riguardante la protezione dei dati in relazione alla tutela della sicurezza e dell'ordine pubblico. La confusione riguardava anche i metodi di implementazione delle norme, in quanto il primo pilastro era soggetto al metodo comunitario, per cui le decisioni venivano prese dalla Comunità nella sua interezza, mentre nel settore della sicurezza e dell'ordine pubblico prevaleva un processo decisionale intergovernativo, con la concorrenza di tutti gli Stati membri.

Passando all'analisi delle disposizioni date dall'articolo 16, il testo emerso dal Trattato di Lisbona recita:

1. *"Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.*
2. *Il Parlamento europeo e il Consiglio, deliberando secondo la procedura legislativa ordinaria, stabiliscono le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale da parte delle istituzioni, degli organi e degli organismi dell'Unione, nonché da parte degli Stati membri nell'esercizio di attività che rientrano nel campo di applicazione del diritto dell'Unione, e le norme relative alla libera circolazione di tali dati. Il rispetto di tali norme è soggetto al controllo di autorità indipendenti.*
3. *Le norme adottate sulla base del presente articolo fanno salve le norme specifiche di cui all'articolo 39 del trattato sull'Unione europea*."

Si noti che il terzo comma fa riferimento alle disposizioni specifiche adottate dall'articolo 39 del Trattato sull'Unione Europea, con il quale il Consiglio adotta una decisione contenente norme dettagliate riguardante la protezione delle persone fisiche in riferimento ai loro dati e ai trasferimenti degli stessi da parte degli Stati membri e dell'Unione nell'ambito della politica estera e di sicurezza comune. Poiché si tratta di un settore specifico che non investe l'ambito del GDPR qui analizzato, non ritengo opportuno addentrarmi ulteriormente in questo settore.

[47] Da leggere in combinato disposto con l'articolo 39 del Trattato sull'Unione Europea, che sarà analizzato nel paragrafo seguente.

Ciò che invece è opportuno rilevare è che questo articolo contiene un chiaro richiamo alle persone fisiche quali destinatarie del diritto alla riservatezza, che si configura quindi ancora una volta come un diritto fondamentale dell'individuo. Inoltre, poiché ci si riferisce alla protezione dei dati di carattere personale, è sottinteso che la protezione non sia accordata solamente all'individuo nella sua sfera privata, ma anche nelle relazioni sociali in quanto egli è il solo decisore per quanto riguarda l'eventuale diffusione o uso dei dati che lo riguardano. Si può quindi affermare di avere a che fare con un diritto riguardante l'identità stessa dell'individuo.

Nella seconda parte dell'articolo si nota chiaramente la volontà del legislatore di autolimitarsi per lasciare proprio all'individuo il suo spazio di decisione. Non solo, le disposizioni vincolano anche gli Stati membri nei settori in cui prevale il diritto europeo e nei trasferimenti di dati fra gli Stati stessi. Pertanto, tranne necessarie eccezioni, l'individuo è l'unico titolare dei propri dati anche di fronte al suo Stato e all'intera Comunità europea, la quale si trova quindi nella posizione di dover applicare misure attive per la protezione di tali informazioni. Si può quindi affermare che con l'articolo 16 del TFUE si consacra un diritto che comporta doveri sia attivi che passivi in capo all'ordinamento europeo.

Questa impostazione è ulteriormente rafforzata dalle ultime parole del secondo comma, ove si specifica che la vigilanza sul trattamento dei dati in seno all'Unione europea sarà affidata non alla stessa, ma ad organismi indipendenti[48], per rafforzare ulteriormente le garanzie dell'individuo riguardo all'imparzialità della supervisione sul trattamento dei propri dati.

2.3 Principi generali nel trattamento dei dati

Questo paragrafo fa riferimento in generale al capo II del regolamento 2016/679, dove appunto sono illustrati i principi a cui il titolare e le altre figure devono attenersi nel trattamento dei dati personali. Nel primo articolo di questo capo, ovvero l'articolo 5[49], si ritrovano di fatto elencati proprio questi principi, riassunti in parole chiave che ci si appresta a spiegare.

[48] Si tratta delle Autorità Garanti

[49] *"1. I dati personali sono:*
a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);
b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»);
c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);
d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);

In primo luogo sono citati i principi di "liceità, correttezza e trasparenza", secondo i quali il trattamento deve avvenire in modo lecito, corretto e trasparente nei confronti dell'interessato, il quale deve essere informato su tutti gli aspetti riguardanti l'uso che si intende fare dei propri dati.

In secondo luogo si parla di "limitazione delle finalità" sottolineando l'intenzione del legislatore europeo di porre un freno all'uso improprio dei dati da parte dei titolari, i quali molto spesso sono tentati di utilizzare dati entrati lecitamente in loro possesso, per finalità diverse da quelle inizialmente rese note all'interessato.[50] Alla lettera *e* del primo comma troviamo il principio complementare della "limitazione della conservazione", secondo il quale i dati debbono essere conservati per un tempo non superiore al conseguimento delle finalità per le quali sono stati raccolti. Possono essere conservati per periodi superiori quando il trattamento riguarda l'archiviazione nel pubblico interesse o a scopo di ricerca scientifica, storica o ancora a fini statistici.

Rientra in questa ottica di limitazione dell'azione dei titolari anche il principio di "minimizzazione dei dati", che agisce allo stesso modo della limitazione delle finalità, ma sul piano quantitativo anziché temporale. Secondo questa nozione, si deve raccogliere la quantità minima di dati strettamente necessaria al trattamento, senza includere dati superflui, ma considerando solo i dati "*adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati*".

Il principio di "esattezza dei dati" prescrive invece l'obbligo di aggiornamento, rettifica o cancellazione dei dati inesatti, in modo da tutelare l'interessato di fronte ai danni che potrebbero essergli arrecati da informazioni inesatte sul suo conto.

Infine il legislatore europeo introduce il principio di "integrità e riservatezza", riguardante le garanzie sulla sicurezza e la protezione dei dati personali, da perseguire tramite misure adeguate. È interessante notare come, ai fini della protezione dei dati, poco importa se il danno è doloso o accidentale: vengono infatti trattati alla pari sia eventuali trattamenti non autorizzati o illeciti, sia la perdita, la distruzione e il danno accidentale ai dati.

---

e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»);
f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»)."

[50] Per un'analisi più approfondita sulla tematica delle finalità del trattamento si rimanda al paragrafo seguente.

Ma a chi spetta la responsabilità legale del rispetto di tutte queste prescrizioni? Al secondo comma, il regolamento individua il titolare del trattamento[51] come *"competente per il rispetto del paragrafo 1 e in grado di comprovarlo"*. Non solo il titolare ha la responsabilità delle modalità in cui avviene il trattamento dei dati, ma deve anche essere in grado di produrre prove valide di detenere realmente questa responsabilità.

2.3.1 Le finalità della raccolta

Nel paragrafo precedente è già stato introdotto il concetto di finalità della raccolta, che stabilisce il meccanismo secondo cui l'interessato "affida" i propri dati al titolare per un trattamento definito e concordato fra le due parti. Secondo il testo del regolamento, queste finalità debbono essere "*determinate, esplicite e legittime"*. Ma cosa significa questa espressione?

Per finalità determinate si intende che queste debbano essere concordate e delimitate chiaramente fra il titolare e l'interessato, ad esempio attraverso un'informativa, che assume quindi un'importanza capitale per entrambe le parti. Il responsabile, dal canto suo, deve poter garantire che i dati saranno trattati solo ed esclusivamente per quelle finalità.

Sempre per lo stesso motivo, le finalità devono essere esplicite, ovvero chiaramente comprensibili dall'interessato ed allo stesso tempo spiegate in modo sufficientemente dettagliato da non trarre in inganno il consumatore. Ad esempio l'autorità Garante italiana, nel caso dell'informativa riguardante gli impianti di videosorveglianza, ha raccomandato di proporre un'informazione articolata su due livelli: il primo contenente le informazioni più strettamente necessarie e di facile comprensione, il secondo maggiormente articolato e completo per spiegare le norme di dettaglio.

Infine si pone l'accento sulla legittimità del trattamento, che deve essere naturalmente compatibile con le leggi esistenti. Per leggi si dovrebbe intendere una gamma estesa di provvedimenti con valore vincolante, che potrebbero includere regolamenti di autorità locali, giurisprudenza, codici etici o anche clausole contrattuali. Il concetto di legittimità deve essere interpretato ampiamente anche in ambito temporale: poiché le leggi variano nel tempo, è giusto leggere in chiave dinamica questa espressione.

2.3.2 La compatibilità

È ormai chiaro che i dati sono siano affidati dall'interessato al titolare per un determinato trattamento. Si intuisce quindi che l'interessato rimanga sempre l'unico possessore delle informazioni che lo riguardano e perciò il titolare non può usare quei dati per finalità diverse da quelle concordate. Di fatto si viene a creare un rapporto fiduciario fra i due attori, ove il titolare

[51] Figura di cui si tratterà al paragrafo 2.5 di questo capitolo.

può ulteriormente trattare i dati dell'interessato solo se le nuove finalità sono "non incompatibili" con lo scopo della raccolta. Ma quando le finalità sono compatibili con l'obiettivo e quando no?

Tanto per cominciare è naturale che gli ulteriori trattamenti, eseguiti per aggiornare, correggere e conservare i dati raccolti siano non solo necessari ma praticamente obbligatori, per cui non si pongono dubbi circa la loro compatibilità. Anzi, di fatto si possono considerare come la naturale prosecuzione della fase iniziale di raccolta dei dati.

Il testo dell'articolo ci viene poi incontro nel dichiarare esplicitamente che gli ulteriori trattamenti per fini di archiviazione nel pubblico interesse, di ricerca storica, scientifica o statistica non sono da considerarsi incompatibili con le finalità iniziali, in ossequio all'articolo 89 del regolamento stesso, che contiene appunto le garanzie e le deroghe riguardanti questi settori, pur sempre in ossequio ai diritti dell'interessato.

Escluse le fattispecie di cui sopra, è responsabilità del titolare condurre l'analisi di compatibilità qualora voglia dare inizio a trattamenti aggiuntivi. Questa analisi può riguardare sia aspetti formali che sostanziali. Nel caso di un'analisi formale, il titolare è tenuto a rileggere attentamente l'informativa che ha sottoposto all'interessato per individuare eventuali aperture a nuovi trattamenti, sia implicite che esplicite. Naturalmente nulla vieta al titolare di sottoporre una nuova informativa all'individuo per richiedere il suo consenso a ulteriori trattamenti. Nel caso di un'analisi sostanziale invece, si considerano le ragionevoli aspettative sugli obiettivi della raccolta sia da parte del titolare che dell'interessato, per adattare eventualmente il trattamento in tal senso.

Per concludere con un esempio pratico, prendiamo il caso di un corriere. Egli potrebbe utilizzare i dati riguardanti l'abitazione dei clienti non solo per consegnare la merce, ma anche per inviare le fatture. È chiaro che questo uso dei dati del cliente è del tutto congruo con le finalità dichiarate. Se però il corriere passasse queste informazioni ad un gestore telefonico affinché questo possa inviare i propri opuscoli pubblicitari ai recapiti fornitigli, si tratterebbe chiaramente di una finalità non congrua con gli obiettivi iniziali della raccolta (ovvero la consegna della merce).

2.3.3 Il consenso

Nei paragrafi precedenti si è già più volte accennato al fatto che l'interessato debba dare il proprio consenso affinché qualsiasi raccolta e/o trattamento dei propri dati possa avvenire. La prestazione del consenso è quindi una fase fondamentale per tutelare il diritto alla privacy e all'informazione

degli individui, per cui le è dedicato un articolo a sé stante, l'articolo 7 del capo II del regolamento 2016/679, il cui testo si trova in nota.[52]

Prima dell'entrata in vigore del GDPR il consenso era declinato nella formula "libero, informato ed incontrovertibile". Il fondamento è rimasto lo stesso, ma con in nuovo regolamento sono state apportate alcune modifiche: infatti l'articolo 3, comma 11, definisce il consenso come *"qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento"*.

Questa definizione è poi ripresa e approfondita dall'articolo 7. Il quarto comma ad esempio riguarda la libera prestazione del consenso, affermando in particolare che il consenso non è liberamente prestato quando si subordina la prestazione di un servizio contrattuale all'accettazione di un trattamento non strettamente necessario all'esecuzione di tale contratto. In parole povere, non si può costringere l'interessato a dare il proprio consenso come condizione vincolante della prestazione di un servizio, se tale consenso non riguarda un trattamento strettamente necessario per l'erogazione di quel servizio.

Per quanto riguarda il consenso informato, naturalmente l'interessato ha diritto a sapere chi raccoglierà i suoi dati, per quale motivo, per quanti anni saranno conservati e se saranno passati a terzi. Oltre a questa specificazione piuttosto ovvia, il regolamento introduce due importanti novità: una riguardante le modalità e una il linguaggio. Se la richiesta di consenso è presentata in un documento che tratta anche altre materie, essa deve essere chiaramente individuabile e distinguibile dall'interessato rispetto al resto. Inoltre, il linguaggio deve essere di facile comprensione per tutti, per cui non risultano più accettabili informative redatte in linguaggio tecnico o strettamente legale, che sono anzi da considerarsi non vincolanti perché incomprensibili.

---

[52] *"1. Qualora il trattamento sia basato sul consenso, il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali.*
2. Se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Nessuna parte di una tale dichiarazione che costituisca una violazione del presente regolamento è vincolante.
3. L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento. La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca. Prima di esprimere il proprio consenso, l'interessato è informato di ciò. Il consenso è revocato con la stessa facilità con cui è accordato.
4. Nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto."

Riguardo all'incontrovertibilità, si tratta di una formula ridondante che è stata sostituita dal principio di dimostrabilità dell'avvenuto consenso. Infatti, secondo il primo comma dell'articolo 7, il titolare del trattamento deve poter produrre prove certe a sostegno dell'avvenuta prestazione del consenso da parte dell'interessato, senza le quali il trattamento non può avvenire.

Infine resta un aspetto fondamentale, che viene spesso trascurato. Poiché l'individuo è il proprietario dei propri dati, egli può, in qualsiasi momento e senza presentare alcuna motivazione, revocare il proprio consenso al trattamento. Non solo, deve poterlo fare con relativa facilità, sempre secondo il testo dell'articolo. Naturalmente questa revoca non ha effetti retroattivi: i trattamenti avvenuti prima di essa sono considerati leciti.

2.4 Le tipologie di dati

Il nuovo regolamento europeo sulla protezione dei dati aggiorna alcune definizioni riguardanti la classificazione dei dati. Ad esempio scompaiono i dati sensibili, che vengono sostituiti con la dicitura "dati particolari", insieme all'introduzione di tutele particolari per i dati biometrici e dei dati genetici. Anche il metodo di trattamento dei dati cambia a seconda della categoria, per cui è opportuno chiarire tutte queste definizioni.

2.4.1 I dati personali comuni

Tanto per cominciare, che cosa si intende per dato personale? Secondo la definizione ex. articolo 4 comma 1 del regolamento in esame, per dato personale si intende *"qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale"*.

L'accento è chiaramente posto sulla possibilità o meno di risalire tramite i dati in questione all'identità dell'interessato a cui appartengono, per cui logicamente sono esclusi i dati anonimi, ovvero quei dati non associabili in alcun modo ad una persona fisica identificata o identificabile.

In particolare nei dati personali comuni rientrano tutte quelle informazioni che possiamo trovare sui documenti di qualsiasi individuo: nome e cognome, indirizzo, numero telefonico, codice fiscale, partita IVA e simili. Si noterà che alcuni di questi dati non sono propri solo delle persone fisiche, ma anche di quelle giuridiche: qualsiasi ente o impresa ha un indirizzo e un numero di telefono.

Fra i dati personali comuni si possono distinguere quelli che permettono un'identificazione diretta, come ad esempio le fotografie o i dati anagrafici, da quelli che permettono

un'identificazione indiretta, in cui rientrano i numeri di identificazione come il codice fiscale, la targa dell'auto o anche un indirizzo IP.

Ci si potrebbe chiedere se le coordinate bancarie rientrino in questa categoria di dati o abbiano delle tutele riservate. Ebbene, si tratta anche in questo caso di dati personali comuni, in quanto non rivelano informazioni relative alla personalità o alla salute dell'individuo, cosa che riguarda i dati particolari, che analizzeremo nel prossimo paragrafo.

Per raccogliere questi dati deve naturalmente sussistere il requisito della liceità, ovvero il titolare del trattamento deve avere un motivo comprovato per raccoglierli e rispettare tutte le prescrizioni riguardanti la prestazione del consenso e le finalità della raccolta. Come vedremo nel paragrafo seguente, proprio in questo sussiste la differenza sostanziale con i dati particolari.

2.4.2 I dati particolari

Si è già accennato come il nuovo regolamento in materia di privacy abbia eliminato la categoria dei dati sensibili per sostituirla con quella dei dati particolari. Ma quali dati rientrano in questa definizione?

Si occupa di questa materia l'articolo 9 del capo II[53], il quale riguarda i *"dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o*

---

1. [53] *"È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.*
2. *Il paragrafo 1 non si applica se si verifica uno dei seguenti casi:*

a) *l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al paragrafo 1;*
b) *il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato;*
c) *il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;*
d) *il trattamento è effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato;*
e) *il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato;*
f) *il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;*
g) *il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato;*

l'appartenenza sindacale, nonché […] 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."

Per scopi pratici, i dati particolari si possono quindi dividere in alcune macro categorie: per primi i dati riguardanti la personalità dell'individuo, come appunto l'origine razziale o etnica, le opinioni politiche, religiose, filosofiche, l'appartenenza sindacale e l'orientamento sessuale dell'interessato.

Vi sono poi i dati inerenti la salute del singolo, dove per salute si intende anche quella psicologica, nonché i trattamenti a cui l'individuo è sottoposto. In questa categoria il GDPR introduce anche i dati biometrici, ovvero *"i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici"*[54] e i dati genetici, definiti come *"i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione"*[55].

h) *il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità, fatte salve le condizioni e le garanzie di cui al paragrafo 3;*

i) *il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale;*

j) *il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.*

3. *I dati personali di cui al paragrafo 1 possono essere trattati per le finalità di cui al paragrafo 2, lettera h), se tali dati sono trattati da o sotto la responsabilità di un professionista soggetto al segreto professionale conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti o da altra persona anch'essa soggetta all'obbligo di segretezza conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti.*

4. *Gli Stati membri possono mantenere o introdurre ulteriori condizioni, comprese limitazioni, con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute."*

[54] PARLAMENTO E CONSIGLIO EUROPEO, *Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali* dati, 27 aprile 2016, art. 3 capo I – *Definizioni*.

[55] *Ibid.*

Come anticipato, la differenza sostanziale sta nel fatto che il trattamento di questi dati è sempre vietato come regola generale dal legislatore europeo, salvo poi introdurre le eccezioni elencate dal secondo comma dell'articolo 9. La regola generale impone perciò una completa tutela della persona sia nella sua fisicità che nella sua interiorità. Naturalmente se il divieto fosse assoluto anche nei fatti, questo andrebbe a danno del singolo stesso, per cui sono introdotte numerose e necessarie eccezioni.

In primo luogo, alcune eccezioni riguardano la volontà stessa dell'individuo: il trattamento dei dati particolari è legittimo se l'interessato presta il proprio consenso esplicito o se egli stesso li rende pubblici (lettere *a* ed *e* del secondo comma dell'articolo 9).

Vi sono poi una serie di deroghe a favore degli interessi di natura sanitaria, anche dello stesso individuo, che vanno ragionevolmente tutelati anche in opposizione al diritto alla privacy: ad esempio nel caso in cui l'interessato sia incosciente o incapace di prestare il consenso per un trattamento dei propri dati necessario a tutelare un suo interesse vitale (lettera *c*, basti pensare ad un ricovero di emergenza in stato di incoscienza); per finalità di medicina preventiva o medicina del lavoro (lettera *h*) o ancora per tutelare interessi pubblici nel settore della sanità pubblica (lettera *i*).

Naturalmente contro la disposizione del primo comma è soppesato anche l'interesse pubblico e giudiziario: alla lettera *f* è prevista una deroga per le autorità giurisdizionali nell'esercizio delle loro funzioni, a cui segue alla lettera *g* una deroga per più generali *"motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri"*, a patto che vi sia proporzionalità fra il trattamento richiesto e gli interessi in gioco.

Il trattamento dei dati può anche rendersi necessario a fronte di disposizioni date dal diritto del lavoro, da leggi sulla protezione sociale o ancora da contratti collettivi stipulati secondo il diritto dell'Unione o degli Stati membri. Questi obblighi potrebbero sorgere sia in capo al titolare che all'interessato, per cui con la lettera *b* si autorizzano anche in questi casi.

Sono dispensate dall'obbligo di astenersi dal trattare dati personali anche le fondazioni, associazioni e organismi senza scopo di lucro che perseguono finalità politiche, filosofiche, religiose o sindacali, le quali però possono trattare soltanto i dati dei propri membri, ex membri o comunque di persone che abbiano regolari contatti con l'organismo stesso.

Infine ritroviamo la ormai familiare dispensa per fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici come elencati nel primo paragrafo dell'articolo 89 del regolamento stesso.

Un'altra differenza sostanziale fra i dati comuni e quelli particolari riguarda gli addetti al trattamento. Infatti nel secondo caso il trattamento deve avvenire per mano o sotto la

responsabilità di un professionista, che sia vincolato dal segreto professionale dal diritto dell'Unione, degli Stati membri o dagli organismi nazionali competenti in materia. Agli Stati è inoltre affidato un certo margine di discrezionalità nell'introdurre ulteriori condizioni o limitazioni nel trattamento dei dati relativi alla salute, dei dati biometrici e dei dati genetici.

2.4.3 I dati giudiziari

L'articolo 10[56] contiene la disciplina riguardante il trattamento dei dati personali relativi a condanne penali e reati. Si tratta di una prescrizione piuttosto semplice, che incarica legittimamente del trattamento di tali dati solo e soltanto l'autorità pubblica secondo il diritto dell'Unione o degli Stati membri. Inoltre è previsto che solo l'autorità pubblica possa tenere un registro completo delle condanne penali, in modo da bilanciare il diritto alla riservatezza con il grado necessario di tutela dell'ordine pubblico.

Di fronte a questa disposizione, che può sembrare piuttosto scarna per un argomento così importante, va ricordato che le norme specifiche riguardanti i dati giudiziari e il loro trattamento da parte delle forze dell'ordine e degli altri titolari legittimi sono contenute nella "Direttiva 2016/680 del Parlamento europeo e del Consiglio d'Europa, 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", meglio nota come "Direttiva Polizia". Questa è entrata in vigore il 5 maggio 2016, si può dire contestualmente al GDPR, per poi essere recepita nell'ordinamento italiano tramite il decreto legislativo 51 del 18 maggio 2018.

Restano naturalmente valide le disposizioni riguardanti la liceità, la correttezza e la proporzionalità del trattamento così come indicate dal Regolamento. A questi principi si aggiungono poi numerose specificità introdotte dal decreto, ad esempio differenze nel trattamento a seconda della posizione giuridica dell'interessato (parte civile, testimone, persona informata sui fatti, …) oppure la distinzione tra dati fattuali e valutazioni.

2.4.4 I dati anonimi e la pseudonimizzazione

Poiché un dato personale non è più tale, quando non risulta più associabile ad una persona fisica (ma anche giuridica), il dato anonimo non ricade più sotto la tutela del GDPR, bensì nelle disposizioni riguardanti la sicurezza dei dati aziendali generici. Per questo motivo, l'anonimizzazione dei dati è un metodo efficace per tutelare le persone fisiche e

[56] *"Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza sulla base dell'articolo 6, paragrafo 1, deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati. Un eventuale registro completo delle condanne penali deve essere tenuto soltanto sotto il controllo dell'autorità pubblica."*

contemporaneamente sgravare i soggetti che trattano dati da una serie di pesanti responsabilità nei confronti degli interessati. Non a caso, l'articolo 3 del decreto legislativo del 30 giugno 2003, n. 196, afferma che *"I sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità."*

Nel caso in cui la finalità del trattamento renda necessario mantenere un certo grado di identificabilità dell'interessato, basti pensare alla necessità di ricontattarlo, il Regolamento mette a disposizione uno strumento meno drastico dell'uso dei dati anonimi: la pseudonimizzazione. Fra le definizioni dell'articolo 3 si può leggere *"«pseudonimizzazione»: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile"*.

In parole povere, assegnando un identificativo in codice (numerico, alfabetico o alfanumerico) all'interessato, di fatto nessuno può risalire alla sua identità, tranne naturalmente il titolare del trattamento, il quale detiene lo strumento di "decodificazione" che permette di associare i dati alla persona fisica, come ad esempio nei processi di crittografazione.

In questo modo l'identità dell'interessato acquisisce un ulteriore livello di protezione, mentre il titolare ha una maggiore libertà nell'utilizzare i dati "mascherati" a patto che la chiave di decrittazione goda di sufficiente protezione e sia a conoscenza solo ed esclusivamente degli addetti.

2.5 I nuovi attori introdotti dal regolamento

Rispetto alla precedente direttiva, il regolamento 2016/679 ha il merito di fare chiarezza sulle definizioni e i ruoli delle figure chiave nel trattamento dei dati personali, oltre ad introdurre alcuni personaggi, che saranno analizzati di seguito. Prima però è necessario offrire al lettore una breve panoramica degli altri attori in gioco e delle loro funzioni. In primo luogo, ogni trattamento necessita di un titolare e di un interessato. Il primo è la persona fisica o giuridica (ma anche autorità pubblica) che decide di dare avvio al trattamento, determinandone quindi i mezzi e le finalità secondo il diritto dell'Unione e degli Stati membri. Per il secondo non esiste una definizione giuridica specifica, in quanto il regolamento si limita a definirlo indirettamente a specificazione della nozione di dato personale. Si può dire che l'interessato sia la persona fisica identificata od identificabile, direttamente od indirettamente, dai dati che sono stati raccolti.

A differenza dell'interessato, la figura del titolare è ritratta nel dettaglio nei suoi obblighi e responsabilità, che consistono di fatto nell'implementare politiche adeguate al fine di garantire un livello di sicurezza dei dati conforme al regolamento e nel poterlo dimostrare. Si rileva il fatto che i titolari possano essere più di uno, i "contitolari" ex. art. 26[57], i quali possono dividere autonomamente fra loro i compiti relativi al trattamento dei dati, anche se ciascun contitolare rimane egualmente responsabile nei confronti dell'interessato, che può esercitare i propri diritti nei confronti di ciascun contitolare.

Qualora il titolare sia stabilito al di fuori dell'Unione europea ma offra beni e servizi o monitori il comportamento di individui stabiliti al suo interno, egli è obbligato a nominare un rappresentante, il quale deve essere stabilito in uno degli Stati ove avviene il trattamento. Sono dispensate da questo obbligo le pubbliche autorità e i trattamenti occasionali non su vasta scala che non riguardino dati giudiziari o sanitari. Questo rappresentante appunto fa le veci del titolare, salve le azioni legali che potrebbero essere intraprese contro il titolare o il responsabile originario.

Stabiliti quindi i due attori principali, ci si appresta ad analizzare altre figure introdotte o modificate dal regolamento, che vanno a completare il novero dei personaggi istituzionalizzati dal GDPR.

2.5.1 Il responsabile del trattamento o data processor

Come si è appena chiarito, la responsabilità del trattamento compete al titolare. Questa figura è però designata in base alla posizione che il soggetto occupa nell'ente o azienda che tratta i dati, non in base alle sue competenze nel campo. Per questo il legislatore si è reso conto della necessità di introdurre una figura professionale specializzata nel trattamento dei dati, ovvero il responsabile del trattamento, definito all'art. 3 come *"la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento"*.

I suoi compiti e le sue responsabilità sono meglio definiti dall'articolo 28, il quale per prima cosa precisa appunto che il *data processor* deve avere una buona conoscenza sia delle misure tecniche che di quelle organizzative al fine di poter trattare i dati in modo adeguato: in pratica si può

[57] *"Allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento. Essi determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal presente regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14, a meno che e nella misura in cui le rispettive responsabilità siano determinate dal diritto dell'Unione o dello Stato membro cui i titolari del trattamento sono soggetti. Tale accordo può designare un punto di contatto per gli interessati."* (PARLAMENTO E CONSIGLIO EUROPEO, *Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali* dati, 27 aprile 2016, art. 26 capo IV – *Contitolari del trattamento*)

affermare che, mentre il titolare è definito dalle responsabilità, il responsabile è definito dalla preparazione tecnica.

Il rapporto giuridico fra queste due figure è piuttosto articolato e deve essere definito da un contratto o da un documento giuridicamente vincolante per il diritto europeo o degli Stati membri. Affinché questo atto sia il più trasparente possibile, la Commissione si è premurata di redigere delle bozze di contratto da seguire. È chiaro che il responsabile debba agire su istruzione del titolare e conformemente al regolamento in esame, anche nel caso di trasferimenti di dati verso l'estero. Il rapporto con il titolare è collaborativo: ad esempio, poiché è il responsabile ad essere maggiormente esperto in materia di trattamento e protezione dei dati, egli deve necessariamente dare adeguate informazioni al titolare. Inoltre entrambi concorrono nel garantire all'interessato gli strumenti adatti e più semplici possibile per attivare i propri diritti, come il diritto di accesso o all'oblio. In questi casi il compito del responsabile è mettere a disposizione del titolare varie opzioni di attuazione per questo obiettivo. Anche nei confronti delle autorità di ispezione e controllo ci si aspetta che il rappresentante sia in grado di assistere il titolare nel dimostrare la conformità alle regole del trattamento in esame.

In caso di cessazione del rapporto contrattuale tra i due attori, il regolamento prevede chiaramente che sia inserita una clausola su come gestire i dati del titolare, che erano stati affidati al responsabile. Le varie soluzioni comprendono la restituzione, la cancellazione o qualsiasi altro compromesso conforme al regolamento.

Va inoltre specificato che il responsabile può essere sia un dipendente del titolare che un soggetto terzo sotto contratto. Sebbene in entrambi i casi il rapporto risulti disciplinato da un contratto, nella prima eventualità potrebbero essere assegnate maggiori responsabilità al responsabile, che potrebbero addirittura sfociare nella responsabilità di fronte alla legge in caso di violazioni. Un responsabile potrebbe anche desiderare di avvalersi di altri collaboratori, ma in questo caso deve ottenere un'autorizzazione specifica da parte del titolare.

Fra gli altri compiti di questa figurati vi è quello di sincerarsi che gli addetti al trattamento, che saranno introdotti in seguito, abbiano adeguate competenze professionali e soprattutto siano vincolati da un obbligo di riservatezza.

Infine, per quanto riguarda le responsabilità penali del responsabile del trattamento, qualora egli si renda responsabile di una violazione delle disposizioni in materia di privacy, non seguendo le istruzioni del titolare nella determinazione delle finalità e dei mezzi, diventa di fatto equiparabile ad un titolare di fronte alla legge. Questa è appunto una delle novità introdotte dal GDPR: oltre alla responsabilità per violazione di obblighi contrattuali, questa figura non può "nascondersi" dietro al titolare, ma diventa direttamente coinvolto nella procedura penale in caso di irregolarità.

2.5.2 L'addetto al trattamento

Va da sé che oltre alle figure di responsabilità e controllo, molte realtà in cui si trattano quantità ingenti di dati necessitino di altre persone incaricate di lavorare all'aggiornamento, alla conservazione e in generale al trattamento dei dati. Per motivi di funzionalità, non avrebbe senso nominare decine di responsabili, quindi si è indirettamente introdotta la figura dell'addetto al trattamento dei dati.

In Italia esisteva già un attore simile, l'incaricato del trattamento, ovvero la persona fisica che, previo incarico e formazione adeguata, materialmente "metteva mano" alle informazioni raccolte come richiestogli dal responsabile.

Il nuovo regolamento non dedica un articolo specifico a questa figura, sebbene nella realtà sia molto comune, ma la sua personalità può essere ricavata dalla lettura dell'art. 29[58]. Sebbene la lettura in italiano possa risultare non chiara, dal testo originale in inglese si intuisce chiaramente che l'articolo sia rivolto a delle persone fisiche, o "natural person", operanti sotto l'autorità del titolare e del responsabile. Anzi, in mancanza di ulteriori precisazioni è necessario assumere che solo una persona fisica possa ricoprire questo ruolo, escludendo le persone giuridiche. Questo sia a logica giuridica che pratica: naturalmente il rapporto con una persona fisica è più immediato e trasparente rispetto alla gestione di una persona giuridica come uno studio o un'agenzia.

L'articolo 29 inoltre sembra mettere sullo stesso piano e senza sostanziali differenze l'eventualità che l'addetto al trattamento possa essere designato dal titolare o dal responsabile. Anzi, si può affermare che queste due figure siano praticamente paritarie nel loro rapporto con l'addetto al trattamento: infatti questo deve operare su disposizione dei superiori, non tanto in senso gerarchico ma organizzativo.

Nella disposizione è contenuta anche una deroga a quanto sopra: infatti in virtù delle disposizioni legali dell'Unione o degli Stati membri, può accadere che un addetto possa operare direttamente e senza designazione, date le proprie qualifiche e specifiche disposizioni legislative o regolamentari.

---

[58] *"Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare 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."*
(PARLAMENTO E CONSIGLIO EUROPEO, *Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali* dati, 27 aprile 2016, art. 29 capo IV – *Trattamento e sotto l'autorità del titolare del trattamento o del responsabile del trattamento*)

Infine, è necessario che l'addetto sia una persona controllata, sia dai suoi superiori, ovvero il titolare ed il responsabile, che dal DPO, una figura di supervisione generale che sarà introdotta nel paragrafo successivo. Queste figure dovranno provvedere anche a sottoporre l'addetto ad un obbligo di riservatezza, anche qualora un regime di tale tipo non sia già previsto dalla legge. Così come per il responsabile, anche per l'addetto questo obbligo di riservatezza rimane in vigore anche dopo la fine del trattamento o la cessazione degli obblighi contrattuali.

2.5.3 Il DPO – data protection officer

Una delle principali novità introdotte dal regolamento europeo sulla protezione dei dati è rappresentata dalla creazione del responsabile della protezione dei dati, in inglese "data protection officer" o DPO. Proprio per la sua importanza, a questa figura è dedicata un'intera sezione del capo IV del documento, che delinea il suo profilo e le sue mansioni.

In generale, si può dire che il responsabile della protezione dei dati sia un soggetto incaricato di dare consigli tecnici e supervisionare tutto ciò che riguarda la protezione dei dati personali. Si deduce poi dall'art. 37.5 che questa figura debba avere un'adeguata preparazione professionale che comprenda sia la conoscenza della normativa in materia di privacy che le competenze tecniche della prassi riguardante la conservazione e la protezione dei dati personali. Non sono presenti altre descrizioni dirette del DPO, che viene definito in merito ai suoi compiti e alle sue responsabilità, più che alle sue qualità personali.

Per prima cosa, il regolamento si premura di specificare in quali occasioni sia obbligatoria la designazione del DPO: in primo luogo questo soggetto deve essere presente ogniqualvolta ci si trovi davanti ad un trattamento effettuato da un'autorità o un organismo pubblico, sia esso europeo, statale, regionale o altro. L'unica eccezione riguarda naturalmente le autorità giurisdizionali nell'esercizio delle loro funzioni. In secondo luogo è obbligatorio designare il responsabile alla protezione dei dati quando si è in presenza di trattamenti che richiedono necessariamente un controllo regolare e sistematico sugli interessati su vasta scala. Si tratta di una formulazione piuttosto oscura in prima lettura, ma in realtà ricomprende un'ampia gamma di casi, basti pensare alla grande distribuzione, ai programmi fedeltà, ma anche agli impianti di videosorveglianza che inquadrino vaste aree. L'ultimo caso contemplato dal primo comma dell'art. 37 è già familiare: il DPO deve sempre essere designato quando si trattano dati sensibili e dati sanitari.

Visto che in realtà una grande quantità di attività richiede la presenza di un responsabile, è permesso ai gruppi di imprese e alle strutture pubbliche di designare un solo DPO per più strutture, a condizione che questo sia comunque facilmente reperibile.

Addirittura il regolamento si spinge a implementare la creazione di associazioni di data protection officer settoriali. Sull'applicazione di questa indicazione sembra però esserci notevole ritardo: fino ad ora l'unica associazione di tale tipo esistente è quella che comprende tutti i DPO delle istituzioni europee e conta quindi circa una settantina di associati.

Poiché comunque non si tratta di un'autorità come il Garante, il responsabile della protezione dei dati può sia essere un dipendente (indifferentemente del titolare o del responsabile del trattamento) oppure essere un soggetto terzo sotto contratto. L'ultimo caso ha suscitato varie perplessità riguardanti l'efficacia: ci si chiede infatti come possa un unico soggetto controllare il trattamento dei dati di diversi enti molto grandi.

Riguardo alla sua posizione ed al rapporto con gli altri attori, il DPO si pone in uno spazio di totale indipendenza e terzietà: il titolare ed il responsabile del trattamento non possono fornirgli alcuna istruzione, né rimuoverlo dall'incarico per aver svolto correttamente i suoi compiti, ad esempio evidenziando delle irregolarità. Egli infatti non riferisce a questi due attori, bensì al loro vertice gerarchico. Sempre per gli stessi motivi, deve essere dotato delle adeguate risorse per svolgere i propri compiti e mantenere la prestazione, per questo motivo il suo aggiornamento professionale è a carico del responsabile o del titolare del trattamento. Addirittura per quanto riguarda le istituzioni europee è stabilita una durata in carica minima, per permettergli di analizzare in dettaglio la situazione e portare a compimento le modifiche suggerite sotto la sua stessa supervisione.

Per quanto riguarda la disponibilità, i dati di contatto del DPO devono essere pubblici e riferiti anche all'Autorità Garante. Inoltre gli interessati possono contattarlo direttamente per qualsiasi questione afferente il trattamento dei propri dati o l'attivazione dei propri diritti.

Veniamo ora alle mansioni del responsabile della protezione dei dati. Per semplificare, queste possono essere divise in due categorie: il controllo e la collaborazione. Nel primo caso questo attore sorveglia l'osservanza del regolamento e delle altre disposizioni in materia di trattamento dei dati personali, siano esse leggi europee e statali, ma anche le politiche del titolare e del data processor. Ovviamente egli deve collaborare con le autorità di controllo e fungere da contatto fra le stesse ed il titolare. Nel secondo caso invece rientrano i compiti consultivi: può fornire un parere sulla valutazione d'impatto sulla protezione dei dati oppure dare consigli al titolare, al responsabile ma anche ai dipendenti.

In questa figura si riuniscono quindi competenze tecniche e responsabilità di controllo che la rendono un fondamentale punto di contatto tra il resto del sistema di attori in gioco e le autorità. Si completa quindi lo schema che vede il titolare come colui che dà impulso al trattamento, il responsabile come colui che ne implementa le tecniche di attuazione e l'addetto come l'operatore che di fatto "muove" i dati.

2.6 I diritti dell'interessato

Come è stato più volte ribadito, l'interessato rimane sempre e comunque l'unico possessore dei propri dati, che può quindi rettificare, cancellare o muovere a suo piacimento. I diritti che i dati portano con sé sono sempre attivabili nei confronti del titolare, del responsabile e del responsabile della protezione. Inoltre al momento della raccolta dei dati, il GDPR fa obbligo al titolare di informare l'interessato dell'esistenza e delle modalità di attivazione dei propri diritti, che creano una sorta di "rete di protezione" intorno alle informazioni dell'interessato, a cui è dedicato tutto il capo III del regolamento.

2.6.1 Il diritto di accesso

La spiegazione del diritto di accesso è piuttosto letterale: si tratta del diritto dell'interessato di avere appunto accesso ai propri dati e ad alcune informazioni essenziali sul loro trattamento. L'art. 15[59] del regolamento elenca chiaramente tutte le informazioni a cui l'interessato può avere legittimamente accesso. Queste comprendono tutte le specificità relative al trattamento, come ad esempio le finalità, le categorie di dati trattati, a chi saranno comunicati e per quanto saranno conservati. A maggior ragione, quando i dati non sono stati raccolti presso l'interessato stesso ma

[59] *"1. L'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni:*

a) *le finalità del trattamento;*
b) *le categorie di dati personali in questione;*
c) *i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;*
d) *quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;*
e) *l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;*
f) *il diritto di proporre reclamo a un'autorità di controllo;*
g) *qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;*
h) *l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.*

2. *Qualora i dati personali siano trasferiti a un paese terzo o a un'organizzazione internazionale, l'interessato ha il diritto di essere informato dell'esistenza di garanzie adeguate ai sensi dell'articolo 46 relative al trasferimento.*
3. *Il titolare del trattamento fornisce una copia dei dati personali oggetto di trattamento. In caso di ulteriori copie richieste dall'interessato, il titolare del trattamento può addebitare un contributo spese ragionevole basato sui costi amministrativi. Se l'interessato presenta la richiesta mediante mezzi elettronici, e salvo indicazione diversa dell'interessato, le informazioni sono fornite in un formato elettronico di uso comune.*
4. *Il diritto di ottenere una copia di cui al paragrafo 3 non deve ledere i diritti e le libertà altrui."* (PARLAMENTO E CONSIGLIO EUROPEO, *Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali* dati, 27 aprile 2016, art. 15 capo III – *Diritto di accesso dell'interessato*)

provengano da un'altra fonte, il soggetto deve legittimamente avere tutte le informazioni su quest'ultima.

Per quanto riguarda i suoi diritti, l'interessato deve conoscerli e sapere come attivarli: può opporsi al trattamento, limitarlo, chiedere la cancellazione od il trasferimento dei dati o ancora rivolgersi ad un'autorità giurisdizionale competente. Tutte queste informazioni devono essere provvedute dal titolare o dal responsabile.

Infine, l'interessato può richiedere una copia dei suoi dati, ma per le copie successive il titolare può richiedere un contributo pecuniario per coprire le spese amministrative.

2.6.2 Il diritto all'oblio

Secondo la compiuta definizione che si può trovare sul sito del Garante Privacy italiano, per diritto all'oblio si intende il "*diritto alla cancellazione dei propri dati personali in forma rafforzata. Si prevede, infatti, l'obbligo per i titolari (se hanno "reso pubblici" i dati personali dell´interessato: ad esempio, pubblicandoli su un sito web) di informare della richiesta di cancellazione altri titolari che trattano i dati personali cancellati"*[60] che vengono così eliminati dagli archivi del titolare del trattamento e di qualunque soggetto a cui questi possa averli comunicati. Il diritto all'oblio non è però assoluto, ovvero non si può richiedere ingiustificatamente in qualsiasi circostanza e per qualsiasi tipologia di dato.

L'art. 17 delimita chiaramente le varie casistiche che andremo di seguito ad illustrare. L'interessato ha diritto a vedere cancellati tempestivamente i propri dati, nonché ogni link, copia o riproduzione degli stessi, se questi non sono più necessari allo scopo del trattamento oppure se l'interessato stesso revoca il proprio consenso o gli si oppone, cosa che egli può fare sempre a meno che non sussista un obbligo legale alla conservazione di quei dati. Inoltre, può capitare che i dati necessitino di essere eliminati per adempiere ad un obbligo legale o ancora che siano trattati illecitamente, caso nel quale l'interessato ha tutte le ragioni per chiederne la cancellazione.

Come già anticipato, non sempre l'interessato può vedere adempiuta la sua richiesta di rimozione dei dati dagli archivi: nel terzo comma dell'articolo il diritto alla privacy è soppesato di volta in volta in relazione al diritto all'informazione, alla sicurezza ed al pubblico interesse. Perciò il trattamento dei dati è autorizzato a continuare quando questi siano necessari all'esercizio del diritto alla libertà di espressione ed informazione (finalità giornalistiche); all'adempimento di obblighi legali in capo al titolare; nell'esercizio di pubblici poteri (di cui lo stesso titolare può essere investito, basti pensare ai dati conservati dalle pubbliche autorità); per tutelare la sanità

[60] "*Diritto all'oblio"*, Garante Privacy, Garante per la protezione dei dati personali, 10 set 2020.

pubblica ed infine per i familiari fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici.

Per chiarire meglio l'applicazione di questo diritto, basti pensare al recente caso che nel 2019 ha visto scontrarsi il gigante Google con la Commission nationale de l'informatique et des libertés (CNIL) francese[61], di cui peraltro si è già parlato. La controversia era nata in seguito ad una sanzione di quest'ultima ai danni di Google, il quale si era rifiutato di cancellare definitivamente alcuni dati, limitandosi ad eliminare i link ad essi nei Paesi facenti parte dell'Unione Europea. Il gigante informatico, ritenendo sufficiente e conforme al GDPR il meccanismo di "geoblocking" implementato, si è quindi appellato alla Corte di Giustizia, la quale ha deliberato che anche i motori di ricerca sono sottoposti all'obbligo di cancellazione (il quale quindi non risulta in alcun modo "aggirabile"), aggiungendo che all'interno dell'Unione europea il diritto alla privacy possa prevalere sull'interesse economico del gestore del motore di ricerca. Tuttavia, la Corte ammette che all'esterno dell'Unione non è possibile verificare il bilanciamento dell'articolo 17 con il diritto all'informazione, per cui nello svolgimento del suo lavoro all'esterno dell'Unione, Google non soggiace più all'obbligo di cancellazione dei dati.[62]

2.6.3 La portabilità dei dati

Il diritto alla portabilità dei dati costituisce senza dubbio una delle novità più rilevanti contenute nel nuovo regolamento. Questo sia perché prima del nuovo regolamento non esisteva nessun meccanismo equiparabile, sia perché si tratta inequivocabilmente di un diritto connesso agli sviluppi tecnologici dell'era digitale. Non a caso, questo diritto è attivabile solo in riguardo ai dati conservati su supporti automatizzati, in quanto sarebbe piuttosto anacronistico pretendere di muovere con la stessa facilità dei documenti cartacei.

Grazie all'articolo 20 del GDPR[63] l'interessato può chiedere i propri dati ad un titolare al fine di trasmetterli ad un altro titolare o addirittura chiedere al titolare stesso di effettuare la trasmissione, senza che il primo possa opporsi in alcun modo. Naturalmente questo diritto è attivabile solo se l'interessato ha dato il consenso al trattamento o se esiste una clausola contrattuale che abbia la stessa valenza.

Per quanto possa costituire una comodità per l'interessato, il diritto alla portabilità dei dati è però fortemente limitato, sia appunto a livello pratico in quanto il trasferimento deve risultare

[61] Sentenza C-507/17 del 24 settembre 2019 "Google LLC, succeduta alla Google Inc./ Commission nationale de l'informatique et des libertés (CNIL)"
[62] Sentenza della Corte di Giustizia C-136/17 del 24 settembre 2019, "GC e a./Commission nationale de l'informatique et des libertés (CNIL)"

"tecnicamente fattibile", sia a livello giuridico poiché questo diritto risulta circoscritto dalle casistiche descritte all'articolo 17, quale ad esempio l'esecuzione di un interesse pubblico.

Curiosamente, si tratta del primo articolo in cui viene introdotto il rispetto delle libertà altrui come parametro di limitazione ai diritti dell'interessato. Si tratta di un vincolo che può riguardare tutti gli attori in gioco: l'interessato, il titolare al quale viene richiesto di trasmettere i dati o il soggetto a cui vengono trasmessi. L'art. 29 Working Party[64] chiarisce quest'ultimo comma in relazione ai diritti di eventuali terzi, che potrebbero essere coinvolti dall'attivazione del meccanismo analizzato precedentemente. I dati dei terzi, seppur oggetto di portabilità quando connessi all'interessato, non possono essere utilizzati né dal nuovo titolare né dall'interessato stesso. In pratica l'attivazione di un trasferimento di dati non può e non deve costituire in alcun modo la base per dare l'avvio ad un nuovo trattamento. Affinché ciò avvenga, deve sussistere un nuovo consenso specifico e separato da parte del soggetto terzo ai sensi degli articoli 6, 9 e 14.

È sempre l'art. 29 Working Party a sollevare un'altra questione: quella dei dati che potrebbero entrare in possesso del titolare durante lo svolgimento del trattamento. Questa definizione potrebbe essere applicata sia ai dati che l'interessato comunica di sua sponte al titolare, sia dei cosiddetti *inferred data*, ovvero letteralmente "dati dedotti". Si tratta in questo caso dei dati generati dalla profilazione dell'interessato, che può avvenire nell'ambito del trattamento. Il parere dello Working Party è che nel secondo caso i dati non siano oggetto di portabilità, in quanto generati dal titolare e non dall'interessato. Si tratta di un interessante spunto che potrebbe però generare non poche perplessità o dare adito a scappatoie verso trattamenti illeciti, specie nell'era dei *big data*.

2.6.4 Il diritto di opposizione

Sebbene simile negli effetti al diritto all'oblio, il diritto di opposizione parte da un presupposto completamente diverso, ovvero il fatto che l'interessato possa appunto opporsi al trattamento dei propri dati ed all'eventuale profilazione ad esso connessa. A questo punto il titolare è obbligato ad astenersi dal trattamento, a meno che non sussistano cause di forza maggiore che eccedano i diritti dell'interessato, oppure il trattamento sia necessario all'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria, oppure all'esecuzione di un compito di interesse pubblico. Insolitamente, questo diritto è attivabile anche nei casi contemplati dall'articolo 89.1, ovvero per i trattamenti a fini di ricerca storica o scientifica o a fini statistici.

[64] Si tratta di un organismo consultivo ed indipendente, composto da rappresentanti nazionali, dal Garante europeo e da un membro della Commissione europea. Questo è rimasto attivo durante i lavori di stesura del GDPR, per poi cessare il suo mandato. In questo ambito era incaricato di fornire pareri, raccomandazioni e indicazioni su tutto ciò che attiene al diritto alla privacy e alla sicurezza dei dati. Questo organismo era composto da rappresentanti nazionali, dal Garante europeo e da un membro della Commissione europea.

Nel Considerando numero 69 si specifica che *"È opportuno che incomba al titolare del trattamento dimostrare che i suoi interessi legittimi cogenti prevalgono sugli interessi o sui diritti e sulle libertà fondamentali dell'interessato."* Quindi, oltre naturalmente all'obbligo di cessazione del trattamento, sorge in capo al titolare anche il dovere di dimostrare la legittimità e la necessità del trattamento in caso egli ritenga di doverlo continuare. In più naturalmente l'interessato va informato dell'esistenza e dell'attivabilità di questo diritto.

2.7 La violazione o la perdita dei dati

All'articolo 32.1[65] del regolamento sono elencati i principali parametri di sicurezza che i titolari debbono rispettare affinché il trattamento dei dati posto in essere sia ritenuto adeguatamente salvaguardato ai sensi delle regole europee. Va da sé che qualsiasi violazione di questi parametri risulti in una violazione dei dati personali dell'interessato, ma in particolare la definizione ufficiale di "violazione dei dati personali" contenuta nell'art. 4 è la seguente: *"la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati"*. Si noti quindi che il regolamento non opera sostanziali distinzioni fra il dolo e un eventuale incidente, in quanto le conseguenze per la sicurezza dei dati e dell'interessato rimangono le stesse.

È emerso anzi che, sebbene le violazioni di natura criminosa non siano da sottovalutare, per la maggior parte si tratta di eventi accidentali, che vanno dalla disattenzione degli addetti, all'utilizzo di supporti inadeguati con protezioni insufficienti, fino all'uso di dispositivi aziendali a scopi privati. Proprio perché purtroppo queste violazioni sono tutt'altro che infrequenti, il legislatore europeo si è attivato per definire una procedura di comportamento volta ad arginare temporalmente e minimizzare quantitativamente i danni che potrebbero essere arrecati all'interessato.

---

[65] *"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."*

(PARLAMENTO E CONSIGLIO EUROPEO, *Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali* dati, 27 aprile 2016, art. 32 capo IV, sez. 2– *Sicurezza del trattamento*)

2.7.1 La valutazione della violazione

Al lettore risulterà immediatamente chiaro che non tutte le violazioni sono egualmente gravi: i rischi connessi ad un'incursione nella privacy dei soggetti sono diversi a seconda della natura dei dati che vengono compromessi, della loro intelligibilità e della possibilità di associarli o meno alla persona fisica dell'interessato. Fortunatamente in molti casi la disfunzione si limita ad un inconveniente per l'azienda che tratta i dati: se una chiavetta contenente dei dati viene smarrita, si dovrà risalire a quei dati tramite l'archivio centrale. Se però quella chiavetta contiene dati particolari riferiti a persone fisiche chiaramente identificabili, la privacy degli interessati è messa in serio pericolo.

Si può quindi dire che la prima domanda da porsi è se la violazione possa avere conseguenze negative sugli individui o meno. In caso di risposta affermativa, resta da valutare la gravità di queste ripercussioni e l'effettiva probabilità che si verifichino. Dal fatto che l'interessato possa essere in pericolo o meno dipendono anche gli adempimenti successivi che il titolare deve portare a termine, che andiamo ora ad analizzare.

2.7.2 Gli obblighi del titolare: notifiche e rimedi

Nel rilevare un'avvenuta violazione dei dati, o *data breach*, sorge automaticamente ed immediatamente un obbligo di notifica in capo al titolare del trattamento: egli deve rendere nota l'infrazione all'autorità Garante competente, ovvero nel territorio della quale è avvenuto il fatto, entro e non oltre 72 ore dallo stesso. Nell'articolo 33 è coinvolta anche la figura del responsabile del trattamento, in quanto egli è verosimilmente la figura più informata sugli aspetti tecnici riguardanti la sicurezza dei dati e pertanto sulle possibili conseguenze della violazione.

Affiché la notifica sia quanto più completa possibile, questa deve contenere informazioni circa la natura della violazione, i contatti del responsabile o di chiunque sia incaricato di dare informazioni in merito, una valutazione in merito alle probabili conseguenze e la descrizione delle misure adottate o che si intende adottare per porre rimedio al *data breach* o almeno limitarne gli effetti negativi.

Come già anticipato, quando sussiste un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare è obbligato a notificare la violazione anche agli interessati nelle stesse modalità descritte per l'autorità Garante. Può esimersi da questo obbligo ad esempio se i dati oggetto di violazione erano adeguatamente protetti da cifratura, in modo da risultare intellegibili solo per chi fosse autorizzato al trattamento. Nella stessa ottica, anche misure successive in grado di scongiurare i rischi per le libertà e i diritti dell'interessato assolvono il titolare dall'obbligo di notifica.

Qualora la violazione riguardi una moltitudine di interessati, per cui lo sforzo richiesto al titolare risulterebbe sproporzionato, egli può effettuare pubblicamente la notifica in modo che gli interessati siano comunque informati con efficacia.

Soffermandosi sull'analisi letterale delle disposizioni dell'art. 34[66] si nota che, relativamente alla qualificazione del rischio, il legislatore scegli la parola "elevato". Più che una specificazione, si tratta purtroppo di un criterio suscettibile di interpretazione da parte del titolare, che potrebbe scegliere di notificare la violazione solo a fronte di situazioni quasi tragiche, oppure potenzialmente in qualsiasi caso.

2.7.3 Ricorsi e sanzioni

Il capo VIII del regolamento si occupa degli aspetti riguardanti la presentazione di un reclamo o di un ricorso, l'attribuzione della responsabilità e la somministrazione delle sanzioni.

L'interessato infatti può sempre presentare un reclamo all'autorità di controllo se ritiene che il trattamento di cui è oggetto violi le disposizioni del regolamento stesso. Se poi non è soddisfatto della decisione presa dall'autorità di controllo o se questa manca di riferirgli circa lo stato o l'esito del reclamo entro tre mesi, l'interessato può proporre un ricorso giurisdizionale effettivo.

Il ricorso può essere presentato anche contro il titolare o il responsabile del trattamento quando si ritiene che questi abbiano violato le disposizioni del regolamento, a condizione che avvenga presso le autorità dello Stato in cui sono stabiliti o in cui l'interessato risiede abitualmente. Non è possibile presentare ricorso presso le autorità statali se il titolare o il responsabile sono autorità pubbliche di uno Stato membro che esercitano poteri pubblici.

---

[66] *"1. Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.*
2. La comunicazione all'interessato di cui al paragrafo 1 del presente articolo descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d).
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."*

(PARLAMENTO E CONSIGLIO EUROPEO, *Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali* dati, 27 aprile 2016, art. 34 capo IV, sez. 2– *Comunicazione di una violazione dei dati personali all'interessato*)

Il GDPR ammette che l'interessato si faccia rappresentare da un'organizzazione o un'associazione senza scopo di lucro definita dal diritto di uno Stato membro in questi ricorsi, a patto che lo scopo statutario di questo organo riguardi appunto la difesa dei diritti e delle libertà concernenti la privacy. In questo modo il legislatore europeo spiana la strada per possibili *class action*, ovvero un'azione legale portata avanti da una moltitudine di querelanti, ciascuno rivendicante i propri diritti singolarmente, in un unico procedimento giudiziale. Si tratta di una eventualità niente affatto remota in casi in cui le violazioni riguardino trattamenti su larga scala.

Sempre in un'ottica globale, nel regolamento è contenuta la disciplina riguardante il caso in cui siano in corso azioni legali contro lo stesso soggetto in vari Stati membri, come nel caso delle multinazionali, stabilendo che le autorità giudiziarie venute a conoscenza dell'esistenza di un procedimento pendente contro lo stesso soggetto in un altro Stato possano sospendere le proprie azioni.

Oltre al ricorso, se l'interessato ha subito un danno materiale o immateriale causato dalla violazione delle disposizioni del regolamento, ha diritto ad ottenere il risarcimento del danno da parte del titolare o del responsabile del trattamento. L'obbligo a risarcire l'interessato sorge in capo a questi due soggetti solo qualora non possano dimostrare che la violazione non è loro imputabile in alcun modo. Al comma 4 dell'art. 82[67] è stabilita la responsabilità solidale per l'intero ammontare del danno, da dividere appunto fra tutti i responsabili e i titolari coinvolti.

I portafogli dei titolari e dei responsabili però non sono a rischio solo per quanto riguarda i risarcimenti, in quanto anche le autorità giurisdizionali hanno facoltà di infliggere loro sanzioni amministrative, anche ingenti. Il legislatore europeo però si limita a regolamentare soltanto alcuni casi sanzionatori, imponendo un tetto massimo di 40 milioni di euro o del 4% del fatturato dell'anno precedente per le imprese. In tutti i casi non contemplati dall'articolo 83, gli Stati membri possono instaurare il proprio regime sanzionatorio, naturalmente comunicando le disposizioni alla Commissione. Questo però non basta a stabilire un criterio univoco sull'amministrazione delle sanzioni in tutta l'Unione, che infatti risulta disomogenea: basti pensare che Danimarca ed Estonia non consentono di applicare alcun tipo di sanzione. Si è cercato di comporre questa discrepanza con il "considerando" 151, che aggira di fatto il problema

[67] *"Qualora più titolari del trattamento o responsabili del trattamento oppure entrambi il titolare del trattamento e il responsabile del trattamento siano coinvolti nello stesso trattamento e siano, ai sensi dei paragrafi 2 e 3, responsabili dell'eventuale danno causato dal trattamento, ogni titolare del trattamento o responsabile del trattamento è responsabile in solido per l'intero ammontare del danno, al fine di garantire il risarcimento effettivo dell'interessato."* (PARLAMENTO E CONSIGLIO EUROPEO, *Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali* dati, 27 aprile 2016, art. 82.4 capo IV, sez. 2– *Diritto al risarcimento e responsabilità*)

.

istituendo un regime equivalente: *"Le norme relative alle sanzioni amministrative pecuniarie possono essere applicate in maniera tale che in Danimarca la sanzione pecuniaria sia irrogata dalle competenti autorità giurisdizionali nazionali quale sanzione penale e in Estonia la sanzione pecuniaria sia imposta dall'autorità di controllo nel quadro di una procedura d'infrazione, purché l'applicazione di tali norme in detti Stati membri abbia effetto equivalente alle sanzioni amministrative pecuniarie"*.

2.8 Le nuove tecnologie

Uno degli aspetti più insistentemente evidenziati nel corso dei lavori preliminari e di stesura del GDPR è stata la necessità di adeguare la legislazione europea alle necessità derivanti dall'evoluzione delle tecnologie di comunicazione, ormai in crescita sempre più rapida. Si trattava quindi di dare un'impostazione generale che, tenendo conto delle peculiarità tecniche di ogni mezzo (PC, *smartphone*, nuovi dispositivi di archiviazione) giungesse a dare un po' di ordine nella giungla telematica in cui oggi l'individuo è sempre più calato.

2.8.1 I dispositivi mobili

Per "dispositivo mobile" si intende un dispositivo portatile, ovvero pienamente utilizzabile dall'utente ovunque egli sia. Possiamo distinguere fra dispositivi mobili attivi (cellulare, *smartphone*, computer portatile, *tablet*) o passivi (dispositivi di archiviazione privi di connessioni remote come ad esempio le chiavette USB).

La vera sfida posta dall'utilizzo sempre più diffuso di queste apparecchiature riguarda la disponibilità in un solo apparecchio di molteplici funzioni, programmi e applicazioni. In questo modo la vita privata si fonde con quella lavorativa, ad esempio ogniqualvolta un dipendente di un'azienda usa il proprio *smartphone* per controllare la casella di posta elettronica del lavoro. Va da sé che le informazioni contenute nelle mail di lavoro, se lo *smartphone* in questione venisse smarrito o rubato, potrebbero trasformarsi in un pericolo per la privacy di svariati soggetti. Ciononostante, moltissime aziende incoraggiano una politica di *"bring your own device"*[68], che potrebbe a lungo andare portare ad una lievitazione delle cifre riguardanti le violazioni accidentali della privacy. Proprio per questo le apparecchiature su cui svolgere le proprie mansioni lavorative andrebbero fornite dall'azienda, in modo da evitare questo tipo di incidenti. Si potrebbero anche adottare tecniche di *mobile device management* o MDM, che consentono di monitorare le attività dei dipendenti. In questo caso però ci si troverebbe di fronte al rischio che siano i datori di lavoro ad invadere la privacy dei propri dipendenti.

[68] Letteralmente "porta il tuo dispositivo", nota anche con l'acronimo inglese BYOD.

Moltissimi dei dispositivi elencati sopra sono poi dotati di tracciatori GPS in grado di localizzare la posizione dell'utente e di trasmetterla al gestore. In questo caso il problema è che non sempre l'utente è consapevole che il proprio dispositivo sta generando dati sulla propria posizione. Ancor più problematico è il caso in cui la geolocalizzazione avviene di *default*, ovvero è una funzione predefinita del dispositivo. In questo caso il soccorso legale potrebbe venire dalle nuove regole sull'informazione dell'interessato, il quale dovrebbe sempre essere a conoscenza del fatto che il proprio dispositivo potrebbe generare dati che lo riguardano.

2.8.2 I dati personali digitalizzati

È innanzitutto fondamentale spiegare che per dati personali digitalizzati non si intendono dati in formato elettronico custoditi su supporti fisici come chiavette USB, CD o *hard disk*, ma piuttosto dati non tangibili e dei quali non ci si può impadronire fisicamente, in quanto convertiti in forma digitale e conservati in ambienti virtuali quali ad esempio i *cloud*.

In questi casi tendenzialmente l'accesso ai dati è di tipo *Single Sign On* o SSO, vale a dire che all'utente basta autenticarsi una sola volta per accedere a svariati siti o applicazioni. Non ricorda ad esempio gli account di Google? Questi infatti possono essere connessi ad un servizio di posta elettronica, ad uno di archiviazione di immagini o ancora ad una mappa GPS. Questo metodo può essere applicato anche nelle aziende: il datore può fornire ai propri dipendenti delle chiavi di autenticazione valide solo per le mansioni lavorative, in modo da evitare pericolose commistioni.

Un altro modo per proteggere la propria identità virtuale, specie se ci si trova nei panni del consumatore oberato di pubblicità, è fornire indirizzi di posta elettronica temporanei. Esistono infatti numerosi servizi che offrono indirizzi di posta elettronica in grado di autodistruggersi dopo un dato tempo, in modo da dare al consumatore la possibilità di accedere a servizi online o siti web senza dover subire poi l'attacco di un plotone di mail pubblicitarie.

A questo punto il lettore potrebbe chiedersi, alla luce di quanto esposto fino ad ora, se non sia più semplice rendere inintelligibili i dati, anche quando si tratta di dati digitalizzati. Nella realtà dei fatti, in effetti, tutte le raccomandazioni basate sul GDPR mirano a ridurre la quantità e la decifrabilità dei dati che gli utenti sono costretti a fornire nell'ambito dei rapporti online. Infatti, minore è la quantità di dati richiesta e minore sarà il rischio connesso ad essi. Le autorità Garanti poi sono concordi nel suggerire sempre, quando possibile, applicativi che rendano indecifrabili i dati a soggetti non autorizzati, come la crittografia, la pseudonimizzazione o l'anonimizzazione.

2.8.3 Una nuova sfida: i big data

Per *big data* si intendono elevati flussi di informazioni, caratterizzati dalla velocità con cui vengono acquisiti e dalla varietà di dati che racchiudono, i quali vengono "catturati" e trattati per sostenere attività principalmente promozionali, ma anche decisionali. Per spiegare meglio di cosa

si tratta, basta relazionarli all'uso dei *social network*, servizi in cui il gestore ha a disposizione una gigantesca quantità di informazioni ogni giorno, presentate in vari formati e modalità, che può raccogliere a velocità impressionante automatizzando il procedimento: basti pensare che Facebook si appropria di circa 500 *terabyte* di dati ogni giorno.

Ma a che cosa servono tutte queste informazioni? Analizzandole, incrociandole ed aggregandole si ottengono dati aggiuntivi, derivati da quelli raccolti, estremamente utili a fini commerciali e pubblicitari. Siamo così in presenza dei cosiddetti *metadati*, appunto informazioni derivate.

Sebbene nel regolamento non esista un articolo specifico dedicato ai *big data*, è chiaro che ci si trova di fronte ad un trattamento del tutto particolare, per il quale è necessario approntare un procedimento particolare, comprendente anche una valutazione dei rischi ad esso connessi. A questo proposito la European Union Agency for Cybersecurity[69] consiglia di adottare l'approccio della *privacy by design*, ovvero di integrare nella struttura stessa del nucleo analitico dei *big data* i meccanismi di sicurezza più congrui, insieme ai dispositivi per limitare la "corsa alle informazioni".

In una disciplina in formazione come questa, il maggior aiuto fornito dal regolamento viene dai meccanismi di consultazione preventiva che sono messi a disposizione dei titolari e dei responsabili. Infatti l'articolo 36 prevede per questi soggetti la possibilità di consultarsi con l'autorità di controllo quando si riscontra che il trattamento potrebbe presentare dei rischi elevati in mancanza dell'adozione di misure specifiche di protezione da parte del titolare e del responsabile stessi. Per velocizzare la procedura, si impone inoltre all'autorità Garante un tempo massimo di otto settimane entro cui rispondere, prorogabile al massimo di altre sei settimane in casi particolari che lo richiedano. Il Garante è quindi costretto ad esprimersi favorevolmente o a vietare il trattamento in attesa che si compiano gli adempimenti necessari a renderlo lecito e sicuro.

2.9 Il trasferimento all'estero dei dati

La necessità, per un titolare, di trasferire i dati da un Paese ad un altro tramite un'operazione di comunicazione è un fatto del tutto normale ed anzi molto comune. Di fatto si tratta di un trasferimento di dati a terzi a tutti gli effetti, ma in questo caso non basta informare l'interessato: affinché il trasferimento sia legittimo, il soggetto estero deve garantire un livello di sicurezza equivalente a quello europeo. Ma prima di addentrarci nelle specificità, è opportuno definire cosa si intende per trasferimento all'estero dei dati.

[69] Agenzia per la Cibersicurezza dell'Unione Europea, nota anche con l'acronimo ENISA. Si tratta di un centro di consulenza per materie informatiche dell'Unione Europea.

Si può affermare di trovarsi dinanzi ad un trasferimento di dati personali all'estero in *"tutti i casi in cui un titolare del trattamento si attiva per rendere disponibili dati personali ad un soggetto terzo, che si trova in un Paese terzo"*[70] da cui la Corte di Giustizia Europea escluse nel 2003 il caso in cui sia una persona fisica a caricare dei dati su internet, purché la pagina sia caricata sul *server* del suo *provider*, localizzato entro i confini dell'Unione europea.

2.9.1 Principi generali

Il regolamento indica all'articolo 44[71] un principio generale universalmente valido per il trasferimento dei dati verso Paesi esteri, traducibile con la garanzia che il livello di protezione delle persone fisiche garantito entro i confini dell'Unione Europea resti invariato anche al di fuori. Infatti, nel muovere informazioni destinate ad essere trattate in un Paese terzo, ci si deve assicurare che il titolare ed il responsabile destinatari rispettino le condizioni dettate dal regolamento, anche in ulteriori trasferimenti verso altri Paesi, nei quali sono quindi obbligati a rispettare lo stesso articolo 44.

Gli articoli successivi entrano quindi maggiormente in dettaglio, analizzando i casi in cui può essere approvato il suddetto trasferimento. L'articolo 45 disciplina il meccanismo secondo il quale la Commissione emette una decisione di adeguatezza, dichiarando che un Paese terzo rispetta i livelli di garanzie richiesti dal regolamento e rendendo quindi possibile il trasferimento di dati verso quel Paese. Nel prendere questa decisione, la Commissione prende in considerazione svariati elementi quali ad esempio quelli di natura legale: lo stato di diritto, la tutela dei diritti umani e delle libertà fondamentali, la legislazione locale in materia di privacy e protezione dei dati personali nonché la sua attuazione, la giurisprudenza in materia e la possibilità di ricorso. Inoltre ai fini della Commissione rileva anche la presenza o meno di un'autorità indipendente che vigili sul rispetto delle norme in materia di privacy, nonché l'impegno a livello internazionale presso organismi o tramite Trattati che si occupino di questi diritti.

La decisione di adeguatezza non è però l'unico modo per poter attivare un trasferimento verso l'estero: infatti la dimostrazione di possedere garanzie adeguate a proteggere i dati personali dei

---

[70] A. BIASIOTTI, *Il nuovo regolamento europeo sulla protezione dei dati,* III ed., Roma, 2018, pag. 774

[71] *"Qualunque trasferimento di dati personali oggetto di un trattamento o destinati a essere oggetto di un trattamento dopo il trasferimento verso un paese terzo o un'organizzazione internazionale, compresi trasferimenti successivi di dati personali da un paese terzo o un'organizzazione internazionale verso un altro paese terzo o un'altra organizzazione internazionale, ha luogo soltanto se il titolare del trattamento e il responsabile del trattamento rispettano le condizioni di cui al presente capo, fatte salve le altre disposizioni del presente regolamento. Tutte le disposizioni del presente capo sono applicate al fine di assicurare che il livello di protezione delle persone fisiche garantito dal presente regolamento non sia pregiudicato."* (PARLAMENTO E CONSIGLIO EUROPEO, *Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali* dati, 27 aprile 2016, art. 44, capo V– *Principio generale per il trasferimento*)

cittadini europei può addirittura essere sufficiente al trasferimento, senza dover richiedere autorizzazioni specifiche alle autorità di controllo. In questo caso basta l'esistenza di un documento giuridicamente vincolante tra autorità e organismi pubblici, di un codice di condotta, di un meccanismo di certificazione o ancora di norme di protezione specifiche. Nell'articolo 46 vengono anche citate le norme vincolanti d'impresa o *binding corporate rules*, ovvero un documento contenente una serie di regole improntate a principi vincolanti al cui rispetto sono obbligate tutte le società appartenenti ad uno stesso gruppo, qualora vogliano trasferire dati fra di loro. In questo caso il documento deve rispettare tutta una serie di parametri indicati dall'articolo 47.

Naturalmente sono previste alcune deroghe al divieto di trasferire dati, fatti salvi gli articoli di cui sopra. Infatti, se l'interessato dà il suo consenso al trasferimento oppure il trasferimento è previsto da un contratto, questo può avvenire senza ulteriori approvazioni. Il trasferimento è inoltre sempre attuabile in caso di necessità, come ad esempio per motivi di interesse pubblico o per l'esercizio di un diritto in sede giudiziaria, nonché per tutelare i diritti stessi dell'interessato qualora non sia in grado di prestare il proprio consenso (abbiamo già analizzato le situazioni di emergenza sanitaria) o il diritto all'informazione dei cittadini.

2.9.2 Il caso Safe Harbor ed il nuovo accordo EU – US Privacy Shield

L'Unione Europea e gli Stati Uniti sono da sempre partner commerciali e non solo: era quindi più che naturale che venisse approvato un accordo sulla base dell'art. 46 per autorizzare il trasferimento di dati fra i due organismi sulla base di adeguate garanzie. Questo accordo specifico, stipulato fra il Dipartimento del Commercio degli Stati Uniti e l'Unione Europea, fu approvato nel novembre del 2000 con il nome di *Safe Harbor* ovvero "porto sicuro".

Le aziende americane potevano così aderire all'accordo e venire automaticamente iscritte alla lista di aziende "degne di fiducia" eliminando il fastidioso problema di ottenere un'autorizzazione specifica per trattare dati di cittadini europei da ogni Garante statale. In questo modo anche i ricorsi presentati da cittadini europei potevano essere gestiti localmente.

Di fatto questo accordo vincolava le aziende al rispetto di un catalogo di sette principi, a cui queste potevano adeguarsi sia seguendo pedissequamente le indicazioni del *Safe Harbor*, sia sviluppando una privacy policy propria ma pur sempre conforme. Questi sette principi comprendevano l'uso dell'informativa, adeguate garanzie di sicurezza ed il diritto di accesso per l'interessato. Naturalmente l'interessato doveva essere sempre informato su qualsiasi decisione e l'ultima parola doveva spettare sempre a lui, sia riguardo la compatibilità fra dati trattati e obiettivi del trattamento (principio di integrità), che riguardo al trasferimento verso soggetti terzi. Infine le aziende aderenti dovevano essere sottoposte ad un'adeguata sorveglianza sull'applicazione di questi principi.

Questo accordo ha avuto una vita relativamente lunga, chi è stata però bruscamente interrotta nel 2015 dallo scoppio della vicenda riguardante Edward Snowden, ex tecnico della CIA e collaboratore della National Secrity Agency, il quale rivelò l'esistenza di programmi segreti di sorveglianza di massa, portati avanti da questo organismo soprattutto ai danni di cittadini non statunitensi. A questo punto la Corte di Giustizia europea, preoccupata dagli avvenimenti, ha deciso di dichiarare inefficace l'accordo Safe Harbor a partire da febbraio del 2016. Questo però ha lasciato in sospeso svariati rapporti in essere fra soggetti americani ed europei, rendendo necessaria la tempestiva approvazione di un accordo equivalente.

Si può dire che contestualmente al decadimento dell'accordo Safe Harbor l'Unione Europea ed il Dipartimento del Commercio statunitense cominciassero già i lavori di stesura del nuovo accordo, nei fatti molto simile al precedente, ma con l'aggiunta di nuove garanzie per i cittadini europei. Di fatto le differenze sostanziali tra il *Safe Harbor* ed il *Privacy Shield* si rilevano non tanto nel settore commerciale, quanto nelle clausole riguardanti la vigilanza sulle attività delle autorità americane, con un accordo scritto riguardante le limitazioni e le salvaguardie per gli accessi effettuati dalle agenzie governative verso i dati provenienti dall'Unione Europea. Viene introdotto anche un meccanismo di risoluzione delle controversie tra USA e UE con la creazione di un'autorità indipendente con sede nell'Unione.

CAPITOLO 3 – La realtà italiana: PMI, sanità e altro

Dopo aver esplorato la genesi del diritto alla privacy ed i principi generali a cui siamo sottoposti in quanto cittadini europei, giunti al capitolo finale ho ritenuto opportuno completare il quadro analizzando il funzionamento dei meccanismi di protezione della privatezza in Italia. Non essendo possibile esaurire ogni aspetto in questa sede, in quanto ciò richiederebbe la stesura di una tesi a sé, saranno toccati alcuni casi particolari ed esemplificativi riguardanti soprattutto il mondo delle attività private, dalle piccole e medie imprese al settore della sanità, ma anche le principali novità giuridiche in materia.

Prima di tutto ciò, ritengo però necessario presentare una brevissima storia dell'evoluzione di questo settore legale in Italia prima del sopraggiungere della normativa europea del 2016.

3.1 I primi passi in Italia

Sebbene prenda le sue prime mosse nei lontani anni Cinquanta, il percorso per giungere ad un'adeguata tutela del diritto alla privacy nella penisola è lento e spesso accantonato in nome di interessi più pressanti. Bisognerà infatti aspettare gli anni Novanta per vedere una legge atta a regolamentare questo settore, mentre fino ad allora la privatezza è vissuta come un diritto "secondario", sempre derivato implicitamente da disposizioni costituzionali oppure dalla giurisprudenza della Corte Costituzionale o della Corte di Cassazione.

3.1.1 Esiste una tutela costituzionale?

Tutti sanno che la Costituzione è la carta fondamentale dell'ordinamento italiano e sicuramente è altrettanto noto che essa contiene il catalogo dei diritti e dei doveri dei cittadini del Bel Paese. La cosa più naturale da fare è quindi ricercare la base giuridica per la stesura di una norma di rango legislativo proprio nella Costituzione. Ebbene, nel fare questo esercizio il lettore scoprirà che non esiste una disposizione specifica di rango costituzionale che protegga il diritto alla privacy. Come può quindi questo diritto entrare nel nostro ordinamento?

Le strade percorribili sono due. La prima, già conosciuta, è il rinvio operato dall'articolo 117, il quale stabilisce che «*La potestà legislativa è esercitata dallo Stato e dalle Regioni nel rispetto della Costituzione, nonché dei vincoli derivanti dall'ordinamento comunitario e dagli obblighi internazionali.*»[72] In questo caso perciò la tutela della privacy entra nell'ordinamento statale in quanto prevista nel catalogo dei diritti dell'individuo presente nella Carta dei diritti fondamentali

[72] Costituzione della Repubblica Italiana, GU n. 298 del 27 dicembre 1947, aggiornata al 23 aprile 2012, titolo V, art. 117.

dell'Unione Europea all'articolo 8, ma anche in quanto prevista dal Trattato internazionale noto come Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali.

L'altra opzione è quella di dedurre implicitamente l'esistenza di una tutela costituzionale della privatezza dalle disposizioni che la Costituzione stessa dà. In questo caso vanno considerati gli articoli 14, 15 e 21, riguardanti rispettivamente l'inviolabilità del domicilio, la libertà e la segretezza della corrispondenza e la libertà di manifestazione del pensiero. Dal combinato disposto di queste disposizioni si evince un sistema piuttosto completo e articolato che protegge la sfera intima dell'individuo: per prima cosa i suoi pensieri, poi la sua corrispondenza ed infine il luogo fisico, ove la sfera privata si manifesta, vale a dire la sua abitazione. Pur non partendo dagli stessi presupposti del legislatore europeo, l'Assemblea costituente ha quindi saputo creare un sistema di tutele del tutto equivalente a quello comunitario, almeno negli effetti.

3.1.2 La "Sentenza Caruso" e la libertà di informazione

Come già accennato, uno dei contributi più importanti allo sviluppo delle norme sulla privacy in Italia arriva dalla giurisprudenza delle Corti superiori. La prima sentenza "storica", se così si può dire, arriva nel lontano 1956 dalla Corte di Cassazione e riguarda un contenzioso fra gli eredi del noto tenore Enrico Caruso e la Asso Film, una casa produttrice. Nel 1951 quest'ultima aveva lanciato nei cinema il film "Enrico Caruso, Leggenda di una voce", che secondo gli eredi dipingeva il defunto in una luce poco lusinghiera, oltre ad includere episodi del tutto falsi.

In prima istanza i giudici conclusero che non si trattava di uso illecito dell'identità del cantante, pur condannando la Asso Film per le fattispecie di offesa al decoro e all'onore nei riguardi di alcune scene che ritraevano il tenore ubriaco e sul punto di uccidersi, nonché per indebita invasione della riservatezza a causa di alcune scene riguardanti la dura infanzia del cantante. Il risultato fu un risarcimento patrimoniale di 2 000 000 di lire agli eredi.

Questi si rivolsero allora alla Corte di Appello di Roma, che con una sentenza del 17 maggio 1955 condannò solo le scene riguardanti l'infanzia di Caruso, ove si ritraeva un pignoramento ed un accesso d'ira del padre, argomentando che queste non fossero necessarie per comprendere la personalità dell'artista.

A questo punto i querelanti adirono la Corte di Cassazione, sostenendo che l'attività del narratore o comunque del biografo debba limitarsi agli episodi determinanti per la comprensione della personalità dell'artista, tralasciando invece i fatti privati, intimi, familiari e affettivi, che non presentano alcun interesse apprezzabile per eventuali terzi, eccezion fatta per una malsana curiosità. È così in gioco il diritto alla riservatezza in quanto tale, ovvero separato dal diritto alla tutela dell'onore, così come riconosciuto nel mondo anglosassone ormai da qualche tempo grazie all'azione di Warren e Brandeis e di Prosser.

La Corte di Cassazione, dal canto suo, concluse in favore l'esistenza del diritto alla privatezza da alcune norme della legge sul diritto d'autore. In particolare nella sentenza n. 4487 del 1956 essa riprese le disposizioni riguardanti il ritratto[73], interpretandole in senso estensivo ed applicandole anche alle opere narrative o rappresentative della vita altrui. Si giunse quindi alla conclusione che nemmeno l'indubbia fama del defunto, né tantomeno il suo status di "personalità pubblica" potessero giustificare la pubblicizzazione di episodi della sua vita privata e familiare, che non fossero pertinenti allo scopo di comprendere la sua personalità artistica.

In seguito a questa pronuncia risultava quindi chiara la linea di demarcazione fra l'esercizio del diritto di cronaca e la tutela della sfera privata, a cui avevano diritto anche le personalità pubbliche o famose. Pur ammettendo la frammentarietà delle disposizioni a tutela della vita privata delle persone, la Corte di Cassazione creava così un precedente nell'affermare che solo un oggettivo interesse pubblico potesse prevalere sul diritto alla privatezza nel portare a conoscenza dell'*audience* fatti riguardanti la vita intima dei soggetti pubblici.

3.1.3 Il ruolo della giurisprudenza

Con la sentenza di cui si è appena discusso si apre anche in Italia il dibattito sull'opportunità di inserire o meno nell'ordinamento un principio unitario di tutela per il diritto alla privacy. Si dovranno però attendere gli anni Settanta per le due sentenze fondamentali, grazie alle quali viene sancita definitivamente l'esistenza di un diritto alla riservatezza, autonomo rispetto alle tutele già esistenti nelle leggi italiane.

La prima di queste pronunce in ordine cronologico risale al 1973. Si tratta di un ricorso alla Corte Costituzionale che vede coinvolti quotidiani come Il Messaggero e Il Corriere d'Italia in un ricorso che vede soppesare sulla bilancia della giustizia ancora una volta la libertà di stampa e di informazione contro il diritto alla riservatezza, questa volta in relazione alla diffusione di immagini e fotografie. Di fronte alla questione di costituzionalità posta di fronte alla Corte riguardo a svariate disposizioni del Codice Civile, della legge sul diritto d'autore e non da ultimo

[73] *«Il ritratto di una persona non può essere esposto, riprodotto o messo in commercio senza il consenso di questa, salve le disposizioni dell'articolo seguente.*
Dopo la morte della persona ritrattata si applicano le disposizioni del 2°, 3° e 4° comma dell'art. 93.»
«Non occorre il consenso della persona ritrattata quando la riproduzione dell'immagine è giustificata dalla notorietà o dall'ufficio pubblico coperto, da necessità di giustizia o di polizia, da scopi scientifici, didattici o culturali, o quando la riproduzione è collegata a fatti, avvenimenti, cerimonie di interesse pubblico o svoltisi in pubblico.
Il ritratto non può tuttavia essere esposto o messo in commercio, quando l'esposizione o messa in commercio rechi pregiudizio all'onore, alla reputazione od anche al decoro della persona ritrattata.»
(Legge sulla protezione del diritto d'autore "*Protezione del diritto d'autore e di altri diritti connessi al suo esercizio*" del 22 aprile 1941, n. 633 aggiornata al 30/06/2020, art. 96-97, titolo II, capo IV, sez. II.)

anche della Costituzione, i giudici si esprimono in un'unica sentenza che afferma di fatto l'infondatezza del ricorso.

Ciò che ci interessa in particolare è la difesa dei commi 2 e 3 dell'art. 21 della Costituzione[74], riguardante proprio la libertà di stampa. La Corte chiarisce inequivocabilmente che questa libertà non può interferire con i diritti inviolabili della persona umana. Il fine dell'articolo 21 è infatti quello di proteggere l'espressione del pensiero per mezzo della carta stampata da censure ingiustificate da parte del potere pubblico, ma ciò non significa che la libertà di informazione possa assolutizzarsi ai danni del singolo: è conseguentemente necessaria la tutela costituzionale dei diritti di onore, riservatezza, intimità e reputazione.

La Corte Costituzionale però non si limita a queste affermazioni, ma inserisce nella sentenza anche un esplicito riferimento ai principi fondamentali sanciti dagli articoli 8 e 10 della Convenzione Europea sui diritti dell'uomo, che formano un sistema di protezione del diritto alla riservatezza. Con un'impostazione simile a quella della nostra Costituzione, l'articolo 10 della Convenzione contiene sia il riconoscimento della libertà di espressione che le sue limitazioni, fra le quali è inclusa proprio quella riguardante la protezione della reputazione e dei diritti altrui. È quindi chiaro che la libertà di stampa finisca dove inizia la sfera privata dell'individuo.

La seconda sentenza che verrà qui presa in esame risale è la n.2129 del 27/5/1975. Questa volta la protagonista è la Corte di Cassazione, chiamata a pronunciarsi sul caso riguardante la principessa Soraya Esfandiary, già moglie dello scià di Persia (Iran) Reza Pahlavi, fotografata nella sua villa, mentre si trovava in atteggiamenti intimi con il regista Franco Indovina. L'ex imperatrice aveva sporto denuncia contro il settimanale "Gente", sul quale erano state pubblicate le fotografie, sostenendo che le immagini fossero state acquisite con mezzi illeciti, atti a catturare momenti di vita quotidiana di una personalità ormai ritiratasi a vita privata.

---

[74] *«1. Tutti hanno diritto di manifestare liberamente il proprio pensiero con la parola, lo scritto e ogni altro mezzo di diffusione.*
2. La stampa non può essere soggetta ad autorizzazioni o censure.
3. Si può procedere a sequestro soltanto per atto motivato dell'autorità giudiziaria [cfr. art. 111 c.l] nel caso di delitti, per i quali la legge sulla stampa espressamente lo autorizzi, o nel caso di violazione delle norme che la legge stessa prescriva per l'indicazione dei responsabili.
4. In tali casi, quando vi sia assoluta urgenza e non sia possibile il tempestivo intervento dell'autorità giudiziaria, il sequestro della stampa periodica può essere eseguito da ufficiali di polizia giudiziaria, che devono immediatamente, e non mai oltre ventiquattro ore, fare denunzia all'autorità giudiziaria. Se questa non lo convalida nelle ventiquattro ore successive, il sequestro s'intende revocato e privo d'ogni effetto.
5. La legge può stabilire, con norme di carattere generale, che siano resi noti i mezzi di finanziamento della stampa periodica.
6. Sono vietate le pubblicazioni a stampa, gli spettacoli e tutte le altre manifestazioni contrarie al buon costume. La legge stabilisce provvedimenti adeguati a prevenire e a reprimere le violazioni.»
(Costituzione della Repubblica Italiana, GU n. 298 del 27 dicembre 1947, aggiornata al 23 aprile 2012, titolo I, art. 21)

La Cassazione riconosce infine a Soraya Esfandiary il diritto al risarcimento, ma con una motivazione piuttosto innovativa. Infatti, anziché far ricadere il caso nella fattispecie di violazione del domicilio, come si era fatto fino ad allora, i giudici scelgono di uniformarsi alla giurisprudenza della Corte Costituzionale nell'affermare l'esistenza di una violazione nei confronti di un autonomo ed indipendente diritto alla riservatezza, superando quindi le sentenze precedenti. La Corte riconosce esplicitamente la necessità di modificare il diritto coerentemente con la chiara tendenza internazionale «*ad estendere la difesa della personalità umana, sia nei confronti dell'abuso dei pubblici poteri, che nei rapporti intersoggettivi individuali.*»[75]

Nella sentenza si trovano anche riferimenti ai repentini cambiamenti tecnologici, grazie ai quale sarà sempre più possibile penetrare nella vita privata delle persone, nonché sempre più veloce la possibile diffusione delle notizie. La raccomandazione della Corte è quindi quella di non tergiversare riguardo alla stesura di leggi, sia in ambito pubblico che privato, per regolare la società dell'informazione che si andava creando.

3.2 Dalla legge 675/96 al GDPR

Purtroppo però il legislatore italiano parve fare orecchie da mercante alle raccomandazioni della Cassazione riguardanti il pronto intervento normativo sul diritto alla privacy. Questo in realtà non va imputato solo all'indolenza del Parlamento, ma anche alla ferma opposizione esercitata da svariate associazioni di categoria, dalla rappresentanza delle compagnie di assicurazioni fino a Confindustria, che avevano impedito nel 1984 l'approvazione della proposta di legge nota come Mirabelli. In conclusione, il Bel Paese dovette aspettare fino al 1996 per vedere approvata una – pur frettolosa – legge riguardante la privacy.

È necessario aggiungere che non si trattava di un'iniziativa autonoma del Parlamento italiano, quanto piuttosto dell'attuazione della direttiva 95/46/CE imposta dalla Comunità Europea, della quale si è già parlato nel primo capitolo. Per la precisione, l'Italia, dopo numerosi dibattiti, fu l'ultimo dei destinatari ad approvare la legge di recepimento, che infatti giunse l'ultimo giorno disponibile previsto dalla direttiva, il 31 dicembre 1995.

Il lungo e penoso iter sopra descritto fa comprendere come la strada per raggiungere una normazione compiuta riguardante la privatezza fosse ancora lunga. Inoltre, il fatto che l'atto europeo fosse una direttiva, vincolante solo negli obiettivi, rende ancora più chiaro il motivo delle disposizioni caotiche e frettolose contenute nella legge 675/96. Non a caso insieme a questa fu promulgata la gemella legge 676/96, contenente una delega di 18 mesi durante i quali il Governo avrebbe potuto emanare decreti correttivi o integrativi per completare il quadro. Fra questi, alcuni

[75] Cass, sent. del 27 maggio 1975 n. 2129

dei più importanti furono la riduzione delle categorie di soggetti, che dovevano notificare il trattamento e l'ulteriore estensione della delega a 24 mesi.

Fra l'approvazione della legge 675/96 e il successivo passo europeo, in Italia molto si deve all'autorità Garante, il cui primo presidente fu Stefano Rodotà. Rendendosi conto della mancanza di uno standard minimo di sicurezza previsto dalla legge, questi attivò una Commissione formata da esperti in materia, con il compito di redigere una bozza di decreto per il Presidente della Repubblica. Questo regolamento, emanato nel 1999, comprendeva fra le altre cose una differenziazione delle disposizioni in base al supporto di conservazione utilizzato e l'introduzione dell'amministratore di sistema, personaggio assimilabile al DPO.

La storia legislativa italiana continua così, fra incertezze e ulteriori decreti, fino al 2003, anno in cui ci si rende conto che il quadro normativo è troppo caotico, essendo articolato in direttive disgiunte fra loro e spesso contraddittorie. È quindi giunto il momento di riunire ed aggiornare tutte le disposizioni in materia di protezione dei dati personali in un unico testo: nasce così con il decreto legislativo n. 196 del 30 giugno 2003 il Codice in materia di protezione dei dati personali, che fa riferimento anche alle ulteriori direttive emanate dall'Unione europea fra il 1996 e il 2003 appunto. A questo testo si affiancano inoltre alcuni codici deontologici riguardanti categorie particolari di trattamento, che non saranno del tutto estranee al lettore: il trattamento in ambito giornalistico, per scopi storici o ancora il trattamento di dati da parte di agenzie nazionali a scopo di ricerca storica o statistica.

Per alcuni anni questo testo unico sembra risolvere la maggior parte dei problemi, salvo alcune leggi specifiche riguardanti settori particolari, come la protezione della posta elettronica o il Provvedimento in materia di videosorveglianza. La rottura arriva nel 2012, con l'approvazione da parte del Governo del decreto legge n. 5, datato 9 febbraio, intitolato "Disposizioni urgenti in materia di semplificazione e di sviluppo". Questo documento, adottato tra l'altro senza consultare il Garante, si limita ad eliminare parte delle disposizioni precedenti, senza però snellire di fatto i procedimenti.

Le vicende continuano fra successivi decreti e leggi di attuazione delle direttive europee fino appunto all'approvazione da parte dell'Unione del primo regolamento in materia, che "assolve" quindi il legislatore statale dal compito di stesura delle norme, fornendo, come si è già considerato, una regolamentazione unitaria e coerente nel quadro della privacy.

3.3 Come funziona in pratica?

Sebbene le norme del regolamento siano identiche per tutti gli Stati membri, resta comunque un certo margine di discrezionalità in capo agli Stati riguardo alle norme di applicazione o agli

strumenti messi a disposizione per adempiere alle disposizioni del GDPR. In questo paragrafo si analizzano quindi le soluzioni esecutive messe in atto a livello italiano a riguardo di due adempimenti: la scelta del DPO e la stesura della DPIA – Privacy Impact Assestment.

3.3.1 Chi può fare il DPO in Italia?

Si è già parlato della possibilità di formare associazioni di categoria per quanto riguarda la figura del responsabile della protezione dei dati. Si è già anche detto che per il momento l'unico "albo" esistente è quello dei DPO delle istituzioni e degli organismi europei, mentre a livello nazionale per ora non esiste nulla di equivalente.

Esiste per sempre un organismo di certificazione della professionalità di queste figure. In Italia infatti tutti i DPO debbono essere registrati presso l'autorità Garante, la quale stabilisce anche il livello di competenze che questa personalità deve presentare in modo più preciso di quanto facciano le indicazioni generali del GDPR.

Ad esempio, esistono svariate associazioni presso cui il DPO può ottenere un certificato che attesti la sua formazione professionale. Questo è un modo piuttosto semplice per dimostrare le proprie competenze, ma non è obbligatorio. Può infatti essere richiesto un titolo di studio minimo di livello, compensabile anche attraverso l'anzianità di lavoro oppure tramite un percorso formativo specifico, la cui durata si aggira intorno alle 90 ore.

In Italia esiste anche la figura del *security manager*, definita dalla norma UNI 10459, che delinea il profilo di un professionista della sicurezza in svariati campi, nei quali si può introdurre anche quello della protezione dei dati personali. Questo professionista sarebbe in grado di gestire il processo di garanzia della sicurezza dall'inizio alla fine, sia in ambiti "ortodossi" come quello degli istituti di vigilanza, sia, con un'adeguata formazione settoriale, in quello più "virtuale" della protezione dei dati.

Sappiamo inoltre che il DPO può essere una figura sia esterna che interna. Ma qual è la soluzione prediletta in Italia? Di fatto raramente ci si imbatte in un responsabile esterno, per il semplice motivo che la protezione dei dati comporta da un lato grandi responsabilità per il *data protection officer* stesso e dall'altro oneri economici in capo ai titolari. Tendenzialmente sono le imprese più grandi a scegliere un costo più alto a fronte di una delega di responsabilità a terzi. Per i motivi opposti invece il "sottobosco" di PMI da cui è composta per gran parte l'economia italiana preferisce nominare un DPO interno per ovviare ai problemi di reperibilità ed abbattere i costi.

3.3.2 Cos'è il DPIA?

DPIA è l'acronimo di *Data Protection Impact Assestment*: si tratta di un documento di valutazione dei rischi del tutto simile a quello richiesto per la valutazione della sicurezza sui luoghi di lavoro:

si può dire che valuti la sicurezza negli ambienti (fisici o virtuali) di conservazione e trattamento dei dati.

Questa valutazione d'impatto non è sempre richiesta, anzi l'art. 35 del GDPR stabilisce che essa sia necessaria solo quando il trattamento, per il suo oggetto e le sue finalità, presenta rischi specifici per i diritti e le libertà delle persone fisiche. Per chiarezza, la disposizione riporta anche un elenco dei casi in cui questo documento è obbligatoriamente richiesto, e cioè per il trattamento dei dati particolari e dei dati giudiziari, per la sorveglianza su vasta scala di zone accessibili al pubblico (videosorveglianza) e per trattamenti che richiedono un monitoraggio sistematico e globale di informazioni, svolto in modo automatizzato, come nel caso della profilazione.

Nel quarto comma dell'articolo riguardante la DPIA è però previsto che ciascuna autorità nazionale rediga una lista delle attività soggette a questo adempimento, per poi inoltrarla al Comitato europeo per la protezione dei dati, così come può elencare tutte le attività esonerate.

Il Garante italiano non si è certo sottratto al compito: la sua lista è stata presentata al Comitato, il quale ha consigliato ulteriori precisazioni. Il Garante si è quindi uniformato maggiormente alle indicazioni dell'art. 29 Working Party, inserendo nella lista, oltre alle fattispecie già menzionate, le attività predittive e di profilazione, i trattamenti automatizzati volti ad assumere decisioni con effetti giuridici sull'individuo (ad esempio per inserire gli interessati nelle categorie di merito delle assicurazioni), i trattamenti nell'ambito lavorativo tramite i quali i dipendenti sono controllati a distanza, trattamenti duraturi di interessati "vulnerabili" (minori, anziani, disabili, richiedenti asilo o persone affette da infermità mentali) e svariate altre categorie.

In merito alla stesura del documento vero e proprio, anche qui i meccanismi di ausilio forniti dai diversi Paesi sono diversi fra loro. Ad esempio l'autorità Garante francese, incarnata dal CNIL, offre la propria assistenza diretta nella stesura del documento, mentre in Italia esistono solo delle indicazioni e dei modelli replicabili, forniti dal Garante. Di fatto per le imprese è quindi più semplice affidarsi a dei consulenti esterni o anche a programmi specifici a pagamento, per farsi assistere nella stesura di questo documento. Invito il lettore a considerare questo aspetto nel proseguimento della lettura, in quanto sarà ripreso più approfonditamente nei prossimi paragrafi.

3.4 Alcuni casi specifici

Passiamo ora ad analizzare due aspetti di applicazione del GDPR, che per forza di cose devono essere demandati agli Stati per la loro applicazione: il primo è il trattamento dei minori, per il quale il GDPR stesso prevede che ogni Stato detti le proprie regole; mentre il secondo è l'ambito sanitario, specie alla luce della recente emergenza legata al Coronavirus. L'obiettivo di questo paragrafo è quindi quello di capire tutte le complessità e le sfaccettature in cui ci si imbatte quando

si tratta di applicare una normativa generale, seppur molto chiara, ad una moltitudine di casi singolari e particolari.

3.4.1 Il consenso dei minori in Italia

Si è già accennato al capitolo 8 del GDPR[76], che contiene le regole generali per la prestazione del consenso di un minore. Il legislatore europeo ha stabilito l'età minima per il trattamento a 16 anni, lasciando agli Stati la possibilità di fissare altri parametri, purché non inferiori ai 13 anni di età. Questa soglia non è casuale, in quanto la maggior parte dei *social network*, a cui si riferisce l'articolo, pone come età minima per l'iscrizione proprio i 13 anni. Il motivo è che la maggior parte delle aziende informatiche che li gestiscono sono basate negli Stati Uniti, dove il *Children's Online Privacy Protection Act* del 1998 stabilisce che le uniche persone giuridiche a poter raccogliere dati di minori al di sotto dei 13 anni sono gli enti pubblici.

Con l'entrata in vigore del GDPR, l'Italia ha deciso di ricalcare nella normativa sulla privacy l'impostazione dello stato giuridico dei minorenni, fissando quindi l'età minima per dare il consenso al trattamento dei propri dati a 14 anni, ovvero un limite fra i più bassi d'Europa.

Si tratta dell'età minima per prestare il consenso al trattamento dei propri dati, per cui incide solo sulla gestione della privacy in capo ai *social* e ai servizi di messaggistica, ma non ha a che fare coi contratti veri e propri firmati per l'iscrizione a questi servizi. Comunque, poiché è il minore stesso ad usufruire in prima persona di questi servizi, sopra i 14 anni non ha bisogno del consenso dei genitori o di chi detiene la patria potestà. Sotto ai 14 anni invece naturalmente è necessaria la prestazione del consenso dei genitori o dei tutori del minorenne affinché i suoi dati possano essere trattati.

---

[76] « *1. Qualora si applichi l'articolo 6, paragrafo 1, lettera a), per quanto riguarda l'offerta diretta di servizi della società dell'informazione ai minori, il trattamento di dati personali del minore è lecito ove il minore abbia almeno 16 anni. Ove il minore abbia un'età inferiore ai 16 anni, tale trattamento è lecito soltanto se e nella misura in cui tale consenso è prestato o autorizzato dal titolare della responsabilità genitoriale.*
2. Gli Stati membri possono stabilire per legge un'età inferiore a tali fini purché non inferiore ai 13 anni. Il titolare del trattamento si adopera in ogni modo ragionevole per verificare in tali casi che il consenso sia prestato o autorizzato dal titolare della responsabilità genitoriale sul minore, in considerazione delle tecnologie disponibili.
3. Il paragrafo 1 non pregiudica le disposizioni generali del diritto dei contratti degli Stati membri, quali le norme sulla validità, la formazione o l'efficacia di un contratto rispetto a un minore.»
(PARLAMENTO E CONSIGLIO EUROPEO, *Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*, 27 aprile 2016, capo II, art. 8 - *Condizioni applicabili al consenso dei minori in relazione ai servizi della società dell'informazione*)

Va anche notato che il legislatore italiano ha previsto l'obbligo di notifica del trattamento al Garante, per i trattamenti basati su interessi legittimi, solo quando il trattamento è funzionale al cambio del nome o del cognome del minorenne.

Cosa succede invece quando si tratta di utilizzare foto di minori per pubblicarle online? In questo caso la giurisprudenza italiana, rifacendosi all'art. 10 del Codice Civile, ha stabilito che sia sempre necessario il consenso di entrambi i genitori per diffondere foto di minori sui social, pena l'entrare in conflitto con il Codice Privacy del 2003 nonché con la Convenzione di New York sui diritti del fanciullo del 1989. In pratica la diffusione di fotografie di minorenni su piattaforme pubbliche viene equiparata alla diffusione di dati particolari (generalmente vietata tranne deroghe) anziché rientrare nel trattamento di dati personali comuni come nel caso degli adulti.

3.4.1 Il trattamento dei dati in ambito sanitario

Il termine "trattamento dei dati in ambito sanitario" in realtà configura una realtà molto più ampia di quella che ci si potrebbe aspettare. Infatti non sono solo medici ed ospedali a trattare dati particolari, ma anche palestre, estetisti e svariate altre categorie. Il lettore capirà da solo che il personale amministrativo di un ospedale non è numericamente assimilabile a quello di un centro estetico, eppure gli adempimenti previsti dalla normativa sono esattamente gli stessi, in quanto questi sono suddivisi in base alle categorie di dati che si trattano, non in base al personale o alla quantità di dati trattati.

Un altro problema riguarda l'obbligo di riservatezza, a cui sono sottoposti tutti coloro i quali vengono in contatto con i dati sanitari (titolari, responsabili, addetti, …). Infatti nel caso dei medici, essi sono vincolati a questo obbligo in virtù della loro stessa formazione professionale, mentre per quanto riguarda il personale di una palestra o di una piscina normalmente non sarebbe ragionevolmente richiesto. La soluzione generalmente consiste nella firma di una scrittura privata in cui si attesta di sottoporsi all'obbligo di riservatezza, persistente anche dopo la cessazione del trattamento o del rapporto lavorativo presso il titolare.

Fra i campi in cui le norme sulla privacy stesse sembrano confliggere fra loro troviamo anche la medicina del lavoro. È noto infatti che il datore di lavoro debba periodicamente far sottoporre i propri dipendenti ad una visita di idoneità da parte del medico del lavoro specializzato. Poiché il datore di lavoro non rientra nelle deroghe al divieto di trattamento dei dati sanitari all'articolo 9, egli non può ricevere informazioni sulle condizioni di salute dei propri dipendenti. Infatti, la cartella clinica di ciascun lavoratore è sigillata e custodita dal medico del lavoro, il quale è l'unico oltre all'interessato che può visionarla. Per ovviare a questo conflitto, il medico comunica al datore di lavoro solo un giudizio circa l'idoneità, l'idoneità parziale o la non idoneità alle

mansioni che il dipendente svolge durante l'orario di lavoro, insieme alle indicazioni riguardo a quali compiti debba evitare.

Infine, alla luce della recente emergenza sanitaria dovuta al Covid 19 si è potuto toccare con mano come possa cambiare l'applicazione della normativa europea sulla privacy in casi in cui prevalga l'interesse verso la salute pubblica rispetto alla protezione delle informazioni. Infatti, nel soppesare i due diritti, il legislatore ha saggiamente deciso di privilegiare il primo, per cui c'è stato un "rilassamento autorizzato" delle regole sulla privacy a favore dell'interesse pubblico. Ciononostante, questa deroga non è certo assoluta. Riprendiamo ad esempio lo scenario del luogo di lavoro. Durante le fasi più critiche dell'emergenza, il datore di lavoro era obbligato a misurare la temperatura dei dipendenti per accertare che non avessero la febbre e mandare a casa gli individui che presentassero una temperatura maggiore a 37.5°.[77] Come ben sappiamo, il datore di lavoro in teoria non potrebbe conoscere i dati sanitari dei propri dipendenti, ed inoltre il trattare tali dati comporta tutta una serie di adempimenti, come la nomina di un DPO. Come ovviare a questa situazione? Nel primo caso non sembra esserci soluzione ragionevolmente praticabile: con i medici già oberati di lavoro non è certo possibile chiamare uno specialista per realizzare le rilevazioni ogni giorno, perciò in nome dell'emergenza è più ragionevole che sia il datore a farsi carico di questo adempimento. Per quanto riguarda la conservazione dei dati sanitari, non potendo dotare tempestivamente ogni azienda e impresa di un DPO, la soluzione è stata molto semplice: è sufficiente infatti non conservare i dati riguardanti la temperatura corporea, perché non si parli più di trattamento, ricadendo quindi al di fuori dell'ambito di applicazione del GDPR.

Il lettore comprenderà quindi perché la tutela dei dati personali non possa mai ragionevolmente essere un diritto assoluto, sebbene negli ultimi anni la tendenza sia stata sempre più inclusiva ed estensiva. Al momento dell'applicazione pratica diventa talvolta piuttosto difficile conciliare la protezione del singolo con l'interesse pubblico, per cui non è infrequente l'imbattersi in espedienti, talvolta macchinosi, per trovare un punto di contatto fra le due cose. Per questo motivo è sempre utile tenere a mente il ruolo della giurisprudenza, preziosa per comprendere le implicazioni giuridiche nei casi pratici e specifici, nonché del potere esecutivo, a cui spetta il non sempre grato compito di conciliare una normazione astrattamente perfetta con una realtà inevitabilmente imperfetta e sfaccettata.

[77] Oggi il datore di lavoro non è più obbligato, ma può comunque misurare la temperatura ai dipendenti se lo ritiene opportuno.

3.5 Piccoli professionisti e PMI

Come il lettore avrà ormai già capito a questo punto della lettura, il GDPR non è un fatto meramente normativo, relegato agli studi legali, ma investe la realtà quotidiana virtualmente di chiunque, sia in veste di interessato "passivo", sia nel caso di tutte le figure "attive" nel trattamento di dati altrui.

Trasportando il discorso nel contesto italiano, la prima cosa da notare è che nel nostro Paese la maggior parte della produzione è concentrata nelle mani di piccole e medie imprese, che arrivano a generare fino all'83% della produzione di alcune regioni. Nel nostro paesaggio economico non sono perciò le grandi imprese a farla da padrone, men che meno le grandi imprese informatiche, bensì aziende che occupano meno di 250 persone, oppure addirittura artigiani autonomi e liberi professionisti.

Incrociando questi dati con il basso livello di digitalizzazione del lavoro riscontrabile oggi in Italia, rispetto alla media europea, non è difficile rendersi conto delle perplessità di molti imprenditori e liberi professionisti riguardo all'implementazione delle nuove norme sulla sicurezza dei dati.

Eppure gli adempimenti previsti dal regolamento europeo non sono differenziati in base alle dimensioni dell'azienda, né in base al settore in cui è attiva. L'unica discriminante è il tipo di dato che viene trattato e per quale finalità. Di fatto quindi gli stessi adempimenti potrebbero sorgere in capo a società che contano migliaia di dipendenti, con fatturati importanti e che quindi verosimilmente sono in condizione di dotarsi di tutta la consulenza legale e tecnica necessaria, sia in capo a piccole realtà a conduzione familiare, senza studi legali né consulenti alle spalle.

Per comprendere meglio le difficoltà a cui potrebbe andare incontro il settore delle piccole e medie imprese in Italia, ho svolto alcune "interviste" presso un'associazione che riunisce agenzie di consulenza nel campo della sicurezza localizzate in tutta Italia. Il contenuto integrale dell'intervista si troverà in un allegato, unito a questo documento, mentre il sunto generale sarà inserito nel prossimo paragrafo.

3.5.1 Novità giuridiche: la responsabilità dell'"onere della prova"

Uno dei grandi cambiamenti introdotti in Italia dall'adeguamento del regolamento europeo riguarda il meccanismo di controllo e supervisione da parte delle autorità sulle aziende che trattano dati. Mi si perdonerà l'aver preso a prestito il termine "onere della prova" dal linguaggio giuridico, sebbene non sia esplicitamente presente nel regolamento o nella legge di adeguamento, in quanto piuttosto adatto a sintetizzare il concetto.

In questo caso per "onere della prova" si intende la responsabilità di dimostrare la regolarità o meno del trattamento in corso, per determinare se vi sia stata un'infrazione delle leggi. Prima dell'avvento del GDPR, questo onere spettava all'autorità giudiziaria, istruita riguardo alle ispezioni di volta in volta dall'autorità Garante o dalla magistratura. Va da sé che tendenzialmente il Garante si occupa della fase di controllo generale, ma può anche agire su segnalazione. Se l'infrazione ha natura di reato, naturalmente è più indicato che sia la magistratura ad avviare i controlli.

Con la legge di adeguamento del GDPR invece avviene il contrario: è il titolare, in fase di ispezione, a dover produrre tutte le prove riguardanti la regolarità del trattamento in atto. Si tratta quindi di esibire tutti i documenti, quali la DPIA ed il registro del trattamento, nonché di mostrare i supporti sui cui sono conservati i dati ed illustrare le strategie di protezione messe in atto. In pratica, prima del 2018 era l'autorità giudiziaria a dover dimostrare la presenza di irregolarità, mentre oggi è il titolare a dover provare di non aver commesso alcuna deviazione dal codice.

Si tratta quindi di una responsabilità che ricade ancora una volta sui titolari, vale a dire spesso e volentieri sui datori di lavoro. Mi sembra a questo punto doverosa una considerazione riguardo all'effettiva funzionalità di questo metodo: come lo stesso GDPR prevede, il titolare non necessita di avere conoscenze specifiche in materia di conservazione e protezione dei dati personali. Come può quindi interfacciarsi efficacemente con l'autorità, se egli stesso non conosce a fondo la materia? Naturalmente entra in gioco l'assistenza del responsabile del trattamento, ma l'interazione rischia di essere più caotica del dovuto.

Svariate perplessità sono state dettate anche dal fatto che l'autorità giudiziaria preposta ai controlli sul rispetto della privacy in Italia sia la Guardia di Finanza. Questo corpo non dispone però di un nucleo speciale istruito *ad hoc*, mentre altri corpi, come ad esempio la Polizia postale. Ci si chiede quindi se anche da parte del "controllore" sia presente un'adeguata formazione specifica.

Poiché il GDPR è attivo dal 2018, in soli due anni non si è ancora potuta constatare l'effettiva efficacia di questo dispositivo di controllo, in quanto non si sono verificate ispezioni di larga scala che permettessero di testare realmente questo metodo "sul campo". L'auspicio è che alla prova dei fatti si riveli adatto ad individuare le irregolarità gravi, senza ingarbugliarsi nei cavilli procedurali, diventando quindi un efficace strumento di protezione degli interessati e non l'ennesima imposizione burocratica sulle imprese.

3.5.2 Come fare formazione: intervista ai diretti interessati

Una delle soluzioni più comuni, per le piccole e medie imprese alle quali è richiesto l'adeguamento al GDPR, è quella di affidarsi ad agenzie di consulenza per ricevere le

certificazioni necessarie, come ad esempio quella di DPO, nonché per la stesura di documenti quali la PIA o il registro del trattamento.

Una di queste associazioni di consulenza è A.N.C.O.R.S[78], presso la cui sede piemontese ho potuto svolgere una piccola ricerca sul campo, per capire quali sono le maggiori difficoltà che incontrano i piccoli imprenditori nell'adempiere agli adeguamenti richiesti dalla normativa europea.

Il primo aspetto che è emerso nel corso dei colloqui riguarda lo scoglio rappresentato dal fatto che molti piccoli imprenditori non comprendono il motivo per cui rientrano nel campo di applicazione del GDPR. In effetti vanno considerati due aspetti: molti piccoli imprenditori, per una questione puramente generazionale, non sono familiari con l'uso delle nuove tecnologie, né tantomeno molte delle conoscenze richieste dagli adempimenti, anche se si tratta semplicemente di aprire un account di posta elettronica. Questo non dovrebbe stupire, considerato che, secondo gli archivi ISTAT, in Italia più di un terzo della popolazione non possiede nemmeno un computer. L'altra considerazione è che non sempre risulta immediato il motivo per cui dovrebbero occuparsi di protezione dei dati. In effetti, è palese che un'azienda che fa profilazione debba tutelare la privacy degli interessati, ma perché un'impresa di pulizie dovrebbe avere a che fare con questo settore? In realtà, anche quando l'attività principale non rientra nel trattamento di informazioni personali, ogni datore di lavoro raccoglie almeno i dati dei propri dipendenti, per cui secondo le regole europee deve conformarsi al GDPR.

Molte delle perplessità degli impresari riguardano naturalmente i costi. Quello che spesso non viene specificato è che la preoccupazione non riguarda tanto i costi diretti, ad esempio pagare un consulente affinché eroghi i corsi di formazione, quanto piuttosto i costi opportunità derivanti dal tempo che impiegato nella burocrazia, anziché nell'attività produttiva. Ad esempio, il corso di formazione per il DPO interno dura all'incirca 40 ore, il che corrisponde a cinque giornate di lavoro di un dipendente a tempo pieno. Privarsi di un dipendente per cinque giorni corrisponde quindi ad una perdita economica per il datore di lavoro. Nelle grandi imprese invece questi tempi non comportano un problema, in quanto la scelta più comune è quella di pagare un soggetto esterno affinché svolga la mansione di responsabile della protezione dei dati.

Emerge quindi una problematica di fondo, a cui sono riconducibili tutte queste considerazioni: manca una differenziazione dei doveri in base alle dimensioni ed ai servizi offerti dall'azienda. La sola discriminazione in base ai dati trattati non permette di creare impostazioni sufficientemente funzionali a garantire un'adeguata protezione unita allo snellimento delle

[78] Acronimo per "Associazione Nazionale Consulenti e Responsabili della Sicurezza", un'associazione abilitata a livello nazionale che rappresenta gli operatori italiani nel settore della sicurezza sul lavoro.

procedure richieste agli imprenditori. Alla domanda riguardante le possibili soluzioni, le risposte sono varie. Per prima cosa si evidenzia la necessità di includere gli operatori del settore nella stesura delle norme, ma la discussione verte soprattutto sulla necessità di differenziare le aziende: c'è chi propone in base alle dimensioni, mentre altri aggiungono una divisione settoriale in base ai codici ATECO[79]. Si potrebbe quindi adottare un approccio simile a quello della famigerata "legge 81"[80] in materia di sicurezza sui luoghi di lavoro, dove si considerano i rischi specifici di ogni azienda per poi determinare una linea di condotta da seguire. Uno dei formatori considera: «Lo scopo di base della normativa europea era mettere un freno allo strapotere delle grandi aziende informatiche e dei *social network*, come Google e Facebook, costringendoli a rispettare una normativa *ad hoc* per l'Europa. Questo obiettivo si è però realizzato a scapito delle piccole realtà, le quali hanno gli stessi adempimenti, pur rappresentando in maniera infinitesimale rispetto alle grandi aziende un rischio per la privacy degli individui.»

[79] Il codice ATECO è una combinazione alfanumerica che identifica le attività economiche, individuandone il settore economico e le caratteristiche specifiche. È utilizzato dalle agenzie statali a scopo statistico, ma anche di esazione fiscale e contributiva.
[80] Con questa espressione si identifica il d.lgs n. 81 del 9 aprile 2008, intitolato "*Testo unico sulla salute e sicurezza sul lavoro"* che ad oggi rimane il testo di riferimento per gli adempimenti in materia di sicurezza dei lavoratori.

CONCLUSIONI

Giunti alla fine della trattazione sembra quantomeno necessaria una ricapitolazione di quanto detto e trattato, insieme all'esposizione delle conclusioni a cui si può giungere sulla base delle informazioni ricevute.

La prima domanda a cui è necessario rispondere, per poter comprendere tutto il resto, è che cosa sia il diritto alla privacy. La prima definizione che si incontra è l'ormai famosa "*the right to be let alone*" ovvero il diritto ad "essere lasciati in pace" di Warren e Brandeis. Se questa poteva essere una nozione piuttosto accurata per il 1890, quando gli attentati alla sfera privata dell'individuo potevano verosimilmente provenire dalla stampa, dalla concorrenza (nel caso della reputazione o dell'immagine) o dai pubblici poteri, è chiaro che adesso non può più essere sufficiente. Infatti prima dell'invenzione del computer, ogni attacco alla propria privacy era compiuto plausibilmente da altre persone o gruppi. Oggi invece la vera minaccia, o quantomeno la più sentita, arriva da servizi elettronici ed informatici, come i *social network* o gli *online stores*, ovvero automazioni che agiscono in un ambiente virtuale e non fisico, per cui sono più difficili da rintracciare.

Inoltre ormai "essere lasciati in pace" non può più essere la base del diritto alla privacy, perché nella società dell'informazione non si dà più solo il caso in cui esiste una sfera privata, protetta e "statica", verso la quale si dirige l'intrusione. Spesso e volentieri oggi è il singolo che decide di "aprire" la sua sfera personale verso l'esterno, condividendo delle informazioni, come nel caso dei *social network*. Cosa rimane a tutela di questi dati, se il diritto alla privacy è percepito solo come una difesa dalle invasioni esterne? Per questo motivo la tendenza uniforme nelle legislazioni è stata quella di allargare l'ambito di applicazione di questa fattispecie, per arrivare a proteggere uno spazio sempre più ampio dell'azione dell'individuo.

Sempre per questi motivi, è ragionevole concludere che il diritto, di fronte al quale ci troviamo, non sia più una libertà negativa, ma sia divenuto ormai un diritto positivo. Se nel XIX e all'inizio del XX secolo ci si poteva accontentare di uno Stato che non si intromettesse senza ragionevoli motivazioni nella propria intimità, con l'avvento dapprima della stampa di massa e dopo di internet è chiaro che in capo allo Stato sorga una responsabilità ben maggiore. A mano a mano che ci si avvicina alla contemporaneità il legislatore attribuisce tutele crescenti all'individuo, che corrispondono ad eguali garanzie da parte del potere centrale: non solo lo Stato stesso deve dare prova di rispettare la privacy degli individui (basti pensare al Privacy Act statunitense, che permette ai cittadini di esercitare autonomamente i propri diritti nei confronti delle agenzie pubbliche) ma deve farsi carico attivamente della protezione della personalità del singolo anche nei confronti di terzi, sia normativa che concreta.

L'ultima domanda da porsi circa la natura del diritto alla privacy è se sia un diritto assoluto o meno. La risposta che emerge è chiaramente positiva: come ogni altro diritto della personalità, il diritto alla privacy è assoluto, ovvero si può far valere nei confronti di chiunque, che questi sia volente o nolente. L'individuo ha diritto alla privacy in quanto tale e dal momento della sua stessa nascita. Chiunque altro ha semplicemente il dovere passivo di non turbarne il godimento. Ciò non significa però che il diritto alla privacy possa imporsi sui diritti altrui o sugli interessi pubblici: si è sottolineato più e più volte come la libertà di informazione o l'interesse pubblico possano ragionevolmente prevalere sulla volontà di un individuo di mantenere il segreto sui propri dati. In questo senso si può quindi affermare che la privatezza sia un diritto "limitato" nella sua assolutezza: esso si arresta sempre al sopraggiungere di interessi altrettanto fondamentali degli altri individui.

Naturalmente i percorsi seguiti dalle varie culture per giungere al riconoscimento del diritto alla privacy sono stati diversi e spesso divergenti, sebbene ad oggi si possa affermare che le conclusioni a cui hanno portato siano uniformi. In molti casi anche gli impulsi sono stati i medesimi, primo fra tutti il ruolo fondamentale giocato dalla stampa, sia scandalistica che investigativa. Secondo questo aspetto, le due sponde dell'Atlantico ravvisano una forte somiglianza: dalle infedeltà della moglie di Brandeis, ai pettegolezzi riguardanti l'ex imperatrice iraniana Soraya fino allo scandalo francese di Safari, il programma segreto denunciato dal quotidiano Le Monde.

Il lettore potrà anche notare che, trattandosi di un diritto di nuova generazione, non frutto di consuetudini molto antiche, le pratiche della common law e della civil law in certi casi sembrano mescolarsi, come se gli ordinamenti "prendessero a prestito" l'uno elementi dell'altro. È ad esempio il caso dell'avventura americana di William Prosser, il quale pur partendo dalla giurisprudenza per sintetizzare le proprie quattro fattispecie, finisce per fossilizzarle in nome della certezza del diritto, anteponendo quindi la definizione alla realtà, che risulta assai più variegata di quattro semplici categorie. All'inverso, nel caso italiano è stato un ordinamento dove vige da sempre il primato della legge scritta a seguire un percorso "anglosassone": i primi impulsi verso il riconoscimento del diritto alla privacy in Italia arrivano infatti dalle aule di tribunale, peraltro con largo anticipo anche rispetto ai primi Paesi europei a dotarsi di una legislazione in materia. L'iter però si è arrestato, come già sappiamo, alle soglie del Parlamento per molti anni, fino all'intervento dell'Unione europea.

Infatti, si può affermare che ci sia stato una decisa accelerazione del processo di riconoscimento del diritto alla privacy con l'entrata in gioco dell'Unione europea. Questa ha fatto da sempre del rispetto dei diritti umani e della personalità la propria bandiera, sia attraverso processi autonomi che tramite la volontà di sottoporsi ai Trattati internazionali in materia, come ad esempio la

CEDU. Proprio analizzando questa fonte, che è quella cronologicamente più antica, si noterà l'influenza dell'esperienza dei totalitarismi europei e la volontà di arginare normativamente il controllo capillare che questi avevano esercitato sui propri cittadini. La stessa tensione si ritrova nel Bundesdatenschutzgesetz che, sebbene di quasi tre decenni più giovane della CEDU, proviene dalla Germania, unica nazione occidentale a subire il giogo di uno Stato di polizia, dove la violazione del segreto della corrispondenza e delle comunicazioni era all'ordine del giorno.

Spingendosi avanti nel tempo, le norme diventano sempre meno "di principio" e sempre più "di dettaglio", questo perché ormai l'esistenza di un diritto alla privacy è un fatto assodato nella cultura giuridica occidentale, mentre iniziano a rendersi necessarie normative specifiche adatte a casistiche particolari. Inoltre, con la nascita di internet nel 1972 e il lancio sul mercato del primo *personal computer* nel 1975[81], ha inizio l'era digitale. Lo sviluppo delle strumentazioni elettroniche è sempre più veloce, mentre i prodotti diventano sempre più fruibili dal grande pubblico. La rete, poi, permette movimenti di moli di informazioni prima impensabili in tempo reale, per cui i legislatori non possono più posporre l'emanazione di norme specifiche in materia di protezione dei dati personali. Nel caso che qui si analizza, l'Unione europea prende finalmente le redini della situazione nel 1996, emanando l'ormai nota direttiva 95/46/CE "relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati". Come il lettore già sa, la direttiva per sua stessa natura vincola solo negli obiettivi, perciò viene recepita con leggi diverse per ogni Stato. Questo porta ad una situazione di incertezza normativa: per fare l'esempio dell'Italia, la legge di recepimento è stata integrata con continui decreti per i successivi diciotto anni, fino al 2014.

Questo ci porta al 2016, anno in cui viene emanato il nuovo Regolamento europeo sulla protezione dei dati. Trattandosi appunto di un regolamento, il GDPR va applicato uniformemente su tutto il territorio dell'unione, ponendo fine alla situazione di caos che si era creata negli ulti vent'anni. Sotto molti aspetti, si tratta di un documento rivoluzionario, sia nella classificazione dei dati, sia nell'imposizione di doveri, sia nel riconoscimento dei diritti.

Per comprendere il regolamento 2016/679, per prima cosa è necessario avere chiara la suddivisione dei dati, in quanto su questa distinzione poggia gran parte dell'architettura del regolamento. Infatti, in base al tipo di dato che ci si trova davanti, si hanno regole, figure professionali e diritti completamente diversi.

La categoria più comune e quindi sottoposta a minori regolamentazioni, è quella appunto dei dati personali comuni. Si tratta di dati come il nome, il cognome, l'indirizzo eccetera, attraverso i quali

[81] Si tratta di Altair 8080, il primo "minicomputer" accessibile anche ai singoli ad avere un successo commerciale di massa, messo in commercio dalla società americana MITS.

si può risalire ad una persona fisica identificata o identificabile. È naturale che in gran parte delle transazioni che avvengono nella vita quotidiana di ognuno di noi, questi dati ci vengano richiesti. Per questo motivo il legislatore prevede che, qualora vi sia la necessità di registrarli per un trattamento, gli unici requisiti richiesti sono quelli circa la regolarità del trattamento, che deve essere quindi lecito. Sarà cura del titolare richiedere solo i dati strettamente necessari ai propri scopi. A loro volta, questi scopi devono essere chiaramente esplicitati, per evitare che, una volta in possesso dei dati, il titolare possa usarli per i propri scopi o a fini di lucro ulteriore. È naturale quindi che, essendo l'interessato il primo "controllore", egli debba essere chiaramente informato su tutti questi aspetti, e che solo dopo aver compreso tutto dia il proprio consenso esplicito.

L'impostazione cambia completamente quando invece si parla dei cosiddetti dati particolari[82], definizione che di fatto racchiude due macro categorie: da un lato tutti i dati relativi alla personalità dell'individuo (provenienza etnica, orientamento sessuale, politico, religioso o sindacale, opinioni filosofiche, …) e dall'altro quelli riguardanti la sua salute (dati biometrici, genetici, analisi del sangue, …). Secondo il legislatore europeo, non è mai lecito trattare questi dati, tranne in alcune situazioni previste dal regolamento stesso. La situazione è quindi rovesciata: sussiste un divieto universale di trattamento di questi dati a cui sono poste alcune ragionevoli deroghe, ad esempio per la protezione della salute pubblica in caso di epidemie, che è venuta in rilievo proprio in quest'ultimo periodo a causa del coronavirus. Non solo cambia l'impostazione giuridica, ma sono richieste anche figure professionali diverse nel caso dei dati particolari. Infatti, se per il trattamento di dati personali comuni sarebbero sufficienti un titolare a cui è attribuito il trattamento ed un responsabile del trattamento con competenze tecniche adeguate, coadiuvato in caso di necessità dagli addetti, per quanto riguarda i dati particolari è necessaria una figura nuova, istituita dal GDPR. Si tratta del responsabile della protezione dei dati, il quale, in posizione di totale autonomia ed indipendenza dal titolare e dalle altre figure, svolge un ruolo di supervisione e controllo onde evitare rischi per la privacy e la sicurezza degli interessati. Questa figura è richiesta anche quando sono gli organi istituzionali statali o comunitari a svolgere trattamenti di categorie particolari di dati.

Per quanto riguarda il trattamento dell'ultimo gruppo di dati particolari, ovvero i dati giudiziari, il meccanismo ricalca quello descritto sopra, ma con ulteriori limitazioni. Infatti solo le autorità pubbliche possono trattare autonomamente questo tipo di informazioni, mentre i privati possono manipolarle solo sotto supervisione da parte degli organismi pubblici e con l'ausilio di un DPO. Va ricordato inoltre che solo presso lo Stato può esistere un registro completo delle condanne penali.

[82] O ex "dati sensibili".

Ma l'argomento che forse premerà di più al lettore, in qualità di interessato, è quali siano i propri diritti. Infatti il GDPR, sotto l'ombrello della generale protezione del diritto alla privacy, racchiude tutta una serie di diritti specifici, vale a dire azioni attivabili nei confronti dei propri dati, per ottenere effetti sul trattamento in atto. Alcuni di questi, come ad esempio la possibilità di accedere agli archivi riguardanti sé stessi o di rettificare informazioni sbagliate sul proprio conto, non sono certo una novità. Altri invece sono decisamente più innovativi e per questo controversi.

Ad esempio alcune perplessità riguardano la portabilità dei dati, ovvero la possibilità di richiedere ad un titolare di trasmettere i propri dati ad un soggetto terzo. Sebbene in teoria si tratti di uno strumento molto utile, potrebbe rivelarsi un'arma a doppio taglio. Prendiamo ad esempio il caso di un cliente di una compagnia telefonica, che voglia trasmettere i propri dati ad un'altra compagnia che offre un contratto più vantaggioso. Se l'azienda A applicasse una penale per la recessione dal contratto, l'interessato potrebbe decidere non tanto di dare un nome falso, quanto ad esempio di omettere il proprio secondo nome, per creare una portabilità falsata ed evitare così i costi di cessione sostenendo che si tratta di due soggetti diversi. Corollario generico a questo esempio è che, sebbene sia sempre auspicabile aumentare le tutele dell'individuo, talvolta questi strumenti potrebbero fornire scappatoie per comportamenti disonesti.

Un altro neonato diritto, che si è rivelato più semplice da applicare in teoria che nei fatti, è il diritto all'oblio. Secondo il GDPR, l'interessato può richiedere, quando previsto dal regolamento, che i suoi dati siano cancellati non solo dall'archivio del titolare, ma anche dagli archivi di tutti i soggetti terzi a cui quest'ultimo possa aver comunicato tali informazioni. Ora, se la cancellazione da parte del titolare originario non rappresenta un grosso scoglio, ben diverso è il coinvolgimento di altri soggetti, che non rientrano nel rapporto originario fra titolare e interessato. La situazione si fa particolarmente complicata quando si parla di informazioni reperibili su internet: anche eliminando la fonte originale, potrebbero esistere altri siti o link che riportano gli stessi dati al di fuori del raggio di azione del GDPR stesso, ovvero al di fuori dell'Unione europea. Se la giurisprudenza della Corte di Giustizia europea ha sempre riconosciuto il limite geografico all'applicazione delle norme sulla privacy, ben più coraggioso si è rivelato l'atteggiamento del Garante per la privacy italiano. Con il provvedimento n. 557 del 21 dicembre 2017, infatti, il Garante ha imposto al colosso informatico la deindicizzazione di tutti gli URL contenenti informazioni riguardanti il ricorrente, un cittadino italiano residente negli USA. Non resta che augurarsi che la possibilità della "deindicizzazione globale" venga considerata dagli organismi europei negli stessi termini.

Sia dalla lettura di queste conclusioni, che dall'analisi della realtà italiana, emerge come non sempre la normativa possa applicarsi concretamente nell'ambito della realtà. Questo è normale,

dato lo scontro fra un mondo astratto e per questo prevedibile ed esatto con il mondo reale, in cui esistono imprevisti ed errori. Per esempio, il GDPR prevede l'esistenza della figura del DPO esterno, senza considerare che l'unico mercato per questo tipo di professionista sono le grandi aziende, che formano solo una parte del panorama economico non solo italiano, ma anche europeo.

Per concludere questa trattazione, è opportuno esaminare le sfide che i legislatori dovranno affrontare in futuro, in parte per l'innegabile velocità a cui si muove la società odierna, in parte per mancanza di zelo nel legiferare presente. Indubbiamente una delle più importanti riguarda gli sviluppi tecnologici e le nuove frontiere che esse potrebbero offrire nel mercato dello studio dei dati a scopi di marketing o di pubblicità. Stiamo parlando dei *big data* e degli usi che potrebbero esserne fatti, primo fra tutti la profilazione. Dalla profilazione si ottengono infatti i *metadati*, ovvero dati non forniti direttamente dagli interessati, ma dedotti incrociando ed analizzando i dati veri e propri. Queste informazioni sono una vera e propria miniera d'oro per il mercato digitale, in quanto possono essere venduti al miglior offerente per gli scopi più disparati: dal marketing mirato fino alle campagne elettorali. Poiché questi dati non sono una proprietà intellettuale dell'interessato, il loro utilizzo ad oggi è piuttosto spregiudicato. Resta però da stabilire a chi vada il possesso di questi *metadati*, quali limiti si possano porre al loro uso e quante e quali informazioni possano essere legittimamente "estratte" da ciò che gli individui rendono pubblico prima di trovarsi di fronte ad una violazione della privacy.

Un altro aspetto che si è rivelato una spina nel fianco per le autorità è l'allargamento dei confini dei flussi di dati a tutto il mondo, ovvero la globalizzazione dell'informazione. Non a caso nel nuovo regolamento si ravvisa chiaramente la volontà dell'Unione europea di imporre le proprie condizioni e i propri parametri di protezione dei dati anche a tutti quei soggetti esterni, statali o privati, che trattano informazioni dei cittadini dell'Unione europea. La diffidenza del legislatore si è subito dimostrata più che giustificata: nel 2015 l'ex tecnico della CIA Edward Snowden ha denunciato l'esistenza di programmi di sorveglianza di massa gestiti dal governo degli Stati Uniti ai danni di cittadini non americani sul suolo USA, fra cui naturalmente cittadini europei. Questo ha portato al crollo dell'accordo *Safe Harbor* che regolava prima i rapporti fra i due ordinamenti in questo campo, che è stato sostituito dal più stringente EU-US *Privacy Shield*.

Infine, a livello sicuramente meno globale, si pone un sempiterno problema di adeguamento alla realtà dei fatti. Il GDPR, nel suo sforzo garantistico, ha tralasciato alcune categorie di cittadini, aumentando i loro oneri a fronte di una lista di diritti invariati. Per quanto sia poco romantico dover soppesare l'aspetto economico contro un ampliamento potenzialmente illimitato dei diritti del singolo, va considerato che per ogni diritto che si rende attivabile da parte degli interessati, nasce automaticamente un onere corrispondente in capo al titolare e a coloro che si occupano del

trattamento. Come si evidenzia nell'ultimo capitolo, questi oneri non corrispondono a nessun tipo di compensazione per la categoria dei titolari, i quali si ritrovano quindi oberati di doveri. Quando il titolare è un individuo o un'azienda che trae profitto dal trattamento di dati stesso, questi doveri e quindi i costi che ne derivano possono tranquillamente essere ascritti agli adempimenti del mestiere. Questo è il caso ad esempio delle grandi aziende informatiche o dei social network che rivendono dati a terzi, ma non si può certo applicare alla totalità dei soggetti che trattano dati. Per la maggior parte di questi, infatti, il trattamento dei dati è accidentale rispetto alla propria attività principale, per cui diventa complicato gestire sia l'attività economica centrale ed occuparsi anche capillarmente del trattamento. In pratica sarebbe come svolgere due lavori, dei quali uno solo viene retribuito. È inoltre palese come non sia possibile chiedere a tutti i titolari di delegare questa incombenza a terzi, in quanto non tutte le attività possono permettersi questo tipo di costi. Sebbene uno degli intenti fosse quello di limitare l'arbitrarietà delle grandi aziende e delle multinazionali nel disporre dei dati, di fatto si è inciso maggiormente sul sottobosco delle medie e piccole imprese, mentre i grandi fatturati possono semplicemente pagare un consulente e delegare a quest'ultimo le proprie responsabilità in materia di privacy.

Poiché l'obiettivo della presente trattazione non è certo quello di proporre rimedi al legislatore europeo, ci si limiterà a constatare l'esistenza di queste problematiche, auspicando che nel futuro la protezione del singolo possa coesistere più armoniosamente con la realtà economico-produttiva non solo dell'Italia, ma di tutta l'Europa. In questo modo il diritto alla privacy verrà percepito da tutti come un fattore positivo e non come l'ennesimo scomodo adempimento burocratico.

APPENDICE

Intervista con i formatori

1. In qualità di formatori, come siete stati aggiornati riguardo alle nuove regole imposte dal GDPR? C'è stato un aiuto da parte del Garante?

A/B: No, il Garante non ci ha mai contattati direttamente. L'aggiornamento è avvenuto tramite corsi erogati dagli enti certificati presso il Garante, che si occupano di protezione dei dati.

2. Avete mai avuto opportunità di interfacciarvi con l'autorità Garante?

A/B: No, non abbiamo mai avuto contatti con il Garante per la protezione dei dati.

3. Ci sono stati dei cambiamenti concreti rispetto alla situazione precedente, dopo l'entrata in vigore del GDPR?

A: Sebbene nella sostanza non ci siano modifiche importanti rispetto all'impostazione già esistente, il pubblico sembra più ricettivo rispetto all'argomento della privacy, probabilmente anche per la maggiore copertura mediatica che si dà da qualche anno all'argomento.

B: Nel campo delle PMI, i cambiamenti ci sono stati, ma in peggio. Molti hanno difficoltà ad adeguarsi e percepiscono gli adempimenti solo come un costo ulteriore. Per quanto riguarda le grandi aziende, come Twitter o Facebook, penso che una regolamentazione che li tenga "a bada" sia una buona cosa. L'unico problema è che anche introducendo più regole, le grandi aziende hanno più possibilità di aggirarle. Prendi il caso del DPO: una grande azienda può pagarne uno esterno e delegare così qualsiasi responsabilità.

4. Esistono per le imprese dispositivi gratuiti per aggiornarsi e svolgere gli adempimenti richiesti dal nuovo regolamento?

A/B: Sì, sui siti degli enti pubblici esistono alcuni modelli per stendere la DPIA e simili, ma non sempre sono facilmente accessibili ed ancora più spesso sono difficilmente comprensibili per un profano. Per chi vuole provare il "fai da te" esistono anche *software* a pagamento per compilare i documenti, ma ancora una volta è necessario conoscere il linguaggio legale. L'opzione migliore resta quindi affidarsi ad un consulente, anche se va pagato.

5. Secondo voi le imprese potrebbero decidere di non adempiere alla normativa per risparmiare?

A: Non solo è possibile, è anche molto frequente. Probabilmente sul versante privacy la maggioranza delle imprese non ha ancora svolto adeguamenti. Volendo fare un paragone con la sicurezza sul lavoro, quest'ultima è sicuramente più seguita, anche perché la normativa è in vigore da molto più tempo.

B: Oltre ai costi, c'è anche un elemento di delusione nei confronti delle autorità. Molti vedono i nuovi adempimenti come ulteriori fastidi burocratici oppure non vedono alcun motivo per doversi occupare di privacy, togliendo tempo al lavoro concreto. Per il gestore di un piccolo albergo è difficile capire che raccogliere nomi e cognomi per le prenotazioni vale già come trattamento di dati e che quindi si è soggetti al GDPR.

6. È difficile per i vostri clienti capire il meccanismo che c'è dietro alla protezione dei dati?

A: Finché si parla di gesti pratici, ad esempio come conservare le cartelle, non è difficile da spiegare. Il vero scoglio sono le capacità informatiche medie dei lavoratori: quando si inizia a parlare di gestire un indirizzo di posta elettronica dedicato o di cambiare ogni tre mesi la password molti lavoratori, specie quelli più anziani, si trovano completamente spaesati.

7. Qual è la vostra esperienza con la figura del DPO esterno?

A/B: Nel campo delle piccole e medie imprese, si tratta di una figura mitologica. Per poter avere un guadagno proporzionale alle responsabilità, un DPO esterno dovrebbe curare almeno una decina di imprese, ma in questo modo non riuscirebbe a seguirle tutte approfonditamente. Per questo di solito solo le grandi imprese possono permettersi un DPO esterno. Lo stesso Garante si è più volte mostrato perplesso sull'effettiva utilità di questa figura in Italia.

8. In qualità di interessati "informati sui fatti", vi sentite più sicuri riguardo ai vostri stessi dati?

A: La situazione ora è sicuramente più chiara, ma non mi sento di dire che ci siano stati grandi cambiamenti di fatto. L'unico miglioramento che ho veramente trovato è stato nella scrittura delle informative, anche se molte sono ancora scritte in "legalese".

B: Personalmente, nonostante l'entrata in vigore del GDPR, non mi sembra che sia cambiato molto. Specie navigando su internet continuo a ricevere pubblicità mirata riguardo a prodotti che potrebbero interessarmi, anche quando non rispondo ad alcun questionario né segnalo il mio interesse per quei prodotti. Questo si può spiegare solo con l'uso improprio dei dati da parte di alcune piattaforme

9. C'è più attenzione sulla sicurezza sul lavoro o alla sicurezza dei dati?

A: Per ora c'è maggiore attenzione alla sicurezza "fisica" nei luoghi di lavoro, sia perché è facile capire che la sicurezza vada tutelata, sia perché la normativa è attiva da molti più anni e quindi è più semplice assimilare la struttura, la necessità dei corsi di formazione eccetera. Nello sviluppo della sicurezza "immateriale" molto dipenderà dallo sviluppo futuro che avrà la normativa e da quanta informazione si farà sull'argomento.

10. A proposito di corsi, le ore di formazione sono sufficienti?

A/B: Per le piccole realtà sì. Sebbene i corsi oscillino fra le quattro e le otto ore, di fatto le piccole imprese non effettuano trattamenti potenzialmente rischiosi per gli interessati. Anche se avvenisse una perdita di dati in molti casi non ci sarebbero ripercussioni pericolose. Va aggiunto anche che corsi più lunghi toglierebbero troppo tempo a persone che hanno più bisogno di lavorare che di passare il tempo a lezione.

11. Gli adempimenti richiesti sono proporzionali alle realtà delle imprese?

A/B: Per quanto riguarda la realtà italiana, no. La maggior parte dei nostri clienti sono liberi professionisti e piccolissimi imprenditori, per i quali diventa difficile seguire tutte le disposizioni del GDPR, alle quali si aggiungono come minimo quelle della legge 81 sulla sicurezza sui luoghi di lavoro, e anche lavorare. C'è un dispendio di tempo e risorse esagerato per una piccola impresa, mentre si tratta di una mole del tutto ragionevole per le grandi aziende o per i gestori dei social network, che possono anche appoggiarsi a team di avvocati.

12. Come si potrebbe ovviare a questo problema?

A: Una soluzione potrebbe essere adeguare la normativa in base al numero di dipendenti dell'azienda. In questo modo si eviterebbe di intralciare il lavoro delle aziende a conduzione familiare, controllando maggiormente le grandi realtà, che hanno a che fare con flussi consistenti di dati.

B: Bisognerebbe anche introdurre una divisione per settori: è chiaro che uno studio che gestisce supporti informatici, anche se ha dieci dipendenti, tratta un numero considerevole di informazioni. Un'azienda agricola con trenta impiegati invece si occupa solo dei dati dei propri dipendenti, quindi non ha bisogno di speciali controlli. Si potrebbero usare i codici ATECO a questo scopo.

13. Per quanto riguarda le tutele speciali per i dati sanitari, come sono state conciliate con l'emergenza Covid?

A/B: Tolto il fatto che l'emergenza sanitaria è più importante della puntuale applicazione del GDPR, si sono trovate soluzioni alternative. Ad esempio nel caso della misurazione della febbre, si è aggirato il problema non registrando i dati, in modo che di fatto non ci sia trattamento.

14. Sarebbe stato meglio un maggiore coinvolgimento degli Stati nella possibilità di adattare la normativa all'ordinamento interno?

A: Se si trattasse di coinvolgere maggiormente i lavoratori del settore, la mia risposta sarebbe sì. C'è però da considerare il rischio che, emanando una normativa statale, le Regioni inizino a recepirla ognuna a modo suo come è successo con la legge 81. Adesso ci troviamo in una situazione dove l'HACCP si fa in modo diverso per ogni Regione.

B: Potrebbe essere una soluzione che permette di considerare il panorama economico di ciascuno Stato. Ad esempio l'Italia non conta molte grandi aziende, men che meno multinazionali. Questa è una cosa da tenere in conto nella stesura di una legge, ma ovviamente a livello europeo si è considerata la situazione globale.

BIBLIOGRAFIA

MONOGRAFIE, ARTICOLI e RICERCHE

Barbera A., Fusaro C., *Corso di diritto pubblico*, Bologna, Il Mulino, 2016

Biasiotti A., *Il nuovo regolamento europeo sulla protezione dei dati*, Roma, EPC, 2018

Bobbio N., *L'età dei diritti*, Torino, Einaudi, 1990

Boucher P., *SAFARI ou la chasse aux Francais,* in *Le Monde*, Parigi, 21 mar 1974

Brandeis L. D., Warren S. D., *Right to privacy*, in *Harvard Law Review,* Boston, The Harvard Law Review Association, 1890

Cassella F., Comba M., Palici di Suni Prat E., *Le Costituzioni dei Paesi dell'Unione Europea*, Padova, CEDAM, 1998

Daniele L., *Diritto dell'Unione europea. Sistema istituzionale – Ordinamento – Tutela giurisdizionale – Competenze*, Milano, Giuffrè, 2003

Dworkin G., *The Younger Committee Report on Privacy*, in *The Modern Law Review*, John Wiley and Sons, Hoboken, 1973

Prosser W., *Privacy*, in *California Law Review*, Berkeley, University of California, 1941

Richards N. M., Solove D. J., *Prosser's Privacy Law: A Mixed Legacy,* in *GW Law Publications & Other Works*, Washington D.C., The George Washington Law Faculty Publications & Other Works, 2010

TNS Opinion & Social, *SPECIAL EUROBAROMETER 359. Attitudes on Data Protection and Electronic Identity in the European Union*, Bruxelles, European Commission, 2011

SENTENZE

Cassazione Civile, sentenza del 22 dicembre 1956, *Soc. di produzione associata Tirrena Asso Film contro Caruso*, n. 4487

- sentenza del 27 maggio 1975, *Esfandiari contro Soc.* Rusconi, n. 2129

Corte EDU, sentenza del 3 ottobre 2014, *Jeunesse contro Paesi Bassi*.

- sentenza del 6 aprile 2010, IV sez., *FLinkkila and Others contro Finlandia*, n.75.
- sentenza del 7 febbraio 2012, Grande Camera, *Von Hannover contro Germania*, n. 95.
- sentenza del 5 dicembre 2013, V sez., *Henry Kismoun contro Francia*.
- sentenza del 26 giugno 2014, *Mennesson contro Francia*.

US Supreme Court, *New York Times Co. v. Sullivan*, 1964, n.376 U.S. 254

REGOLAMENTI e LEGGI

1° United States Congress, *United States Bill of Rights* 15 dic 1791, New York

93° United States Congress, *Privacy Act*, 31 dic 1974, Washington

100° United States Congress*, Computer Matching and Privacy Protection Act,* 18 ott 1988, Washington

107° United States Congress, *E- Government Act*, 17 dic 2002, Washington

114° United States Congress, *Judicial Redress Act, 2015, Washington*

Parlamento europeo e Consiglio, *Direttiva 94/46/CE relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*, Gazzetta ufficiale n. L 281, 23 nov 1994

- *Regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio, del 18 dicembre 2000, concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati*, L.008 del 12 gen 2001
- *Regolamento (UE) 2016/679, del 27 apr 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*, L. 119/1 del 4 mag 2016

Trattato sul funzionamento dell'Unione Europea, C. 326/47 del 26 ott 2012

Convenzione per la salvaguardia dei Diritti dell'Uomo e delle Libertà fondamentali, Roma, 4 nov 1950

Camera e Senato della Repubblica Italiana, *Legge n. 633 del 22 apr 1941, Protezione del diritto d'autore e di altri diritti connessi al suo esercizio,* G.U. n. 166 del 16 luglio 1941

- *Legge n. 675 del 31 dicembre 1996*
  Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali, G.U. n. 5, 8 gen 1993

Costituzione della Repubblica Italiana, GU n. 298 del 27 dicembre 1947

Assemblée Nationale et Sénat de la République française, *Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.*

SITOGRAFIA

Trattato sul funzionamento dell'Unione Europea, C. 326/47 del 26 ott 2012, consultato il 24 giu 2020

https://eur-lex.europa.eu/

CNIL – *Loi informatique et libertés*, consultato il 3 lug 2020

https://www.cnil.fr/fr/la-loi-informatique-et-libertes

Eurobarometer, *Special Eurobarometer n. 359 - Attitudes on Data Protection and Electronic Identity in the European Union*, giu 2011, consultato il 13 lug 2020

https://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_359

93° United States Congress, *Privacy Act*, 31 dic 197, consultato il 20 lug 2020

www.justice.gov/opcl/privacy-act-1974

Garante Privacy, *Diritto all'oblio*, consultato il 7 set 2020

https://www.garanteprivacy.it/regolamentoue/oblio

Garbagnati Re E., *Il tuo cervello è un super computer: può memorizzare 1 petabyte di dati*, in *Repubblica.it*, 24 gen 2016, consultato il 21 set 2020

https://www.repubblica.it/scienze/2016/01/24/news/capienza_dati_cervello_umano