

**Parte Prima**

**Riservatezza della vita privata  
e protezione dei dati personali.  
Un quadro di insieme**



# Capitolo Primo

## Tra privacy e protezione dei dati personali: la nascita di un diritto

### Sezione I

#### Il diritto europeo dei dati personali

SOMMARIO: 1. Una bussola per orientarsi. – 2. La protezione dei dati personali come diritto fondamentale di libertà. – 3. La protezione dei dati personali, diritto fondamentale di libertà nella società digitale e delle comunicazioni elettroniche. – 4. La privacy: fragile ma inviolabile barriera al controllo sulla vita privata. – 5. La protezione dati nella società digitale e delle comunicazioni elettroniche: unica, fragile ma inviolabile, barriera al controllo totale. – 6. La difficoltà di garantire in modo efficace la protezione dei dati personali nel mondo di oggi e di domani. – 7. Il diritto alla conservazione dei dati personali e delle notizie (diritto alla “memoria”) e l’opposto diritto alla cancellazione dei dati non più necessari (diritto all’“oblio”). – 8. I dati “sensibili” e la loro protezione. – 9. Opportunità e pericoli della società digitale.

#### 1. Una bussola per orientarsi

Questo volume è destinato innanzitutto agli studenti del corso di laurea in giurisprudenza e dei corsi di perfezionamento in diritti fondamentali e in diritto della protezione dei dati personali, con particolare riguardo a quelli che dovranno essere organizzati, dentro e fuori le Università, per preparare la nuova figura del *privacy officer* o, come è meglio dire in conformità al nuovo Regolamento europeo in via di definitiva approvazione, del *data protection officer*<sup>1</sup>.

---

<sup>1</sup> Il *privacy officer* è una figura che in realtà alcuni considerano già prevista dalla Direttiva 95/46/CE all’art. 18, par. 2, nella parte in cui stabilisce che gli Stati membri possono prevedere una semplificazione o addirittura un esonero dell’obbligo di notificare trattamenti di dati personali alle Autorità di controllo quando la legislazione nazionale consenta al titolare del trattamento di designare un incaricato che garantisca, in maniera indipendente, l’applicazione della normativa nazionale e tenga un registro dei trattamenti conformemente all’art. 21, par. 2 della

Si tratta di una specifica figura professionale, estremamente importante nel contesto della protezione dei dati personali, tanto più oggi, nel quadro della società digitale.

Al *data protection officer* il nuovo Regolamento europeo<sup>2</sup> dedica l'intera Sezione IV del Capitolo IV, relativo alla responsabilità del titolare (*controller*) e del responsabile (*processor*) dei trattamenti. Una collocazione normativa che, insieme al contenuto delle regole relative a questa figura, segna con evidenza tanto l'importanza quanto il ruolo che il *data protection officer* è destinato ad avere nell'imminente nuovo sistema di regolazione.

---

Direttiva. Solo poche leggi nazionali hanno, però, previsto questo, e tra esse non vi è il Codice della protezione dei dati personali italiano. A sua volta, alcuni anni dopo, la Direttiva 2009/136, modificativa della Direttiva 2002/58 (e-privacy), ha introdotto, all'art. 2, punto 4), il concetto di sicurezza come un insieme di vincoli specifici nei confronti del titolare dei servizi di comunicazione. Vincoli che in alcune legislazioni nazionali hanno dato luogo alla figura del *data security officer*.

Anche questa figura, affidata sostanzialmente alle legislazioni nazionali, non ha trovato però una specifica disciplina legislativa in molte legislazioni degli Stati membri, e comunque non in quella italiana. Anche in questo caso il Codice della protezione dei dati personali, pur molte volte rivisto, non ha colto questa opportunità.

Tutto questo non ha però impedito che da alcuni anni si svolgano numerosi corsi per la preparazione di questa nuova professionalità, ovviamente sulla base di visioni del suo ruolo non sempre coincidenti, e comunque non chiaramente fondate su una normativa specifica. Ora, come si dirà più avanti, il nuovo Regolamento europeo in materia di protezione dei dati personali prevede specificamente questa figura, dettando anche una ampia e importante disciplina relativa ai suoi compiti e alle sue responsabilità. È da augurarsi dunque che, approvato il nuovo Regolamento, anche in Italia questa figura si affermi, e siano organizzati, anche nelle Università, adeguati e seri corsi formativi. Sul punto vi sono già nella letteratura italiana molti contributi, spesso orientati anche a promuovere specifici corsi di formazione. Qui ci si limita a segnalare, per una migliore comprensione di questo istituto soprattutto nelle Direttive, CNIL (Autorità francese di protezione dati), *Which countries in Europe have adopted Data Protection Officer*, in *DPO in Europe*, marzo 2012. Per il dibattito intorno al nuovo Regolamento europeo nel corso della sua elaborazione, cfr. M. SIANO, *Le recenti proposte di revisione della normativa europea di protezione dati e il mood dei Garanti europei della privacy*, in *Media Law*, febbraio 2013. Si vedano anche il sito European Privacy Officer (EPOF) [www.epof.org](http://www.epof.org) e il sito Federprivacy, [www.federprivacy.it](http://www.federprivacy.it).

<sup>2</sup> In questa sede si dedicherà ampio spazio all'analisi sia delle norme oggi in vigore, contenute prevalentemente nelle Direttive 95/46/CE e 2002/58/CE come modificata dalla Direttiva 2009/136/CE, sia alle norme contenute nel nuovo Regolamento Europeo di protezione dati già approvato in via definitiva dal Parlamento Europeo il 17 dicembre 2015 e ora in attesa di definitiva approvazione da parte del Consiglio, prevista per la prima metà del 2016. Secondo quanto attualmente previsto dall'attuale art. 91 del testo, esso entrerà in vigore solo due anni dopo la sua adozione. È molto importante però mettere a punto già oggi strumenti di analisi della normativa vigente che siano anche un ponte verso quella futura. Per questo qui si dà molto peso anche alla nuova normativa, pur nella consapevolezza che alcuni riferimenti ad articoli o paragrafi potranno avere una numerazione diversa nella redazione del testo coordinato definitivo. La versione usata in questa sede è quella pubblicata da Statewatch, il 17 e 18 dicembre 2015, intitolata "*Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Analysis of the final compromise text with a view to agreement*".

Il volume ha però anche l'ambizione di poter essere utile a chiunque, studente universitario o meno, voglia avvicinarsi al mondo della protezione dei dati personali con l'obiettivo di capire meglio una materia tanto spesso citata, esaltata, difesa, vilipesa, negata, ma quasi sempre, e quasi da tutti, assai poco conosciuta e compresa.

Parleremo dunque di "diritto" perché nessuno può negare che la protezione dei dati sia oggi considerata come un diritto fondamentale della persona in moltissime Dichiarazioni, Carte, Convenzioni e Costituzioni.

Parleremo del significato polisensibile che si accompagna al termine "privacy" e cercheremo di spiegare perché il diritto fondamentale, che molto spesso viene ricondotto a questo concetto, nel diritto europeo si configura invece come "protezione dei dati personali".

Spiegheremo perché, man mano che si è diffuso il sistema delle telecomunicazioni e il mondo è entrato nell'era digitale e della comunicazione globale, il diritto fondamentale alla protezione dei dati personali è diventato, e sempre più diventerà, centrale per la difesa della libertà di ognuno e di tutti.

Cercheremo di far capire perché interessati *opinion makers* del mondo del market, prima, di quello degli OTT<sup>3</sup>, poi, degli operatori della sicurezza, sempre, continuino a dire con crescente insistenza che nel mondo delle telecomunicazioni e della rete la privacy è morta per sempre<sup>4</sup>. Allo stesso tempo, cercheremo di considerare anche le ragioni per le quali i *social network*, e in genere gli OTT, siano sempre più attenti ad assicurare se non la privacy intesa come riservatezza della persona, almeno la protezione dei dati, considerata

---

<sup>3</sup> OTT è un acronimo, per la verità già un poco "invecchiato", che riguarda le imprese che forniscono servizi, contenuti (video, foto) e applicazioni che consentono la vendita di prodotti o di pubblicità connessi ai contenuti trasmessi e ad altri tipi di servizi forniti come, ad esempio, i motori di ricerca. Queste imprese, delle quali fanno parte anche marchi famosissimi del mondo digitale come *Google, Apple, Facebook* e molti altri, sono definite *Over The Top* proprio perché per trasmettere i contenuti non si servono di strutture proprie ma delle reti di telecomunicazioni e quindi "operano sopra le reti". Cfr., a questo proposito, AGCOM, *Relazione annuale 2012*.

<sup>4</sup> Il più noto e famoso personaggio ad aver affermato con convinzione questo concetto è stato, come è noto, M. Zuckerberg, il fondatore di *Facebook*, che l'11 gennaio 2010 sostenne in una intervista a N. Bruno sul *Corriere della sera* che "è ormai finita l'era della riservatezza". Va detto però che Zuckerberg, la cui frase è diventata famosa in particolare in Italia, parlava volutamente di riservatezza, sottolineando che *Facebook*, che pure si basa su una *autoesposizione informativa*, ha avuto grande successo. Insomma, Zuckerberg parlava non della fine della protezione dei dati, e nemmeno della fine della privacy come tale, ma soltanto della fine del desiderio di riservatezza. Quello che appunto è il *Right to be alone* nel quale si sostanzia la *privacy* di Faulkner: una visione essenzialmente letteraria che è al centro del noto saggio di questo autore dal titolo *On the privacy. The american dream: What happened to it*, in *Harper's Magazine*, 211, July 1955. Naturalmente la frase di Zuckerberg ha avuto una risonanza assai ampia, anche perché ha permesso a molti di forzarne e mutarne il significato, traendo da essa una sorta di controprova che nella nostra epoca è sempre più difficile, e di conseguenza inutile, voler assicurare, anche attraverso norme giuridiche, la protezione dei dati personali. È questa infatti, come si dirà più avanti, l'altra e ben più moderna accezione europea di *privacy*, ed è questa la vera questione aperta della nostra epoca.

come garanzia della veridicità e affidabilità dei dati circolanti sulla rete, primi fra tutti quelli degli utenti. Nessuno più di loro, infatti, teme la fuga degli utenti dalla rete spinti dalla preoccupazione che le proprie informazioni siano rubate o manipolate. Un timore che in una certa fase ha rischiato di colpire al cuore anche il mondo dell'*e-commerce* e dell'*e-banking*<sup>5</sup>.

Cercheremo, infine, di spiegare perché, mai come oggi, e ogni giorno di più, la protezione dei dati personali sia una condizione essenziale per mantenere un minimo di autonomia, di libertà di autodeterminazione e di sicurezza specialmente nel nuovo mondo dell'IOT (acronimo di *Internet of things*) e davanti ai nuovi sterminati orizzonti aperti dai *big data*<sup>6</sup>.

Naturalmente si tratterà di un "viaggio" complesso, perché dovremo tenere insieme il passato, il presente e il futuro; diritto e vita reale; visioni e progetti relativi allo sviluppo delle tecnologie; orizzonti e anticipazioni che sembrano muoversi più nel mondo della fantascienza che in quello della realtà.

## 2. La protezione dei dati personali come diritto fondamentale di libertà

Nel cominciare questo cammino è bene dire subito che al centro dell'attenzione deve essere la persona umana e i suoi diritti fondamentali. L'obbiettivo è quello di affacciarsi sul mondo di oggi, e ancor più su quello di domani, per capire cosa significhi, e sempre più significherà, la tutela della persona, delle

---

<sup>5</sup> Estremamente significativa di questa preoccupazione crescente delle OTT, è la vicenda che ha contrapposto *Apple* alla richiesta dell'FBI di avere accesso a tutti i dati conservati nello smartphone di Syld Farrok, uno dei terroristi coinvolti nella strage di S. Bernardino (California).

Alla richiesta dell'FBI, avvalorata dall'*Exhibit* di un giudice federale, *Apple* ha opposto un netto rifiuto sulla base di motivazioni rese pubbliche in una lettera del 16 febbraio 2016 del CEO Tim Cook intitolata "*A message to our Customers*" e resa pubblica sul sito di *Apple* (cfr. [www.apple.com/cusomerletter](http://www.apple.com/cusomerletter)). Su questa vicenda *Apple* ha anche ricevuto la pubblica solidarietà di *Google*, *Whatsapp*, *Mozilla*, *Facebook*, *Twitter*.

<sup>6</sup> Su "Internet delle cose" si veda il Parere n. 8/2014 del Gruppo articolo 29 (WP n. 223), intitolato "*Recenti sviluppi di Internet delle cose*".

Giova anticipare qui cosa sia il Gruppo di lavoro comune articolo 29 o, in inglese, il *Working party art. 29* (WP29). Si tratta di un Gruppo di lavoro comune delle Autorità nazionali di controllo e protezione dati degli Stati dell'Unione, che si riuniscono insieme per svolgere una serie di attività puntualmente individuate dall'art. 29 della Direttiva 95/46/CE. Si farà molto spesso riferimento nel corso di questo volume sia alla Direttiva 95/46 che ai Pareri e Documenti di lavoro del Gruppo articolo 29. È utile segnalare che, sia nel testo che nelle note, talvolta si userà la dizione Gruppo articolo 29 e i Pareri saranno indicati con il titolo italiano. Talaltra invece si farà riferimento al Working Party 29 e al posto del termine Parere si userà il termine *Opinion* e il titolo sarà in inglese. Questo deriva dal fatto che non tutte le *Opinions* e i *Working's documents* del Working Party sono tradotti in italiano. Spesso ne esiste solo la versione inglese, qualche volta anche quella francese e tedesca, e in questi casi si preferisce usare la versione inglese, che è sempre quella originale. In linea di massima comunque la maggior parte delle *Opinions* e dei *Working's Document* sono tradotti anche in italiano, e in questi casi si farà riferimento a questa versione.

sue libertà e, in ultima analisi, della dignità sua e della sua famiglia, come recita l'art. 2 della nostra Costituzione.

La dignità della persona umana come valore e come oggetto di diritti fondamentali è da molti, e con ragione, considerata un po' datata e legata soprattutto al personalismo cattolico francese del secolo scorso<sup>7</sup>.

Essa tuttavia aiuta a cogliere nella visione della libertà personale, economica, sociale e politica, il "cuore" dei diritti universali dell'uomo e soprattutto ha, nella nuova realtà globalizzata, una forza e una "capacità di senso" eccezionalmente importante<sup>8</sup>. In un mondo attraversato da migrazioni di milioni di persone da uno Stato all'altro e da un continente all'altro, e che non ha ancora potuto dimenticare le cicatrici della seconda guerra mondiale e dei conflitti del Novecento, proprio la dignità della persona è diventata, insieme e più della stessa libertà personale, il valore dominante di tutte le Carte dei Diritti, da quella dell'ONU<sup>9</sup> a quella CEDU<sup>10</sup>, fino alla Carta di Nizza<sup>11</sup>, contenente i diritti fondamentali dell'Unione europea. Proprio la Carta di Nizza peraltro rappresenta, col suo art. 8, il punto più alto del riconoscimento della dignità della persona, ora anche esplicitamente estesa al diritto alla protezione dei dati personali<sup>12</sup>.

Del resto, proprio l'evoluzione tecnologica delle comunicazioni elettroniche, che è alla base della società digitale e della globalizzazione delle relazioni interpersonali, economiche, finanziarie e sociali, ha visto sempre di più il diritto alla dignità della persona ampliarsi fino a comprendere anche il diritto alla protezione dei dati personali come diritto fondamentale ed elemento essenziale del rispetto della persona e della sua vita familiare<sup>13</sup>.

---

<sup>7</sup> La letteratura su questa corrente del cattolicesimo francese ed europeo è sterminata. In questa sede, dato il tenore del volume, ci si limita a rinviare al sintetico ma pregevole saggio di J.-M. DOMENACH, *Personalismo*, in *Enciclopedia del Novecento*, Treccani, Roma, 1980.

<sup>8</sup> In questo senso la Enciclica "*Laudato si*" di Papa Francesco "*sulla cura della casa comune*", del 24 maggio 2015 è assolutamente moderna e offre un quadro del mondo di oggi e di quello che verrà nella quale si ritrovano tutti i temi della contemporaneità, dalla difesa intransigente dei diritti fondamentali dell'uomo, all'attenzione alla tutela dell'ambiente fino all'analisi delle promesse e dei pericoli della società digitale.

<sup>9</sup> Cfr. Dichiarazione universale dei diritti umani, proclamata dall'Assemblea generale delle Nazioni Unite il 1° dicembre 1948 a Parigi. Merita segnalare che il Preambolo inizia con queste parole "*Considerato che il riconoscimento della dignità inerente a tutti i membri della famiglia umana e dei loro diritti, uguali e inalienabili, costituisce il fondamento della libertà, della giustizia e della pace nel mondo*".

<sup>10</sup> Cfr. Convenzione europea dei diritti dell'uomo, firmata a Roma il 4 novembre 1950, *Preambolo* e art. 8, dedicato al "*Diritto al rispetto della vita privata e familiare*".

<sup>11</sup> Cfr. Carta dei diritti dell'Unione Europea. Questa Carta, detta anche Carta di Nizza, perché proclamata in quella città della Francia il 7 dicembre 2000, è ora riconosciuta, con lo stesso valore giuridico dei Trattati, dall'art. 6 del Trattato sull'Unione Europea, così come modificato dal Trattato di Lisbona, entrato in vigore il 1° gennaio 2009.

<sup>12</sup> Cfr. Carta dei diritti fondamentali dell'Unione europea, art. 7 intitolato "*Rispetto della vita privata e della vita familiare*" e l'art. 8 "*Protezione dei dati di carattere personale*".

<sup>13</sup> Cfr. su questo, oltre alla Carta dei diritti fondamentali dell'Unione europea, cit., art. 8,

Infine, va ricordato che, proprio sulla dignità della persona la scienza giuridica italiana e la Corte costituzionale hanno da tempo fondato il valore costituzionale di questo diritto anche in una Costituzione che non ne fa altrimenti parola<sup>14</sup>.

La protezione dei dati personali, nata come risposta alla tecnologia legata al trattamento automatizzato dei dati, è oggi diventata anche l'ultima e più importante barriera allo straripare della società digitale che, anche al fine di assicurare servizi che la stessa persona richiede, fa circolare in rete, e rende quindi potenzialmente acquisibili e controllabili, i dati personali di ognuno. Informazioni che ci riguardano, e che ci vengono chieste o che noi spontaneamente diamo, e che spesso non sono utilizzate solo al fine di assicurarci i vantaggi che la rete ci mette a disposizione.

Proprio la rete e i servizi che essa offre consentono una circolazione potenzialmente illimitata nel tempo, nella qualità e nella quantità, delle informazioni che riguardano una persona umana. Tutto questo comporta pericoli elevati per la libertà e la dignità delle persone, e richiede dunque non già una rinuncia alla protezione di queste informazioni ma, al contrario, sistemi di tutela sempre più raffinati.

Due in particolare sono gli aspetti delle nuove tecnologie che più mettono a dura prova la protezione dati, già messa in difficoltà dall'espandersi della società digitale, sia prima che dopo il web 2.0.

La prima sfida è legata ai *big data*, espressione legata all'utilizzazione di server e sistemi di trattamento digitale automatizzato che consentono raccolte sempre più gigantesche di dati, acquisiti soprattutto, e in modo massiccio, in rete, e trattati per le più diverse finalità, a costi sempre più bassi e con tempi sempre più veloci, grazie a elaboratori sempre più potenti. Una realtà in continua evoluzione, che ha come scopo essenziale utilizzare i dati e le informazioni che si raccolgono in maniera sempre più "bulimica" per trarne

---

anche, la Convenzione n. 108/1981, adottata in ambito CEDU, e la Direttiva 95/46/CE. Sul legame fra sviluppo della tecnologia e protezione dei dati personali si tornerà più ampiamente nel secondo Capitolo di questa Parte.

<sup>14</sup> Sul punto sia sufficiente rinviare a S. RODOTÀ, *Il diritto di avere diritti*, Laterza, Bari, 2012; ID., *La rivoluzione della dignità*, La scuola di Pitagora, Napoli, 2013 e, anche a carattere più informativo, ID., *Il mondo della rete. Quali i diritti, quali i vincoli*, Laterza, Bari, 2014.

Sempre sul tema della dignità, si veda in particolare G.M. FLICK, *Elogio della dignità*, Libreria Editrice Vaticana, Roma, 2015; ID., *La globalizzazione dei diritti: il contributo dell'Europa dal mercato ai valori*, con Prefazione di R. Prodi, Piemme, Casale Monferrato, 2004.

Per la giurisprudenza costituzionale italiana, cfr. Corte costituzionale, sentenza n. 271/2005, che considera il diritto alla protezione dei dati personali non solo collocato nell'ambito del diritto civile, ex art. 117, comma 2, lett. l), ma anche come un diritto che si riferisce "all'intera serie dei fenomeni sociali nei quali questi possono venire in rilievo: da ciò una disciplina che, pur riconoscendo tutele differenziate in relazione ai diversi tipi di dati personali ed alla grande diversità delle situazioni e dei contesti normativi nei quali tali dati vengono utilizzati, si caratterizza essenzialmente per il riconoscimento di una serie di diritti alle persone fisiche e giuridiche relativamente ai propri dati, diritti di cui sono regolate analiticamente caratteristiche, limiti, modalità di esercizio, garanzie, forme di tutela in sede amministrativa e giurisdizionale".



un numero potenzialmente infinito di “*informazioni da informazioni*”<sup>15</sup>.

La seconda sfida, ancora all’inizio ma in continuo e travolgente sviluppo, è l’*Internet delle cose* (IOT): un insieme di tecnologie sempre più raffinate che hanno come scopo far dialogare tra loro le “cose” anche al fine di consentire agli esseri umani di usare le risorse a loro disposizione in modo non solo sempre più efficiente, ma anche più organizzato e più funzionale<sup>16</sup>.

La prospettiva legata all’Internet delle cose apre infatti nuovi scenari perché spinge, e sempre più spingerà, anche le persone comuni a utilizzare nella vita di ogni giorno la rete non solo per entrare in contatto gli uni con gli altri, o per ricevere servizi, o fare ricerche e acquisire informazioni, ma anche per gestire la propria quotidianità, in un ambiente sempre più “robotico” ma anche sempre più ricco di potenzialità e risorse. Il che ovviamente porterà a una proliferazione sempre maggiore di informazioni su ognuno di noi, e sui suoi comportamenti, fatte circolare attraverso la rete. Un aspetto estremamente delicato perché queste informazioni, captate da altri in assenza di adeguate protezioni, e elaborate col sistema dei *big data* o anche con sistemi di analisi dedicate al singolo utente, possono rivelare una quantità sterminata di cose sui comportamenti, le abitudini e le opinioni di ciascuno.

### 3. La protezione dei dati personali, diritto fondamentale di libertà nella società digitale e delle comunicazioni elettroniche

Proprio lo sviluppo della società digitale e della ICT (*Information Communication Technology*) dà oggi ancora più rilevanza che nel passato<sup>17</sup> alla protezione dei dati personali.

Nella società digitale e delle comunicazioni elettroniche il diritto fonda-

---

<sup>15</sup> Sulla complessa tematica dei *big data* e sulle sfide che questa pone alla protezione dei dati personali, si veda lo *Statement* adottato nel 2014 del Gruppo di lavoro articolo 29 intitolato: “*Statement of the WP29 on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU*” (WP n. 223).

<sup>16</sup> Sul tema cfr. recentemente Gruppo articolo 29 Parere n. 8/2014 “*sui recenti sviluppi nel campo dell’Internet degli oggetti*”, 16 settembre 2014.

<sup>17</sup> Va detto che fin dall’inizio della sua attività, il Gruppo di lavoro articolo 29 ha sempre prestato particolare attenzione ai temi della rete nella prospettiva della protezione dati, anche per colmare alcune evidenti lacune del contenuto della Direttiva 95/46, delle quali si dirà più avanti. Qui merita ricordare che dal momento della sua istituzione nel 1997, i primi Pareri e le prime Raccomandazioni di questo Gruppo furono dedicate proprio ai problemi che già allora si profilavano rispetto alla protezione dei dati personali in rete. Basti ricordare che la prima Raccomandazione del Gruppo, la n. 1/97, fu dedicata al tema “*La legge sulla protezione dei dati personali e i media*” (WP n. 1). Nel corso di quell’anno, poi, il Gruppo approvò altre due Raccomandazioni particolarmente significative. La prima fu la Raccomandazione n. 2/97 intitolata: “*Report and Guidance by the International Working Group on Data Protection in Telecommunications (Budapest-Berlin Memorandum on Data Protection and Privacy on the Internet)*” (WP n. 5). La seconda fu la n. 3/97 intitolata: “*Anonymity on the Internet*” (WP n. 6).

mentale alla protezione dei dati diventa anche il presidio irrinunciabile di tutte le libertà classiche delle nostre Costituzioni e, in ultima analisi, della nostra società democratica.

Se, infatti, attraverso la raccolta, l'incrocio e l'analisi dei dati che riguardano una persona, da questa forniti per ricevere un servizio o per utilizzare la rete, si analizza ogni aspetto delle sue attività, fino a poterne prevedere anche i comportamenti e le scelte future, rischia di perdere significato la libertà personale intesa non solo come libertà dagli arresti ma anche da ogni controllo illecito. E perdendo la libertà personale tutte le altre libertà sono perse.

Dalla libertà di manifestare il proprio pensiero a quella di accedere senza doverne rendere conto alle fonti di informazioni preferite, dalla libertà di comunicazione a quella di associazione e di riunione, fino alla libertà religiosa e all'esercizio dei diritti politici e sociali, tutto è in gioco<sup>18</sup>. Rischia di essere messa in pericolo la parità sessuale, l'eguaglianza fra le razze, la libertà di circolazione, di domicilio, la stessa libertà di associarsi, riunirsi, sviluppare liberamente e senza indebiti controlli il proprio sistema di relazioni e di rapporti sociali.

In una parola, rinunciare alla protezione dei dati personali da ogni indebita ingerenza, significa rischiare di vanificare ogni forma di libertà e mettere in pericolo tutti i diritti fondamentali<sup>19</sup>.

Come si cercherà di dire nei paragrafi successivi, questo è un rischio, e un pericolo, che gli esseri umani hanno sempre corso e che è in larga parte legato al fatto stesso che l'uomo è un animale sociale, e come tale al centro di una rete di relazioni. O, come molto meglio dice la nostra Costituzione, e oggi il più moderno costituzionalismo ribadisce, l'essere umano è una persona e non soltanto un individuo. Lo sviluppo della personalità di ciascuno non è un processo individuale che si svolge nell'ambito della "monade" della propria vita ma, al contrario, è un processo di relazioni che si sviluppa all'interno delle formazioni sociali di cui ciascuno fa parte.

Allo stesso tempo è certamente vero che tutta la storia dell'umanità potrebbe essere letta anche secondo la coppia "tutela della propria sfera di azione personale" *versus* "controllo sul comportamento degli altri". Quello che in termini di gergo potrebbe essere "farsi i fatti propri" *versus* "ingerirsi nella vita degli altri".

Così come è vero che tutta la nostra capacità di conoscenza e, in particolare, di quella della storia delle generazioni che ci hanno preceduto, delle loro azioni e dei loro pensieri, è sempre il risultato di una raccolta e di

---

<sup>18</sup> Cfr. su questi temi, con una apertura che va oltre la sola libertà di espressione, M. OROFINO, *La libertà di espressione tra Costituzione e Carte europee dei diritti*, Giappichelli, Torino, 2014.

<sup>19</sup> Non si creda che le espressioni usate nel testo siano dovute a un eccesso di retorica. Esse rappresentano solo la realtà di oggi e i pericoli che corrono le nostre libertà. Non per nulla l'art. 1 del nuovo Regolamento europeo recita al par. 2: "*This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data*".

un'analisi di informazioni sul passato e sul comportamento di chi è vissuto prima di noi. Una raccolta che è poi organizzata secondo le finalità che si vogliono raggiungere, e dalla quale, grazie a queste attività di archiviazione e di analisi, si acquisiscono nuove informazioni più complesse e organizzate di quelle originali.

Né d'altra parte è possibile ignorare che un aspetto costante della vita degli uomini nelle loro relazioni sociali, e cioè nell'ambito delle società umane, è legata alla coppia "tutela della propria libertà da ogni ingerenza altrui" *versus* "controllo inevitabile della comunità sulla vita e le attività dei propri membri". È proprio l'inevitabile rapporto di comunità che spinge ciascuno dei suoi membri verso il famoso e irresistibile bisogno di "farsi i fatti degli altri", ed è proprio per limitare, ridurre e contrastare questo controllo che nascono e si invocano tanto la privacy, intesa come riservatezza, quanto la protezione dei dati personali, intesa come tutela delle informazioni che ci riguardano.

La tecnologia, insieme allo svilupparsi sempre più oppressivo dello Stato come esercizio del potere sovrano e come tutore della sicurezza interna e della difesa dal nemico esterno, ha poi condotto, soprattutto nel periodo e nell'ambito degli Stati autoritari, a forme moderne di controllo, finalizzate ad ascoltare, registrare e conservare tutto senza alcun limite, fino a sviluppare una ossessiva volontà dello Stato e dei suoi agenti di "vivere le vite degli altri"<sup>20</sup>.

A prima vista, sembrerebbe logico che mentre il pensiero sociale e giuridico sviluppava nei secoli specifiche garanzie e definite libertà costituzionali a favore delle persone e delle loro forme associative, anche la protezione dei dati personali, almeno come rispetto della vita privata, fosse riconosciuta diritto fondamentale, senza attendere le tragedie della prima metà del Novecento.

Così invece non è successo, anche se nei paragrafi successivi proveremo a rendere conto meglio di come la privacy non sia un concetto sociale e giuridico legato solo alla nostra epoca.

#### **4. La privacy: fragile ma inviolabile barriera al controllo sulla vita privata**

È indiscutibile che di privacy come diritto si comincia a parlare solo negli Stati Uniti di fine ottocento, grazie al famoso articolo di Warren e Brandeis *Right to privacy*, pubblicato nella *Harvard Law Review* del 1890, mentre la protezione dei dati personali è un istituto giuridico che trova particolare fortuna dopo la seconda guerra mondiale, in particolare nell'ambito culturale e giuridico europeo che aveva attraversato l'esperienza degli Stati totalitari e

---

<sup>20</sup> È chiaro che il virgolettato richiama volutamente il titolo del noto film del 2006 "Le vite degli altri" (*Das Leben der Anderen*), scritto e diretto da Florian Henckel von Donnesmarck.

aveva visto la loro capacità di raccogliere, trattare e utilizzare milioni di informazioni sui loro cittadini, sia grazie all'ascolto delle comunicazioni telefoniche che all'organizzazione automatizzata dei dati.

La protezione dati ha successivamente trovato uno sviluppo ulteriore nell'ambito della società digitale. La *ICT society* trasforma ogni dato in bit e sviluppa modalità sempre più ampie e pervasive di scambio, raccolta, archiviazione e uso delle informazioni che ciascuno, per il fatto stesso di navigare in rete, diffonde e che la rete raccoglie e conserva, quale che sia il servizio, l'utilità o le finalità per i quali questi dati sono stati forniti. Tutto questo ha reso sempre più importante la necessità di stabilire quali siano gli usi legittimi e quali quelli illegittimi di queste informazioni, e come esse debbano essere protette.

Nella nostra epoca, infine, la necessità di proteggere i dati, che contengano o meno informazioni riconducibili a persone o gruppi, ha ormai assunto una dimensione sociale di interesse generale.

Non si tratta più di tutelare solo gli individui, garantendo il rispetto del loro diritto fondamentale alla protezione dei dati personali.

È sempre più necessario proteggere le società democratiche dal rischio del controllo globale. Esso, infatti, anche se organizzato dalle Autorità di polizia e sicurezza per tutelare i cittadini, significherebbe inevitabilmente la perdita della conquista più importante della democrazia, che consiste nel riconoscimento di una sfera di libertà che è compito primario dello Stato garantire.

È vero che il sogno di una società della libertà totale può trasformarsi rapidamente nella realtà di una società del pericolo e della paura per tutti. Così come è evidente che la società del controllo globale non è più quella della libertà totale da ogni minaccia, ma piuttosto quella dell'oppressione e della paura di essere costantemente spiati e "monitorati".

Nel mondo contemporaneo, inoltre, accanto al potere di controllo degli Stati e delle loro istituzioni, si è sviluppato, proprio grazie all'espandersi del sistema delle telecomunicazione e della *ICT society*, *un enorme potenziale di controllo dei privati sui privati*.

Anche in questo caso tuttavia occorre essere equilibrati.

Forme di controllo di privati su privati ci sono sempre state, legate o meno a un rapporto di subordinazione o persino di schiavitù.

In tutte le strutture sociali, infatti, vi sono inevitabilmente uomini e organizzazioni, pubbliche o private, che possiedono, e hanno sotto controllo, informazioni che riguardano altri. Anche volendo guardare soltanto alle esperienze delle società dei secoli scorsi, si pensi, da un lato, ai liberi professionisti, dai notai ai medici, dall'altro, alle organizzazioni complesse, come le scuole, gli ospedali, gli ospizi, le caserme, le strutture di vita collettiva insomma.

Fin dall'epoca rinascimentale, e poi in quella delle grandi scoperte, non sono certo mancate le banche, le compagnie titolari di concessioni coloniali, le compagnie di assicurazioni, e così via, che possedevano e trattavano quantità molto rilevanti di informazioni e, in modo particolare, di informazioni relative a persone: dagli schiavi, ai marinai, agli eventuali passeggeri, ai membri del-

l'equipaggio fino agli armatori e ai soci degli istituti e delle compagnie titolari di concessioni.

Nel passato però la conservazione dei dati significava essenzialmente archivi o raccolte di documenti, anche organizzati facendo uso dei materiali più diversi. A sua volta, ogni archivio o raccolta faceva generalmente capo a una struttura o a un settore di attività.

Allo stesso tempo, anche ogni linea di trasmissione organizzata di documenti e di informazioni faceva capo a strutture specifiche e diverse: dalle società o strutture, pubbliche o private, che gestivano la posta a cavallo, alle relazioni tra ordini religiosi; dal sistema della trasmissione di informazioni affidate ai girovaghi e ai mercanti, alle comunicazioni e alle notizie portate da un continente all'altro e da un porto all'altro dalle navi che collegavano le varie parti del mondo; dagli eserciti in marcia, alle strutture di collegamento fra colonie e madre patria.

Accanto a queste linee di circolazione organizzate, e di conseguenza generalmente "protette", correivano parallele le linee di diffusione delle notizie affidate alle "storie" e ai "racconti" che, correndo di bocca in bocca, da mercato a mercato, da fiera a fiera, da corte a corte, si trasformavano e ingigantivano, spesso fino a costruire una narrazione fantasiosa, spesso lontana dalla realtà.

Era il mondo nel quale aveva un senso concreto la prospettiva di "rifarsi una vita" trasferendosi da una regione all'altra, da un regno a un altro, da un continente all'altro.

Anche allora esisteva, e spesso in modo molto concreto, il problema di nascondere o proteggere i propri dati o di sfuggire al controllo degli altri. La differenza tra allora e oggi è però sostanziale: la possibilità di sottrarsi al controllo aveva allora una sua concretezza, così come quella di nascondere e persino distruggere i propri dati; oggi, tutto questo è sempre più difficile e persino astratto.

Il formarsi dello Stato moderno, che comincia con le grandi organizzazioni burocratiche delle monarchie assolute e dei grandi imperi moderni, e raggiunge il suo apice con la costruzione napoleonica dell'amministrazione francese, rende via via più invasivo il ruolo dello Stato e sviluppa forme di archiviazione di dati e informazioni sulle persone e sulle comunità sempre più dettagliate.

Lo stesso fenomeno, ovviamente, si sviluppa in parallelo nell'ambito delle grandi strutture commerciali e produttive, tanto a carattere pubblico che privato.

Anche la capacità delle informazioni di circolare e la diffusione organizzata del pensiero crescono, soprattutto attraverso lo sviluppo della stampa, che aiuta non solo la circolazione delle idee ma anche delle informazioni, comprese quelle a carattere legale o commerciale.

Le innovazioni tecnologiche, specialmente nel sistema dei trasporti e delle linee di comunicazione, sono alla base tanto del restringersi del mondo quanto dell'aumentare della capacità di controllo degli Stati, mentre si forma una opinione pubblica internazionale che anticipa il peso e il ruolo di quella europea del XIX secolo.

Tra il XIX e il XX secolo lo sviluppo delle tecnologie legate all'archiviazione delle informazioni, alla stampa e, infine, alla comunicazione a distanza, fanno un balzo in avanti che cambia di nuovo sostanzialmente i termini dei confini tra pubblico e privato, tra la possibilità di reprimere e perseguire il pensiero e la capacità delle idee di circolare e diffondersi fino a incidere sui sistemi sociali e determinarne il cambiamento, a volte anche in modo violento.

Infine, con la formazione della società dell'informazione nell'ambito delle democrazie più solide e la quasi contemporanea crescita di nuove e più totalizzanti forme di Stato autoritarie, il rapporto tra difesa della vita privata e controllo della pubblica opinione, da un lato, tutela della propria libertà e controllo sempre più invasivo dello Stato, dall'altro, muta di nuovo.

È in questo contesto che un tema vecchio come il mondo, legato alla necessità di proteggersi dalla curiosità degli altri e dal controllo asfissiante del potere, dà vita alla "riservatezza" come diritto autonomo che, però, si articola presto in due nuovi e distinti diritti. Quello alla privacy, storicamente legato al potere dell'informazione nell'ambito delle società democratiche; quello alla protezione dei dati personali, legato invece alla volontà di porre un limite al potere di controllo legato alla raccolta e uso delle informazioni sulla vita delle persone, dall'altro.

Come vedremo meglio più avanti, questo è il percorso che segna il nostro passato, fino agli anni, davvero recenti, della diffusione della rete e della rivoluzione digitale.

## **5. La protezione dati nella società digitale e delle comunicazioni elettroniche: unica, fragile ma inviolabile, barriera al controllo totale**

La grande novità della ICT (*Information and Communication Technology*) è che oggi le comunicazioni nella società digitalizzata passano attraverso un sistema molto diffuso e veloce di trasferimento dei dati, e quindi delle informazioni che essi veicolano.

Questo vale innanzitutto per quanto riguarda le linee di trasmissione (ancor oggi prevalentemente telefoniche e dunque gestite da *provider* telefonici, fisicamente collocate sul territorio o attraverso cavi o ponti radio). Vale però anche, e con non minor impatto, per le società multinazionali che sono riuscite, in pochi anni, a concentrare in un numero molto piccolo di OTT il possesso delle piattaforme e larga parte dei servizi accessibili in rete.

La conseguenza di questa doppia concentrazione del sistema delle telecomunicazioni, basato da un lato sui fornitori di rete e dall'altro sui fornitori di servizi, è che, in assenza di misure adeguate di protezione dei dati personali, la società del controllo da un lato, si *espande frammentandosi*, e dall'altro, si *concentra espandendosi*.

Si estende frammentandosi perché essendo pochi, ma comunque pur sempre un certo numero, i soggetti che, o a titolo di gestori delle reti o a titolo di

fornitori di servizi, trattano dati, il sistema tende a frammentarsi tanto nella loro raccolta quanto nel loro sfruttamento. Proprio per questo, però, il fenomeno assume anche una forma di concentrazione crescente, legata ai fornitori di servizi, che offrono sempre più servizi e mettono a disposizione sulle loro piattaforme sempre più applicazioni. Il che consente a questi soggetti di disporre di una quantità sempre crescente di dati e informazioni sugli utenti.

Allo stesso tempo gli apparati preposti alla sicurezza, sulla base o meno di specifica previsione legislativa o autorizzazione giudiziaria, possono chiedere, e di norma ottenere, sia dai provider telefonici che dagli OTT, i dati in loro possesso.

Si possono così accumulare numeri sterminati di dati che, considerando la potenza dei server attuali e l'esistenza delle tecniche di *big data*<sup>21</sup>, legate a server e processi di dimensioni impensabili fino a qualche anno fa<sup>22</sup>, avvicinano sempre di più il nostro mondo alla società del controllo globale.

Sempre più è evidente che nella società contemporanea dominata dalla rete e dal digitale non vi è più alcun luogo per nascondersi, per parafrasare il libro di Glee Greenwald, premio Pulitzer 2014<sup>23</sup>.

È chiaro il rischio che, volendo difendere le società democratiche, si finisca, invece, per portare le nostre società fuori dalla democrazia, come avviene inevitabilmente se le libertà individuali e collettive devono vivere in un ambiente in cui ogni azione di ciascuno può essere, ed è, sotto controllo.

---

<sup>21</sup> La letteratura sui *big data*, termine peraltro polisemo, che si riferisce sia allo svilupparsi di server sempre più capaci di conservare e processare una quantità sterminata di dati, sia alla capacità di ottenere dal trattamento di questi dati, grazie a algoritmi che sappiano interrogare la macchina in modo da avere da essa la risposta voluta o la informazione ricercata, una quantità sempre più sterminata di nuovi dati, che consentano nuove conoscenze e analisi relative ai fenomeni naturali e ai comportamenti umani. Qui si ricorda, uno per tutti, il lavoro di V. MAYER-SCHONBERGER-K. CUKIER, *Big Data*, pubblicato nella traduzione italiana da Garzanti, Milano, 2013 ed uscito nella versione originale inglese presso Houghton Mifflin Hartcourt Publishing Company, 2013.

Per una analisi molto sintetica ma utile, corredata da ampia bibliografia di cosa si intenda oggi per *big data* e quali problematiche questa espressione coinvolga, si rinvia a *Big data-Wikipedia, the free encyclopedia* che su questo tema è affidabile e facilmente comprensibile.

<sup>22</sup> Anche in questo caso la letteratura su dove, e come, siano allocati i server di maggiore potenza utilizzati per i trattamenti di *big data* è, se possibile, ancora più complessa di quella che si limita a indicare quali possano essere le utilità di nuove modalità di trattamento dati.

L'attenzione sul fenomeno dei *big data* connesso al possesso di server di particolare potenza e allo stesso tempo alla possibilità di raccogliere quantità di dati finora impensabili è legato però, nella memoria collettiva, al caso Snowden e all'attività della NSA. Viene cioè normalmente, anche se del tutto erroneamente, connesso ad attività legate alla sicurezza.

Per questo, e anche per la sua capacità di analizzare il fenomeno senza eccessivi allarmismi, si veda il recentissimo M.S. BROWN, *NSA Mass Surveillance: Biggest Big Data Story-Forbes*, in *www.forbes.com*, 27 agosto 2015. Della stessa autrice, M.S. BROWN, si possono utilmente vedere anche *Data Mining for Dummies* e *Storytelling for Data Analysts and Storytelling for Tech workshops*, entrambi rintracciabili su *www.metabrown.com*.

<sup>23</sup> Cfr. G. GREENWALD, *No place to hide, Edward Snowden e la sorveglianza di massa*, Rizzoli, Milano, 2014.

Le cose si complicano ancora, poi, se teniamo conto di altri aspetti, alcuni già presenti in modo capillare nel nostro sistema delle telecomunicazioni, e altri in fase di avanzato sviluppo.

Il primo fa riferimento all'enorme dimensione che ha assunto il fenomeno delle "app", moltissime delle quali gestite da singoli fornitori di servizi che utilizzano le piattaforme OTT<sup>24</sup>.

Ovviamente anche l'uso di queste app determina necessariamente l'invio, la raccolta, il trattamento di dati degli utenti in una quantità variabile ma comunque sempre cospicua, e spesso addirittura senza interruzioni. È generalmente difficile, spesso impossibile, conoscere i titolari e, soprattutto, le modalità di uso e conservazione dei dati raccolti nonché le finalità per le quali essi sono trattati, anche al di fuori del singolo servizio di volta in volta prestato.

Il secondo fenomeno, legato in particolare al diffondersi dell'Internet delle cose (IOT), riguarda i nuovi aspetti di una tecnologia che ha l'obiettivo di consentire sempre di più che oggetti diversi tra loro possano dialogare.

Si tratta di una tecnologia e di un campo di applicazioni relativamente nuovi che superano non solo i sistemi tradizionali di relazione tra le cose (la chiave che gira nella toppa e apre la serratura, per esempio), ma anche i sistemi più recenti, legati comunque al contatto fisico fra le cose (il badge che registra l'ingresso e l'uscita dal luogo di lavoro, per fare un esempio simile al precedente) o al contatto tramite radio frequenza proprio dei sistemi RFID<sup>25</sup>.

---

<sup>24</sup> Ovviamente qui per "app" si intende il neologismo col quale si indicano le applicazioni informatiche per dispositivi mobili come *smartphone* o *tablet*. Come è noto le app a loro volta si suddividono in "app native" e "web app".

Le prime sono installate e utilizzate direttamente sul dispositivo mobile che si possiede e di norma il costruttore del sistema operativo risponde del loro funzionamento, anche sotto il profilo dei dati trattati. Una *web app* invece è un collegamento verso un applicativo remoto, che non incide che in modo minimo sulle capacità di memoria e di elaborazione del dispositivo, in quanto l'interfaccia utente dell'applicazione è collocata su server molto lontani. Queste app operano esclusivamente via Internet, dipendono dalla connessione e sono certamente quelle di maggiore pericolosità perché è difficilissimo sapere con sufficiente certezza chi è, e dove si trova, il responsabile dei trattamenti di dati che il loro uso comporta, per quanto tempo questi dati sono conservati e come sono protetti. Anche su questa tematica la letteratura, specialmente in lingua inglese, è sterminata. Qui ci si limita a indicare S. GULIZIA, *App native contro web app: quali sono meglio?*, in *Wired*, 2 aprile 2012.

<sup>25</sup> Per quanto l'attenzione sull'uso e sui conseguenti pericoli delle RFID in ordine alla privacy sia relativamente recente (basti citare la Conferenza annuale di primavera delle Autorità di protezione dati europee (*Spring Conference*) tenutosi a Martigny nel 2006, dove chi scrive presentò una relazione dal titolo *La sfida della tecnologia Rfid*), la tematica legata a questa tecnologia, specialmente in campo militare, è assai risalente. Essa, infatti, è stata già oggetto del noto volume di H. STOCKMAN, *Communication by Means of Reflected Power*, pubblicato nel 1948.

Tuttavia, nei primi anni 2000, il tema ha avuto una particolare ripesa di attenzione, da un lato legata all'abbattimento dei costi di uso, e dall'altro, alle preoccupazioni legate appunto alla privacy. Si veda per tutti C.M. ROBERTS, *Radio frequency identification (RFID)*, in *Otago University Research Archive*, <http://hdl.handle.net/10523/1247>, 2005.

Sul tema si veda anche Working Party 29, *Working document in data protection issues related to RFID technology*, 19 gennaio 2005 (WP n. 105), nonché Working Party 29, *Results of the*



Caratteristica della tecnologia IOT è infatti che le cose dialogano attraverso la rete, con segnali e informazioni trasmessi grazie a questa<sup>26</sup>.

Ovviamente, alla base di qualunque sistema di IOT, e del suo funzionamento, c'è sempre la volontà umana che ne progetta la realizzazione e che dà i comandi che ne assicurano il funzionamento. Il dialogo tra le cose può avvenire a seguito di un impulso iniziale che è sufficiente ad attivare tutto il sistema, ovvero grazie a una pluralità di impulsi finalizzata a sincronizzare le cose tra loro: quello che conta è che questi impulsi null'altro sono che una serie di dati che arrivano in rete e attraverso la rete operano.

In questi casi è evidente che il sistema presenta maggiori problematiche per la protezione dei dati e di conseguenza innalza anche la soglia della necessità di adeguate norme di protezione.

Attraverso queste forme di trattamento dei dati, basate su una sorta di “catena di Sant’Antonio” fra cose che dialogano tramite la rete, i soggetti che potenzialmente possono accedere ai segnali, registrarli e trattarli per altre e diverse finalità da quelle previste, sono moltissimi. Con la conseguenza che possono sorgere problemi estremamente delicati, persino in termini di sicurezza sul funzionamento di questi sistemi e delle persone che li utilizzano o ne sono oggetto.

Sullo sfondo di questo sempre più complesso panorama, qui descritto solo a grandissime linee e in modo molto superficiale, si collocano infine alcuni pericoli crescenti per intensità e sempre più rilevanti anche rispetto al tema della protezione di dati.

Il primo pericolo, fra i tanti che si possono intravedere, sta innanzitutto nel furto di dati da parte di chi non ha diritto di conoscerli, o di un loro uso posto in essere da parte di chi utilizza illecitamente dati acquisiti.

---

*Public Consultation on Article 29 Working Document 105 on Data Protection Issues Related RFID Technology*, 28 luglio 2005 (WP n. 29).

<sup>26</sup> Con l'espressione Internet delle cose o meglio *Internet of Things* (IOT), si intende un network tra oggetti fisici connessi attraverso sistemi elettronici, *software* e sensori, accessibile in modo che da remoto il sistema possa essere avviato, corretto, orientato. In sostanza, un insieme di *device* basati sulla infrastruttura dell'*International Telecommunication Union's Global standards Initiative*. Il sistema opera una interconnessione fra oggetti fisici e sistemi *computer-based* che ha come scopo di aumentare l'efficienza, la qualità e l'economicità dell'attività svolta dalle cose tra loro interconnesse. Il termine è stato coniato dall'impresario inglese Kevin Ashton nel 1999 e oggi la realtà va già oltre le interconnessioni “*machine to machine*”, M2M, per estendersi a una grande varietà di protocolli, domini e applicazioni. Ovviamente, nel periodo più recente l'Internet delle cose sta evolvendo anche verso sistemi detti “intelligenti” perché capaci di autocontrollo senza bisogno di ricevere istruzioni attraverso la rete. Grazie a questi sistemi e a quelli in corso di sperimentazione, si parla spesso anche di Intelligenza Artificiale. In ogni caso, senza voler in questa sede andare oltre, basterà dire che secondo studi recenti l'Internet delle cose potrebbe connettere già oggi da 50 a 100 trilioni di oggetti, mantenendo la capacità di controllo di tutte le interconnessioni che collegano una così sterminata quantità di terminali operanti nell'ambito di una non meno sterminata quantità di sistemi. Tutto questo sta ponendo nuovi e complicati problemi, anche relativi alla privacy e alla protezione dei dati, messi in luce da numerosi studiosi quali Peter-Paul Verbeek, professore all'Università di Twente in Olanda, Justin Brookman, del Center for Democracy and Technology, Tim O'Reilly e l'American Civil Liberties Union (ACLU).

Il secondo pericolo riguarda il rischio di hackeraggio<sup>27</sup> non solo dei dati ma anche dei sistemi che li trattano. Un rischio che può verificarsi in una qualunque delle fasi dei procedimenti inevitabilmente complessi in cui si articolano i trattamenti.

La conseguenza è che i dati possono essere manipolati, falsificati, diffusi illecitamente, assemblati in modo da trarre da essi informazioni ulteriori e diverse da quelle in essi contenute, spesso anche gravemente dannose per le persone alle quali si riferiscono.

Vi è infine un pericolo che va profilandosi come il più grave di tutti e che va ben oltre il tema della protezione dei dati personali, anche se in parte è a questo tema connesso.

Si tratta dell'eventualità, molto più concreta di quanto si pensi, che attraverso l'hackeraggio dei sistemi di trasmissione dati necessari affinché possano funzionare le applicazioni legate all'*Internet of Things*, gli hacker possano modificare i comportamenti e le modalità di uso di queste, fino a provocare anche rischi reali per la vita delle persone coinvolte.

## **6. La difficoltà di garantire in modo efficace la protezione dei dati personali nel mondo di oggi e di domani**

Come si può vedere da quanto fin qui detto, rendere effettivo il diritto alla protezione dei dati personali, così come tutelare i dati nell'interesse pubblico generale, è cosa sempre più complessa e, allo stesso tempo, sempre più importante. Siamo in presenza di un fenomeno che invoca un diritto fondamentale di libertà e una tutela vitale per una società democratica, e che è destinato inevitabilmente a crescere sempre più di importanza man mano che la società digitale e i mille servizi che essa offre, e offrirà ancora di più in futuro, si sviluppano.

In questo quadro un'attenzione particolare va dedicata al rapporto tra la protezione dei dati personali e la manifestazione del pensiero, la libertà di stampa come diritto ad informare ed essere informati, la ricerca e la conservazione della memoria collettiva.

Sono tutti aspetti dell'attività umana che la nostra cultura, nata dalle lotte di religione<sup>28</sup> e dalle grandi Rivoluzioni del settecento<sup>29</sup>, considera come drit-

---

<sup>27</sup> *Hacker* è termine usato per indicare una persona esperta di sistemi informatici in grado di introdursi anche in reti protette, mentre hackeraggio (*hacking*) sta ad indicare l'insieme dei metodi, tecniche e operazioni volte a accedere a un sistema hardware o software, conoscere i dati custoditi o trattati ed, eventualmente, modificarli.

<sup>28</sup> La libertà di manifestazione del pensiero è strettamente intrecciata con la libertà religiosa, che implica anche, come dice l'art. 19 della nostra Costituzione, "*il diritto di professare liberamente la propria fede religiosa, in qualsiasi forma, individuale o associata, di farne propaganda e di esercitarne in privato o in pubblico il culto, purché non si tratti di riti contrari al buon costume*".

<sup>29</sup> Il riferimento è ovviamente alle tre grandi Rivoluzioni del Settecento, legate all'Illuminismo e

ti e libertà fondamentali e che hanno ora al centro il tema dei dati personali, così come esso è considerato nell'art. 8 della Carta dei diritti fondamentali dell'Unione europea.

La manifestazione del pensiero, infatti, è per definizione anche il riflesso della comunicazione e diffusione ad altri di informazioni su se stessi, fosse anche soltanto ciò che noi stessi riteniamo di voler comunicare relativamente a quello che pensiamo. La libertà di stampa, intesa come diritto/dovere ad informare e diritto ad essere informati, è, per definizione, il fulcro delle libertà democratiche, essendo condizione essenziale affinché si formi quella che, a suo tempo, fu definita pubblica opinione e che oggi, immersi come siamo nei *social network*, definiremmo la partecipazione collettiva e circolare delle persone alle vicende che accadono nel mondo.

Informare e informarsi significa però diffondere o acquisire notizie che riguardano anche la vita delle persone e la realtà che le circonda. Dunque, nulla più della libertà di stampa, intesa come libertà di informare, informarsi ed essere informati, tocca e coinvolge la protezione dei dati personali considerati come informazioni che riguardano persone identificate o identificabili.

Anche l'attività di ricerca e, in generale, l'attività scientifica, presentano aspetti che toccano profondamente la tematica delle libertà fondamentali nel loro rapporto con la protezione dei dati.

Siamo infatti di fronte a diritti fondamentali riconosciuti da tempo nelle nostre società, quali la libertà di ricerca scientifica, insegnamento, creazione artistica, che coinvolgono necessariamente l'utilizzazione di informazioni che riguardano persone, e dunque la protezione dei dati personali<sup>30</sup>. Dal ritratto alla biografia, dalle analisi delle terapie sui pazienti alla raccolta di dati statistici e quali-quantitativi sui comportamenti degli individui e dei gruppi sociali, fino alla registrazione e analisi dei dati utilizzate per poter compiere di scelte consapevoli: sono tutte attività che implicano uso di dati, quasi sempre personali, e che, al tempo stesso, ne producono di nuovi.

---

alle scoperte scientifiche, ma anche figlie ciascuna di una propria storia. Il vero filo rosso che lega le tre Rivoluzioni è infatti quello della limitazione del potere sovrano al quale sono contrapposti i diritti dei cittadini. Fenomeno questo che, sia pure con forme diverse, si riscontra sia nella Rivoluzione inglese, col *Bill (or Declaration) of rights* del 1689, che in quella americana, con la *Dichiarazione di indipendenza* del 4 luglio 1776 e coi primi dodici articoli del *Bill of rights* del 1789, che, infine, in quella francese, con la *Dichiarazione dei diritti dell'uomo e del cittadino* del 26 agosto 1789.

<sup>30</sup> Su questi temi una delle questioni più dibattute, e tutt'ora non risolta opportunamente né a livello italiano né a livello europeo, è come si concilia il diritto di autore con la sua protezione in rete. Su questo tema i contributi, anche nella dottrina italiana, sono numerosissimi. Qui ci si limita a ricordare F. PIZZETTI (a cura di), *"I diritti nella rete della rete". Il caso del diritto di autore*, con contributi di L. Ferola, M. Orofino, O. Pollicino, M. Siano, Giappichelli, Torino, 2011.

## 7. Il diritto alla conservazione dei dati personali e delle notizie (diritto alla “memoria”) e l’opposto diritto alla cancellazione dei dati non più necessari (diritto all’“oblio”)

Infine, sono centrali nella nostra epoca sia il diritto alla conservazione dei dati e della memoria in essi racchiusa, che quello alla loro accessibilità e, quando essi non siano più necessari, alla loro cancellazione.

Viene qui in gioco il diritto alla memoria, da un lato, il diritto all’oblio dall’altro.

Non vi è dubbio, infatti, che da sempre gli esseri umani vivono una contraddizione “esistenziale”. Da un lato, essi aspirano all’immortalità e, sapendo di non poterla avere, cercano di lasciare il più a lungo possibile memoria di sé come unico modo per prolungare la propria vita, o meglio il ricordo nel futuro del fatto che essi sono esistiti, e di ciò che hanno realizzato<sup>31</sup>. È su questa spinta che si fonda il desiderio di gloria, la ricerca di fama e la proliferazione di affreschi, ritratti, monumenti, che ricordano personaggi e vicende delle quali si vuole trasmettere ai posteri il più a lungo possibile memoria. La stessa cosa può dirsi per le autobiografie<sup>32</sup>, per i memoriali, per le campagne militari scritte dai generali che ne sono stati i protagonisti<sup>33</sup>.

All’opposto, ogni persona umana ha anche il terrore che ogni atto negativo compiuto nel corso della propria esistenza possa essere ricordato per sempre, o almeno fino a quando è in vita e lo sono quelli che ne hanno memoria.

Per definizione, da Adamo ed Eva che, subito dopo aver mangiato la mela, cercarono di nascondersi l’uno all’altra facendosi cinture di foglie e di celarsi a Dio che li chiamava nel giardino terrestre<sup>34</sup>, tutti gli esseri umani hanno bisogno di poter far dimenticare i propri comportamenti negativi, e persino di riuscire a farli dimenticare a sé stessi.

Dunque, anche qui ci troviamo di fronte a un nodo centrale: il rapporto tra desiderio di essere ricordati e quello di essere dimenticati<sup>35</sup>.

<sup>31</sup> Le stesse attenzioni e cure poste nei secoli alle tecniche di inumazione e alle scritte e lapidi funerarie sono la migliore testimonianza di tutto questo. Del resto, una parte amplissima di ciò che noi sappiamo del nostro passato e delle civiltà che ci hanno preceduto deriva proprio dallo studio delle tombe rinvenute in tutte le parti del mondo e testimoni delle più diverse civiltà.

<sup>32</sup> Come non pensare, ad esempio, al memoriale di Napoleone da lui dettato a S. Elena e pubblicato poi da Emmanuel de las Cases col titolo *Memoriale di Sant’Elena*.

<sup>33</sup> Come non pensare a Giulio Cesare e al suo *De Bello Gallico*?

<sup>34</sup> *Genesi* 3,8-21.

<sup>35</sup> Il tema del c.d. diritto all’oblio è fra quelli che più hanno interessato il dibattito sul rapporto tra tutela dei diritti e mondo della rete, soprattutto con riguardo al motore di ricerca. Si tornerà più volte su questo tema, anche perché il nuovo Regolamento europeo ha una norma apposita, anche se essa è intitolata “*right to erasure*”, dunque diritto alla deindicizzazione. Questa tematica è stata al centro anche di una recente sentenza della CGUE, (Grande Sessione), del 13 maggio 2014, causa C-131/12, *Google Spain SL, Google Inc. c. Agencia Española de Protección de Datos (AEPD), Mario Costeja Gonzalez*. Cfr. su questo F. PIZZETTI (a cura di), *Internet e*