LUISS Guido Carli
LIBERA UNIVERSITÀ INTERNAZIONALE DEGLI STUDI SOCIALI

DIPARTIMENTO DI SCIENZE POLITICHE

Cattedra di Diritto dell'informazione e della comunicazione (C.P.)

L' EVOLUZIONE E LA DISCIPLINA DEL TRATTAMENTO DEI DATI SENSIBILI ONLINE E OFFLINE

RELATORE
Chiar.mo.Prof.
Pietro Santo Leopoldo Falletta

CANDIDATA
Federica Notari
Matr. 622992

CORRELATORE
Chiar.mo.Prof.
Michele Sorice

ANNO ACCADEMICO 2014/2015

Indice

Introduzione

Oggetto del presente elaborato è l'analisi della disciplina dei cd. *dati sensibili*, ossia tutte quelle informazioni che ricadono nella sfera più intima dell'individuo e che dunque necessitano di una tutela maggiormente incisiva rispetto alla categoria più generale dei dati personali. Lo scopo è quello di prendere in considerazione sia la normativa europea sia quella italiana in materia di dati sensibili, esaminando anche il trattamento nell'ambito della realtà *online*, caratterizzata da una maggiore invasività nelle informazioni che riguardano gli utenti nonché da una mancanza di regole specifiche che possono applicarsi al *web* in caso di violazioni della disciplina in esame. A tal proposito, nell'ultimo capitolo, saranno analizzate alcune tra le più rilevanti pronunce della giurisprudenza europea ed interna intervenute, in particolare, in materia di nuove responsabilità in rete.

Nello specifico, l'elaborato risulta suddiviso in tre parti.

Nella prima parte, sarà analizzata l'evoluzione della normativa in materia di dati sensibili nel contesto europeo, sia in sede di Consiglio d'Europa, che in seno all'Unione europea. Innanzitutto, si partirà dalla nascita del concetto di *privacy*[1], in quanto le informazioni particolarmente riservate di cui si parla ricadono nella dimensione più generale della tutela alla *privacy*, nelle sue molteplici accezioni. In primo luogo, sarà analizzato come il Consiglio d'Europa si è occupato del diritto in questione: prima, attraverso la Convenzione europea dei diritti dell'uomo e delle libertà fondamentali, che all'art 8 ha previsto un *diritto al rispetto della vita privata e familiare* e l'interpretazione che di tale diritto ne ha dato la Corte Edu; successivamente, con la Convenzione n. 108 del 1981 che ha contemplato espressamente una disciplina specifica per categorie "speciali" di dati che sono oggetto del presente elaborato. In secondo luogo, sarà mostrato come l'Unione europea abbia dato particolare rilievo al tema attraverso la previsione di una normativa applicabile alla protezione dei dati personali con la direttiva *privacy* 46/95/CE, recepita in tutti gli Stati membri dell'Unione, che, sul modello della Convenzione n. 108, ha definito un regime per i dati sensibili all'art. 8. Come si vedrà, l'Unione si è occupata della questione anche in alcune previsioni normative previste dai Trattati, da ultimo quello di Lisbona e nella Carta dei diritti fondamentali dell'Unione definendo per la prima volta un *diritto alla protezione dei dati a carattere personale.* Infine, una particolare attenzione, a conclusione del paragrafo verrà data al nuovo pacchetto di regole sulla *privacy* proposto dalla Commissione europea nel 2012 e che, se sarà definitivamente approvato nei prossimi mesi, riformerà e attualizzerà la materia attraverso numerose disposizioni a garanzia di

[1] Come si vedrà nel primo capitolo, si fa tradizionalmente risalire l'origine del concetto di *privacy* inteso quale diritto ad essere lasciato solo (*the right to be let alone*) ad un saggio pubblicato a Boston da due avvocati, Samuel D. Warren e Louis D. Brandeis, intitolato *"The Right to privacy".*

una protezione maggiore delle informazioni personali presenti sul *web* e sarà direttamente applicabile in tutti gli Stati membri dell'Unione.

Nella seconda parte, si vedrà come l'Italia abbia affrontato con ritardo il tema della tutela della *privacy.* In assenza di un fondamento costituzionale del diritto in questione[2], sarà soltanto attraverso la legge n. 675 del 1996 che sarà prevista per la prima volta una disciplina completa e specificamente dedicata al trattamento dei dati sensibili, ai sensi dell'art. 22 della stessa legge. Nel prosieguo, si vedrà come tale normativa è stata abrogata dal *Codice della privacy*[3] - attualmente in vigore in attesa dell'approvazione finale delle nuove regole sulla *privacy* da parte dell'Unione - che, più attento al cambiamento del processo tecnologico, ha riformato la materia. In particolare, con riferimento ai *dati sensibili*, il Codice, pur riprendendo il doppio regime garantistico previsto dalla normativa previgente[4], ha distinto i casi in cui il trattamento di tali dati venga effettuato da soggetti pubblici e da soggetti privati. Inoltre, sempre nell'ottica di una richiesta di maggiore protezione di tali informazioni, saranno considerate anche le cd. *autorizzazioni generali* che il Garante della *privacy* ha adottato in riferimento ai *dati sensibili* e *giudiziari* e l'attenzione posta dalla normativa ai dati idonei a rivelare lo stato di salute e la vita sessuale degli individui, identificati come dati *supersensibili.*

Infine, nella terza parte, sarà considerato come sul *web* sia messa maggiormente a rischio la tutela dei dati personali e di quelli sensibili. Dapprima saranno analizzati i nuovi profili di responsabilità per i contenuti che contengono informazioni personali immessi *online* nei confronti dei fornitori della rete, i cd. *Internet service provider (ISP)* per i quali tanto la normativa europea quanto quella italiana hanno previsto una disciplina specifica: la prima nella direttiva *e-commerce* n. 2000/31/CE, la seconda, in recepimento di quest'ultima, nel decreto legislativo n. 70 del 2003. In secondo luogo, saranno analizzati alcuni casi di cui si è occupata la giurisprudenza italiana ed europea, contemperando di volta in volta il diritto alla riservatezza con l'attività di impresa dei fornitori della rete e le relative responsabilità poste a loro carico. Un intervento particolarmente significativo in tal senso che sarà affrontato è il caso *Google Vs Vividown*, che ha riguardato un trattamento illecito di dati sensibili contenuti in un video pubblicato *online* da alcuni utenti e in cui la Cassazione, al termine di una complicata vicenda giudiziaria, ha considerato il *provider*, nel caso di specie *Google,* irresponsabile per tale trattamento ai sensi della normativa in materia vigente. Negli altri casi giurisprudenziali considerati, invece, soprattutto la Corte di Giustizia dell'Unione europea sembra aver fatto

[2] Tuttavia nel secondo capitolo si vedrà come parte della dottrina abbia ritrovato un fondamento implicito del diritto alla *privacy* in alcune disposizioni costituzionali.

[3] Ci si riferisce al decreto legislativo del 30 giugno 2003, n. 196.

[4] Si fa riferimento al consenso scritto del soggetto interessato e della previa autorizzazione del Garante della *privacy.*

prevalere il rispetto alla protezione dei dati personali piuttosto che l'attività di impresa[5], soprattutto nell'ultima pronuncia analizzata, la cd. *sentenza Schrems* in cui la Corte ha invalidato una decisione della Commissione del 2000[6] che premetteva il trasferimento verso gli Stati Uniti dei dati personali provenienti dall'Europa facendo dunque prevalere il diritto alla *privacy* dei propri cittadini. Relativamente a tale aspetto, nelle conclusioni saranno prese in considerazione le prospettive che si apriranno nel periodo *post – Safe Harbor* con la necessità della previsione di un nuovo accordo tra Unione europea e Stati Uniti per raggiungere quell' *adeguato* livello di protezione dei dati personali che il cd. *approdo sicuro* non aveva garantito secondo la Corte di Giustizia.

[5] Come si vedrà nel terzo capitolo, si fa riferimento al caso *Digital Rights Ireland* e *Google Spain.*

[6] Il cd. *Safe Harbor* è l'accordo tra Unione Europa e Stati Uniti che consentiva alle imprese americane di conservare i dati personali degli utenti europei anche negli Stati Uniti.

Capitolo Primo

La disciplina del trattamento dei dati personali e sensibili nel contesto europeo: un problema di bilanciamento tra interessi contrapposti

1. Una tutela rafforzata per dati "particolari" alla luce delle proposte di riforma della Commissione europea

"Senza una forte tutela delle informazioni che le riguardano, le persone rischiano sempre di più d'essere discriminate per le loro opinioni, credenze religiose, condizioni di salute: la privacy si presenta così come un elemento fondamentale dalla società dell'eguaglianza. Senza una forte tutela dei dati riguardanti le convinzioni politiche o l'appartenenza a partiti, sindacati, associazioni, i cittadini rischiano d'essere esclusi dai processi democratici: così la privacy diventa una condizione essenziale per essere inclusi nella società della partecipazione."

Sono queste le parole di Stefano Rodotà nel discorso conclusivo tenutosi durante la Conferenza internazionale sulla protezione dei dati del 2004[7], che dimostrano l'importanza data ad alcune tipologie di "informazioni" personali: quelle, appunto, concernenti le opinioni (politiche), credenze religiose, quelle volte a rivelare le condizioni di salute o l'adesione a partiti politici, sindacati, organizzazioni religiose. Queste rientrano nella categoria dei cd. *dati sensibili* come definiti dal Codice in materia di protezione dei dati personali[8] ma, come si vedrà nel presente elaborato, considerati in una pluralità di fonti normative anche a livello internazionale e soprattutto europeo. Essi, incidendo sulla sfera più intima dell'individuo, necessitano di una tutela maggiore rispetto alle categorie "normali" di dati personali soprattutto con l'avvento del *web* e delle nuove tecnologie che mettono sempre di più a dura prova il livello di protezione di tali informazioni. L' attenzione particolare rivolta a tale tipologia di dati è stata messa in luce anche dalla Commissione europea che ha proposto nel gennaio 2012 una riforma globale delle norme sulla *privacy* introdotte nel 1995 e che potrebbe entrare in vigore in tutti gli Stati membri dell'Unione nei prossimi mesi, come sarà dettagliatamente trattato nel paragrafo conclusivo del presente capitolo, ponendosi il compito di rafforzare i diritti alla privacy *online* e stimolare

[7] Si tratta della Conferenza internazionale sulla protezione dei dati (26th International Conference on Privacy and Personal Data Protection Data) del 14,15 e 16 settembre 2004 a Cracovia, in Polonia. Il discorso integrale di Rodotà è disponibile su *www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1049293.*

[8] La definizione di dato sensibile è presente all'art. 4 lettera d) del *Codice in materia di protezione dei dati personali*, adottato con decreto Legislativo 30 giugno 2003, n. 196. Per un'analisi della disciplina del *Codice* si rinvia al capitolo successivo.

l'economia digitale europea: dando attenzione a tutti gli aspetti che ricadono nell'ambito della *privacy*, la Commissione ha dedicato una specifica attenzione alla disciplina dei cd. *sensitive data* per i quali prevede l'applicazione di regole più stringenti rispetto ai "generali" dati personali[9].

Infatti, tanto nella normativa europea quanto in quella nazionale i dati personali vengono pertanto divisi in due grandi gruppi: quelli *comuni,* che riguardano in linea generale la persona (quali il numero telefonico, indirizzo, ma anche una fotografia, la voce, il reddito percepito, etc.) e quelli *particolari*, ai quali facciamo più specificamente riferimento nel presente elaborato, che si riferiscono a determinati aspetti della persona il cui trattamento indiscriminato potrebbe danneggiare l'immagine, la vita di relazione e anche la salute psico-fisica dell'individuo[10]. Pertanto, proprio perché rientranti nella categoria generale di dati personali, tutte le considerazioni riportate quì di seguito si riferiranno prima di tutto all'evoluzione storica e normativa del concetto di *privacy latu sensu* impiegato in ambito europeo e nazionale.

2. Il riconoscimento della *privacy* nel contesto europeo come libertà positiva e il problema del bilanciamento tra interessi contrapposti

"I mutamenti politici, sociali ed economici obbligano al riconoscimento di nuovi diritti"[11]*:* è in questi ultimi a doversi ritrovare il primo "pubblico" riconoscimento della *privacy*, secondo un saggio pubblicato nel 1890 da due avvocati di Boston, S. D. Warren e L. D. Brandeis.

Riprendendo infatti anche quanto sostenuto da Norberto Bobbio[12], i diritti umani sono capaci di rinnovarsi nel corso del tempo grazie a fattori storici, politici, sociali senza però portare a "sostituzioni" tra diritti ma solo ad accumulazioni o anche a riformulazioni di uno stesso diritto che acquisisce nuove e diverse manifestazioni attraverso cambiamenti storici[13] e tecnologici. È

[9] Nel testo di riforma in materia di protezione dei dati personali prospettato dalla Commissione nel 2012, una specifica sezione è dedicata ad alcune categorie di dati. In particolare si tratta dei cd. *sensitive data*, in particolare*:" Very stringent rules apply to processing sensitive data: data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs trade union membership, data concerning health or sexual preference. In principle, such data cannot be processed. Derogation is tolerated under very specific circumstances. These circumstances include the data subject's explicit consent to process sensitive data, the processing of data mandated by employment law, where it may be impossible for the data subject to consent (e.g. blood test to the victim of a road accident), processing of data has been publicly announced by the data subject or processing of data about members by trade unions, political parties or churches. Member states may provide for additional exceptions for reasons of substantial public interest."* Per maggiori informazioni sull'iniziativa della Commissione del 2012 si rinvia a *www.ec.europa.eu/justice/data-protection/.*

[10] J. Monducci, *Diritti della persona e trattamento dei dati particolari*, Milano, 2003, Introduzione.

[11] L. D. Brandeis, S. D. Warren, *The Right to Privacy*, in *Harvard Law Review*, 1890, p.193.

[12] N. Bobbio, *L'età dei diritti*, Torino, 1990 scrive che i diritti umani sono *"sono diritti storici, cioè nati in certe circostanze, contrassegnate da lotte per la difesa di nuove libertà contro vecchi poteri, gradualmente, non tutti in una volta e non una volta per sempre".*

[13] S. Rodotà, *Apologia dei diritti,* La Stampa, 2 luglio 2002 in *www.ossimoro.it/diritti1.htm.*

proprio grazie alla dinamicità che contraddistingue i diritti[14] che, ai fini della nostra analisi, possono mostrarsi le diverse accezioni di *privacy* che si sono susseguite nel corso del tempo senza portare necessariamente ad una sostituzione di una rispetto ad un'altra: come diritto ad essere lasciati soli, come possibilità di ciascuno di controllare l'uso delle informazioni che lo riguardano oppure ancora come "mezzo" per tutelare la dignità umana e il suo sviluppo all'interno della società, che come si vedrà nel prossimo capitolo, si ritroverà nel *Codice della privacy*.

Volendo dedicare attenzione al concetto della *privacy* così come viene inteso nel contesto europeo caratterizzato da un'accezione diversa rispetto alla matrice di stampo anglosassone, è tuttavia doveroso risalire alle sue origini. Ritornando infatti al saggio del 1890, intitolato *The Right to Privacy*, questo nasceva come reazione alle notizie indiscrete pubblicate dall' *Evening Gazette* di Boston sulle amicizie della moglie di Warren, figlia di un noto senatore e sulle nozze della figlia di Warren. Per la prima volta si pose quella che sarebbe stata successivamente la questione alla base del tema della *privacy*, in quanto i due avvocati si trovarono a dover effettuare un *bilanciamento tra interessi contrapposti*: quello di rendere pubbliche le informazioni riguardanti la vita personale di un individuo o quello di tutelare tali informazioni dall'invadenza altrui. Nel saggio scritto a quattro mani venne fuori una sistematica discussione sul *diritto alla privacy* tenendo conto anche dell'impatto dell'innovazione tecnologica[15] su tale nuovo diritto e mettendo in luce come alcune invenzioni del loro tempo potessero dar luogo a tutta una serie di violazioni della riservatezza dell'individuo, rendendo pubblici particolari sulla vita altrui. Il contenuto della *privacy* veniva così a coincidere con quella che sarebbe diventata poi la sua componente principale: il diritto di essere lasciati soli, *the right to be let alone.* Tale espressione non è da intendersi come astratta aspirazione di una persona ad essere lasciata sola, ma come la possibilità di decidere se portare o meno alla conoscenza altrui i pensieri e le emozioni personali[16]. Tuttavia, pur avendo tale elaborazione concettuale una portata innovativa[17], la *privacy* continuava ad essere legata ad uno schema classico della cultura

[14] A tal proposito di parla di tre, o secondo alcuni, anche quattro generazioni di diritti: la prima porta alla nascita, alla fine del Settecento, dei diritti civili e politici; la seconda tra Ottocento e Novecento a quelli sociali e infine quelli di nuova generazione. Cfr. E. Brugiotti, *La privacy attraverso le "generazioni dei diritti". Dalla tutela della riservatezza alla protezione dei dati personali fino alla tutela del corpo elettronico.,* in *www.dirittifondamentali.it/unicas_df/index.php/11-dottrina/118-la-privacy-attraverso-le-generazioni-dei-diritti-dalla-tutela-della-riservatezza-alla-protezione-dei-dati-personali-fino-alla-tutela-del-corpo-elettronico,* 2013, pp. 1-5.

[15] In particolare, poiché le indiscrezioni sulla vita di Warren erano state pubblicate su un quotidiano dell'epoca, le considerazioni dei due giuristi vertevano sulla stampa a rotativa. Oggi, lo stesso ragionamento può essere facilmente esteso a tutte le nuove tecnologie arrivando alla nascita del *web* e della sua incidenza sulla tutela della sfera privata come si dirà successivamente.

[16] G. Gardini, *Le regole dell'informazione. Principi giuridici, strumenti, casi.,* Milano, 2009, p. 241.

[17] Poiché aveva attribuito alla *privacy* la consistenza di un vero e proprio diritto della personalità, risarcibile in caso di lesione.

giuridica: la logica della proprietà privata, basata sul rispetto dei "confini" senza invadere lo spazio altrui, stesso ragionamento applicato dalla nuova classe borghese per ottenere un uguale riconoscimento del proprio spazio interiore.[18] Nell'interpretazione seguita dai due giuristi e poi quella propria della dottrina statunitense, la *privacy* era concepita come una delle c.d. *"libertà negative"*, intese come tutte le rivendicazioni rivolte a respingere lo Stato dalle scelte individuali[19] oltre anche dalle ingerenze esterne di tipo "privato".

È nella realtà europea[20] che, nel corso del tempo, può parlarsi dello sviluppo di una *libertà* o *diritto positivo,* insistendo sulla possibilità dell'individuo di scegliere senza alcun condizionamento attraverso la previsione di un'accezione più socio-relazionale della *privacy* con una maggiore attenzione alla tutela dei dati personali e quindi ai connotati informazionali del diritto in oggetto. La "compresenza" di "vecchi" e "nuovi" diritti di cui si è detto, e quindi anche del riconoscimento della *privacy*, è da ricercarsi attualmente nella Carta dei diritti fondamentali dell'Unione europea, in cui *"il vecchio ed il nuovo riescono ad intrecciarsi perché il catalogo dei diritti guarda ad una persona situata nel suo tempo e nella sua condizione concreta, calata nella realtà ma non dimentica della storia"*[21]. Tale aspetto, fatto proprio dalla Carta dei diritti dell'Unione ma presente sin dalla nascita di un diritto finalizzato alla tutela della vita privata degli individui, rileva per un ulteriore considerazione di cui si è accennato: il problema del bilanciamento tra valori contrapposti. Infatti, l'intervento giurisprudenziale delle due Corti europee nel corso del tempo ha mostrato come sia necessario un contemperamento del diritto in questione con altri valori degni di eguale tutela[22]: si tratta delle "tradizionali" *libertà di espressione, libertà di arti e scienze, protezione della proprietà* ma anche legati alle *esigenze di sicurezza interna* e *ordine pubblico* e i più "nuovi" interessi quali l'*accesso ai documenti* e la *trasparenza amministrativa.*

Dunque, sarà nell'ambito del Consiglio d'Europa che la protezione dei dati personali si qualificherà per la prima volta come diritto della persona e più precisamente come un diritto fondamentale della persona a partire nel 1950 dalla redazione della Convenzione europea per la

[18] S. Rodotà, *Intervista su privacy e libertà*, a cura di Paolo Conti, Roma-Bari, 2005, pp. 8-9.
[19] R. Bin, G. Pitruzzella, *Diritto costituzionale*, Torino, 2014, p. 514.
[20] Ogniqualvolta si parla di "Europa" si fa riferimento sia alle Istituzioni legate sia al Consiglio d'Europa sia all'Unione europea.
[21] S. Rodotà, *op cit.*
[22] Per una disamina sulle decisioni della Corte EDU e della Corte di Giustizia dell'Unione finalizzate a far prevalere un diritto piuttosto che un altro si rimanda a Agenzia dell'Unione europea per i Diritti Fondamentali, *Manuale sul diritto europeo in materia di protezione dei dati*, Belgio, 2014, pp. 22-34. Disponibile su *www.fra.europa.eu/en.*

salvaguardia dei diritti umani e delle libertà fondamentali (CEDU)[23], come si vedrà nel prossimo paragrafo.

3. La *privacy* nell'ambito del Consiglio d' Europa

Prima di mostrare il punto di approdo della *privacy* intesa come tutela dei dati personali nell'ambito più specifico dell'Unione europea con le novità introdotte nel *post*-Lisbona, occorre partire dalla prima ricostruzione di tale tutela avvenuta nel Consiglio d'Europa, la prima organizzazione regionale intergovernativa con vocazione universale nata dopo la Seconda Guerra Mondiale e in particolare attraverso la già citata CEDU[24]. Sarà infatti grazie all'elaborazione giurisprudenziale della Corte di Strasburgo su alcune disposizioni di tale Convenzione che saranno date le basi della nozione "attuale" di tutela dei dati personali ed il fondamento della normativa comunitaria che sarà seguita dall' "altra" Corte europea.[25] Inoltre, nell'ambito del Consiglio d'Europa verrà data per la prima volta attenzione a categorie *"speciali"* di dati personali prevedendo per essi garanzie rafforzate.

3.1 L'art. 8 della Cedu e la sua interpretazione da parte della Corte europea dei diritti dell'uomo

La CEDU rappresenta il primo dei grandi trattati di carattere generale in materia di tutela dei diritti della persona, nonché quello più avanzato sotto il profilo del sistema internazionale di controllo sul rispetto tali diritti[26]. Tra i diritti legati alla persona è stato rinvenuto nell'art.8, da parte della giurisprudenza della Corte di Strasburgo, un riferimento indiretto alla *privacy*. Nel contesto delle istituzioni internazionali, prima ancora, un richiamo di tale concetto era stato ripreso in termini generalissimi ma sufficientemente efficaci all'art. 12 della Dichiarazione Universale dei Diritti dell'Uomo del 1948[27] che parla di un divieto di *"interferenze nella vita*

[23] F. Pizzetti, *La privacy come diritto fondamentale alla protezione dei dati personali nel Trattato di Lisbona,* in P. Bilancia, M. D' Amico (a cura di), *La nuova Europa dopo il Trattato di Lisbona,* Milano, 2009, pp.83-84.
[24] Il Consiglio d'Europa, la principale organizzazione in difesa dei diritti umani del contenente, è composta da 47 Stati membri tra cui i 28 facenti parte dell'Unione europea. Tutti gli Stati membri sono segnatari della CEDU, un trattato concepito per proteggere i diritti umani, la democrazia e lo stato di diritto. La supervisione dell'attuazione della CEDU negli Stati membri spetta alla Corte europea dei diritti dell'uomo con sede a Strasburgo. Il sito del Consiglio d'Europa è consultabile su *www.coe.int/it/web/portal/home*.
[25] Il riferimento è alla Corte di Giustizia dell'Unione europea (CGUE).
[26] M. Pedrazzi, *La Convenzione Europea sui diritti umani e il suo sistema di controllo*, in L. Pineschi (a cura di), *La tutela internazionale dei diritti umani. Norme, garanzie e prassi*, Milano, 2006, p. 236.
[27] F. Macario, *La protezione dei dati personali nel diritto privato* europeo, in V. Cuffaro, V. Ricciuto (a cura di), *La disciplina del trattamento dei dati personali*, Torino, 1997, p.10.

privata" e di lesioni all'onore e alla reputazione ma anche in altri trattati e interventi delle Istituzioni internazionali successivi all'entrata in vigore della CEDU[28].

Ritornando all' 8 Cedu, esso 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.".

La Convenzione, quindi, non contiene una norma specificamente dedicata alla tutela dei dati personali[29], ma la disposizione è riferita al rispetto della vita privata e familiare. Già al secondo comma però si pone un limite alla portata del primo riconoscimento europeo del diritto alla *privacy*, con una serie di deroghe[30] che rischiano di "svuotare" la portata del primo comma, specificando in quali casi la pubblica autorità possa interferire con l'esercizio del diritto alla riservatezza, inteso come diritto a non vedere diffuse notizie concernenti la propria sfera privata. Il riferimento del diritto "*al rispetto della vita privata e familiare*" piuttosto che "*al diritto alla vita privata e familiare*" fa derivare sia un obbligo negativo di non interferenza da parte dello Stato sia un dovere di tipo positivo dello stesso di dover garantire il rispetto effettivo della tutela della vita privata e familiare, nonché quello di prevenire e contrastare eventuali ingerenze da parte di Paesi terzi[31].

L'art. 8 CEDU ha poi un ambito di applicazione particolarmente vasto tale da ricomprendere situazioni giuridiche eterogenee: si estende ad aspetti dell'identità personale di una persona con riferimento al nome quale mezzo di identificazione personale, all'identità, alle relazioni sessuali o all'eventuale comportamento omosessuale che rappresenta una manifestazione privata della personalità umana. A tal proposito, il rispetto della vita privata non si limita solo a tutelare l'integrità morale dell'individuale ma dell'individuo ma anche quella fisica dalle ingerenze che

[28] L'idea della *privacy* compariva infatti all'art.17 della Convenzione Internazionale sui Diritti Civili e Politici entrata in vigore nel 1976. Ancora prima, nel Protocollo di Teheran del 1968 si faceva appello alla necessità di evitare che il progresso tecnologico potesse mettere in percolo diritti e libertà degli individui. Nella stessa direzione. anche le *Guidelines* adottate nel 1980 sotto forma di Raccomandazione dall'OCSE con il compito di approfondire l'incidenza della *privacy* sugli obiettivi economici degli Stati appartenenti a tale Organizzazione.

[29] Al contrario della Convenzione del Consiglio d'Europa del 28 gennaio 1981 e della Carta di Nizza, all'interno delle quali sono presenti riferimenti espliciti alla tutela della *privacy* e dei dati personali.

[30] Il diritto in questione non ha carattere assoluto, infatti le ingerenze da parte della pubblica autorità possono effettuarsi solo se sono previste dalla legge, perseguono uno scopo legittimo e siano necessarie in una società democratica.

[31] C. Pitea, *L'interpretazione evolutiva del diritto al rispetto della vita privata e familiare in materia di libertà sessuale e di tutela dell'ambiente*, in L. Pineschi (a cura di), *op. cit* , p. 428.

possono intaccarla[32].

La giurisprudenza della Corte di Strasburgo ha adattato il testo della Convenzione del 1950 ad una società caratterizzata dall'evoluzione sociale, economica, culturale e tecnologica, estendendo la formula della "vita privata", presente all'art. 8, ed affermando la sua applicabilità anche alle ipotesi di raccolta e conservazione dei dati (seppur concettualmente diverse). Inoltre, tale giurisprudenza riveste un'indubbia importanza ai fini della dell'evoluzione della disposizione in esame e, considerato che, anche l'Unione Europea riconosce e garantisce i diritti inviolabili dell'Uomo quali riconosciuti dalla CEDU, non si può certo prescindere dall'interpretazione che di tali diritti viene fatta proprio dalla Corte Europea di Strasburgo. Si deve tenere anche in considerazione il fatto che la stessa giurisprudenza ha acquisito nuovo interesse alla luce dell'adesione dell'Unione Europea alla CEDU, come sancita dal Trattato di Lisbona, di cui si tratterà nel prosieguo.

Come è stato anticipato, la giurisprudenza della Corte EDU ha approfondito ulteriormente il diritto previsto all'art. 8 della Carta, pronunciandosi in numerosi casi aventi ad oggetto anche situazioni molto eterogenee. Fin dai primi interventi, la Corte è intervenuta ad interpretare in particolare i casi previsti al secondo paragrafo dell'art'8 ossia il meccanismo che legittima le ingerenze statali nella vita privata, che come si è visto, possono avvenire soltanto se considerate necessarie in una società democratica e se finalizzate a perseguire uno degli scopi legittimi espressamente previsti. Innanzitutto, il concetto di *legge* è stato specificato in un caso sottoposto alla Corte nel 1984, in cui ha affermato, come nell'accezione propria del termine, debba ricomprendersi tanto il diritto scritto quanto quello non scritto compresa la prassi amministrativa[33]. Tuttavia, pur affermando che l'ingerenza statale nella vita privata debba avvenire in base ad un fondamento nel diritto interno, questo non si traduce in una semplice conformità della legge al diritto nazionale, ma la stessa legge deve essere sufficientemente accessibile da parte dei cittadini: in questi termini, la Corte enuclea il cd. *principio della qualità della legge*. Oltre, all'accessibilità da parte dei cittadini, tale principio, secondo la Corte, deve prevedere anche la prevedibilità da parte degli stessi ossia permettere di poter prevedere le conseguenze che derivano da una determinata azione. Nel caso di specie, la Corte afferma che la legge debba delimitare l'estensione e le modalità di esercizio del potere statale con precisione sufficiente, al fine di garantire all'individuo una protezione adeguata qualora vi sia un'eccessiva ingerenza da parte dello Stato. Tale interferenza, oltre ad essere prevista dalla legge, deve anche un secondo requisito specificato dalla disposizione in esame: deve essere necessaria in una società democratica. È tale aspetto che implica un bilanciamento, di cui si è detto, tra il diritto

[32] F. Pizzetti, *op. cit.*, p.83.

[33] Corte Edu, Ricorso n. 8691/79, sentenza del 2 agosto 1984, *Malone Vs Regno Unito.*

del singolo e le finalità di interesse pubblico, ma anche un controllo sul rispetto della *proporzionalità* della misura rispetto al fine perseguito. In tal senso, la Corte in un caso del 1976 ha affermato che gli Stati non dispongono di un margine illimitato di discrezionalità nell'assoggettare a misure di sorveglianza segreta, potendo tali interventi distruggere il regime democratico che intendono difendere[34]. Anche il tema del vaglio della proporzionalità dell'ingerenza allo scopo legittimo è stato oggetto di un intervento della Corte in un caso che riguardava il trattamento di informazioni riguardanti lo stato di salute delle persone[35]: la Corte ha osservato come il carattere confidenziale di tale tipo di informazioni costituisca un principio essenziale comune a tutti i Paesi che hanno sottoscritto la Convenzione. Nel caso di specie, la Corte ha ravvisato la violazione dell'art. 8 Cedu in quanto, rendendo pubbliche dette informazioni, non era rispettata la necessità dell'ingerenza in una società democratica pur essendo prevista dalla legge.

Oltre tali interventi giurisprudenziali della Corte intervenuti a specificare quali fossero gli obblighi "negativi" previsti all'art. 8 Cedu, in altri casi, la stessa ha focalizzato l'attenzione sull'esistenza di obblighi di tipo "positivo" posti a carico degli Stati finalizzati ad assicurare l'effettivo rispetto del diritto in questione e a prevenire e a contrastare le interferenze illegittime da parte di soggetti terzi. In tal senso, la Corte ha affermato, ad esempio, come tra di questi rientrasse l'obbligo nei confronti degli Stati di consentire l'accesso degli interessati alle informazioni personali riguardanti la propria vita privata e un diniego in tal senso rappresenterebbe una violazione dell'art. 8 Cedu[36]; oppure, il mettere a disposizione del soggetto leso da una pubblicazione, da parte di uno sconosciuto, di un annuncio su un sito per adulti a nome di un minore, gli strumenti significativi finalizzati all'identificazione e al perseguimento dell'autore dell'annuncio[37].

3.2 La Convenzione di Strasburgo n. 108 del 28.1.1981: il primo riferimento a dati "speciali"

La protezione dei diritti della persona si ritrova nella Convenzione n. 108 *sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale* promossa dal Consiglio d'Europa nel 1981[38] sulla scia delle citate enunciazioni formulate in sede di

[34] Corte Edu, sentenza del 6 settembre del 1978, *Klauss Vs Repubblica Federale di Germania.*
[35] Corte Edu, sentenza del 25 febbraio 1997, *Z. Vs Finlandia.*
[36] Corte Edu, ricorso n. 10454/83, sentenza del 7 luglio 1989, *Gaskin Vs Regno Unito.*
[37] Corte Edu, ricorso n. 2872/02, sentenza del 2 marzo 2008, *K. U. Vs Finlandia.*
[38] La Convenzione è stata adottata a Strasburgo dal Consiglio d'Europa il 28 gennaio 1981 ed è stata ratificata in Italia con la legge 21 febbraio 1989, n. 98 (*Ratifica ed esecuzione della convenzione n. 108 sulla protezione delle*

disciplina internazionale dei diritti dell'uomo. La Convenzione trae infatti ispirazione della art. 8 della CEDU e rimane ancora oggi l'unico strumento giuridico internazionale fondamentale in materia favorendo maggiori garanzie rispetto ai precedenti interventi. Tra gli aspetti di particolare rilevanza che ha introdotto uno è il suo carattere tendenzialmente universale poiché all'art. 23[39] prevede, differenziandosi dalle altre convenzioni dello stesso Consiglio, la possibilità di adesione anche di Stati non membri dei Consiglio d'Europa, su invito del Comitato dei Ministri[40]. La Convenzione, come dimostra anche il titolo, focalizza l'attenzione sul legame tra la protezione dei dati personali e la gestione automatizzata dei questi poiché a partire dagli anni Sessanta l'emergere delle tecnologie dell'informazione aveva determinato la necessità di prevedere norme più dettagliate per la tutela delle persone proteggendone i rispettivi dati. Dunque, garantisce un'interpretazione del *diritto alla riservatezza* soprattutto come *controllo dei dati* in quanto, la gestione automatizzata dei dati, aumentando la quantità di informazioni disponibili, ha trasformato la *privacy* in un problema di tutela dei dati personali che vengono rilasciati e che finiscono negli archivi informatici[41].

La Convenzione, indirizzandosi alla tutela delle persone fisiche, si applica a tutti i trattamenti dei dati personali effettuati sia dal settore pubblico sia dal settore privato e proprio quest'ultimo aspetto evita il sorgere del dubbio della non applicabilità della Convenzione ai rapporti tra i privati come era invece accaduto per l' art.8 della CEDU.[42]

Per quel che riguarda proprio l'analisi che intende soffermarsi su categorie di dati "speciali", è proprio la Convenzione n.108 a prevedere per la prima volta un riferimento specifico ai dati sensibili trattando all' art. 6 di *"catégories particulières de données"* e vietando la gestione automatica di tali dati, relativi alla razza, alle opinioni politiche, alle convinzioni religiose, allo stato di salute ed alla vita sessuale, a meno che il diritto interno non preveda garanzie adatte dal

---

persone rispetto al trattamento automatizzato di dati di carattere personale, adottata a Strasburgo il 28 gennaio 1981).

[39] L'art. 23 infatti prevede:*" 1. Successivamente all'entrata in vigore della presente Convenzione, il Comitato dei Ministri del Consiglio d'Europa potrà invitare ogni Stato non membro del Consiglio d'Europa ad aderire alla stessa con una decisione presa dalla maggioranza prevista all'art. 20 d) dello Statuto del Consiglio d'Europa e all'unanimità dei rappresentanti degli Stati contraenti aventi diritto di far parte nel Comitato.*

2. Per ogni Stato aderente, la Convenzione entrerà in vigore il primo giorno del mese successivo allo scadere del periodo di tre mesi dalla data del deposito dello strumento di adesione presso il Segretario Generale del Consiglio d'Europa."

[40] La Convenzione del 1981 ha previsto all'art.18 l'istituzione di un Comitato che si occupa della protezione dei dati (T-PD). Il T-PD ha il compito di interpretare le disposizioni della Convenzione n. 108 e di assicurarne l'effettiva applicazione, anche suggerendo modifiche ed adeguamenti. Il Comitato si riunisce in sede plenaria una volta l'anno, mentre il bureau del Comitato, una sorta di esecutivo, tiene generalmente più riunioni annue. È convocato dal Segretario generale del Consiglio d'Europa e sottopone direttamente al Comitato dei Ministri l'esito dei lavori svolti. Per maggiori informazioni sul comitato consultare il sito *www.garanteprivacy.it/web/guest/home/attivita-e-documenti/attivita-comunitarie-e-internazionali/cooperazione-in-ambito-extra-ue/consiglio-d-europa.*

[41] F. Pizzetti, *op. cit.*, p.85-86.

[42] G. Cellamare, *Tutela della vita privata e libera circolazione delle informazioni in una recente convenzione del Consiglio d'Europa*, in *Rivista di Diritto Internazionale*, 1982 , pp. 802 e ss.

punto di vista della loro tutela[43]. Sono poi indicati dalla Convenzione i principi che riguardano la raccolta e il trattamento dei dati personali, come quelli che si riferiscono alla correttezza e liceità della raccolta e al trattamento automatizzato dei dati, archiviati per specifici scopi legittimi, non destinati a un uso incompatibile con tali scopi né conservati oltre il tempo necessario; e, quelli che, invece, riguardano la qualità dei dati, in particolare in riferimento alla loro adeguatezza, proporzionalità nonché esattezza[44]. La Convenzione ha anche introdotto il principio della protezione "equivalente" che sarà poi fatto proprio dalla direttiva 95/46/CE della quale si tratterà nel prossimo paragrafo secondo il quale, il trasferimento tra due Stati aderenti a tale Convenzione dei dati personali può avere luogo soltanto ove il sistema giuridico dello Stato destinatario del flusso di informazioni garantisca il medesimo livello di tutela dello stato di origine.

Al fine di dare attuazione alla Convenzione, il Comitato dei Ministri del Consiglio d'Europa è intervenuto successivamente in materia attraverso l'utilizzo di strumenti di *soft law*[45] privi di efficacia vincolante, quali le Raccomandazioni, che però non sono state ritenute dotate di particolare incisività nelle legislazioni degli Stati[46]. È da evidenziare come, comunque, gli Stati membri abbiamo ratificato la Convenzione emendata nel 1999, per permettere all'Unione di divenire parte contraente e rafforzando le esigenze di tutela dei dati personali attraverso l'introduzione di disposizioni in materia di flussi frontalieri verso Paesi terzi e con la previsione dell'istituzione obbligatoria di autorità nazionale di protezione dei dati, previste a partire del 2001 dal Protocollo addizionale alla Convenzione[47].

[43] Gli aspetti concernenti i diritti sanitari, invece, sono stati trattati prima dalla Raccomandazione R(81) 1 del 23 gennaio 1981 e poi dalla più recente Raccomandazione R(97) 5 del 13 febbraio 1997.

[44] Agenzia dell'Unione europea per i Diritti Fondamentali, *op. cit.*, p. 16. Disponibile su *www.fra.europa.eu/en.*

[45] Termine ambiguo e impreciso data la loro non obbligatorietà che però non esclude che costituiscono l'avvio alla formazione di norme consuetudinarie o la premessa della conclusione di accordi internazionali: una prassi in tal senso è quella delle Dichiarazioni di principi dell'Assemblea generale delle Nazioni Unite. Per un'analisi maggiormente dettagliata B. Conforti, *Diritto internazionale*, VIII edizione, Napoli, Editoriale scientifica, 2010, pp. 40- 43 e 174-176.

[46] In particolare, si fa riferimento alla Raccomandazione n. R(86)1 del 23 gennaio 1986 *relativa alla protezione dei dati a carattere personale utilizzati a fini di sicurezza sociale* e la Raccomandazione n. R(89)2 del 18 gennaio 1989 *relativa alla protezione dei dati a carattere personale utilizzati ai fini dell'occupazione*, adottate dal Comitato dei Ministri del Consiglio d'Europa.

[47] Il Protocollo (*Protocollo addizionale alla Convenzione sulla protezione delle persone rispetto al trattamento automatizzato dei dati a carattere personale, concernente le autorità di controllo ed i flussi transfrontalieri*) è stato stipulato a Strasburgo l'8 novembre 2001 ed entrato in vigore il 1 luglio 2004. Inoltre, nell'ambito di una consultazione pubblica svoltasi nel 2011 finalizzata a modernizzare la Convenzione, prendendo in considerazione l'evoluzione delle nuove tecnologie, sono stati rafforzati i due obiettivi a fondamento della stessa: il rafforzamento della protezione della vita privata nel settore digitale e il consolidamento del meccanismo di attuazione della Convenzione.

4. La *privacy* nella normativa dell'Unione europea

Concentrando adesso l'attenzione sulla normativa in materia di *privacy* adottata dalle Istituzioni europee, nei seguenti paragrafi ci si soffermerà sui principali interventi in materia a partire dall'impatto decisivo dato alla direttiva "madre" del 1995 , passando a delineare le novità nel settore del commercio elettronico introdotte con la direttiva 2002/58/CE, per giungere, infine, alla previsione di un Regolamento europeo della *privacy* che rappresenta il punto di arrivo di un percorso iniziato nel 2012 e conclusosi lo scorso dicembre 2015 in cui le istituzioni europee sono giunte ad un accordo[48]. Come si vedrà a conclusione del capitolo, il Regolamento delineerà una disciplina finalmente uniforme in tutti gli Stati membri in materia di protezione dei dati personali soprattutto con riferimento alla richiesta di una tutela rafforzata richiesta a causa dell'"invadenza" delle nuove tecnologie.

4.1 La direttiva "madre" 95/46/CE: una disciplina completa sui dati personali

Trascorsi alcuni anni dall'adozione Convenzione del 1981, la Comunità europea si occupa della materia soltanto nel 1995 con la Direttiva del Parlamento europeo e del Consiglio n. 95/46/CE[49] introducendo un sistema più complesso di garanzie per i dati personali anche con riguardo ai trattamenti non automatizzati che intende armonizzare le legislazioni degli Stati membri. La direttiva, adottata sulla base dall'art. 95 del Trattato della Comunità europea e quindi in un'ottica ancora prettamente economica[50], è attualmente la base normativa di riferimento della protezione dei dati personali fino a quando gli Stati membri non si adegueranno al nuovo Regolamento europeo della *privacy*, che dovrebbe essere definitivamente approvato nei prossimi mesi. La direttiva si ricollegava anche ad altri interventi normativi comunitari adottati in campi analoghi come la direttiva n. 96/9/CE sulla protezione giuridica delle banche dati, che aveva lo scopo di proteggere gli investimenti fatti per la raccolta e l'elaborazione dei dati[51].
Diversamente dalla natura del Consiglio d'Europa, la Comunità Economica Europea (CEE) e,

[48] Dopo quasi quattro anni dalla proposta della Commissione europea nel gennaio 2012, il 15 dicembre 2015, durante i negoziati tra Commissione, Consiglio e Parlamento europeo, è stato trovato l'accordo per il nuovo Regolamento europeo della *privacy* nonostante lo stallo degli anni passati. Nell'ultimo paragrafo del presente capitolo verrà posta l'attenzione su tale tema.
[49] *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.*
[50] A partire dalla direttiva del 1995, i principali testi legislativi in materia di protezione dei dati personali di cui si dirà, fino al Trattato di Lisbona, sono stati adottati, sulla base di tale articolo che garantisce alle Istituzioni dell'Unione il potere di armonizzare il mercato interno, attraverso la procedura di codecisione, che comporta una decisione congiunta del Parlamento europeo e del Consiglio, secondo il principio di base secondo cui tali Istituzioni possono agire soltanto quanto espressamente previsto dai trattati.
[51] *Direttiva 96/9/CE del Parlamento europeo e del Consiglio dell'11 marzo 1996 relativa alla tutela giuridica delle banche di dati.*

prima ancora, la Comunità europea del carbone e dell'acciaio (CECA)[52] nacquero senza alcun riferimento ai diritti fondamentali ma con scopi di tipo economico quale la creazione di un mercato comune tra gli Stati membri attraverso l'eliminazione degli ostacoli alla libera circolazione delle merci, lavoratori, servizi, capitali rafforzati successivamente dall'Accordo di Schengen del 1985[53], proprio recentemente sospeso in alcuni Paesi che lo avevano sottoscritto di fronte alle recenti minacce alla sicurezza internazionale[54]. Nonostante, infatti, alcuni principi generali congeniti nel diritto comunitario quale il principio di non discriminazione in base alla nazionalità, i Trattati istitutivi non contenevano riferimenti ai diritti fondamentali: questo aspetto, unitamente agli scarsi poteri iniziali del Parlamento europeo, tese ad alimentare tutte quelle opinioni che sostenevano l'esistenza di un *deficit* democratico nel funzionamento delle Istituzioni comunitarie[55]. Il Parlamento europeo si fece così promotore di una vasta gamma di iniziative in materia di diritti fondamentali e in particolare nel 1989 con l'adozione della Dichiarazione sui diritti e delle libertà fondamentali[56], utile tutt'ora ai fini della lettura della Carta di Nizza[57]. Tuttavia, nel corso degli anni grazie al lavoro compensativo della Corte di Giustizia è stato possibile colmare sia il vuoto normativo rispetto ai diritti fondamentali all'interno dei Trattati istitutivi, sia l'iniziale mancata adesione alla CEDU[58] attraverso una "comunitarizzazione" della stessa nel senso della trasformazione dei suoi diritti in principi fondamentali del diritto comunitario. Pertanto, se si ritiene la *privacy* come la protezione dei dati personali intesa come diritto fondamentale, è immediatamente evidente l'ambiguità che si

[52] L'istituzionalizzazione del processo di integrazione tra gli Stati membri, che oggi si identifica con l'Unione europea, ha avuto inizio con l'entrata in vigore del Trattato istitutivo della Comunità europea del carbone e dell'acciaio il 23 luglio 1957. Sei anni dopo, si aggiunsero a questa altre due "Comunità": gli stessi sei Stati firmatari del Trattato CECA (Belgio, Francia, Italia, Paesi Bassi, Lussemburgo, Germania) sottoscrissero, il 25 marzo 1957, i Trattati istitutivi della Comunità economica europea (CEE) e della Comunità europea per l'energia atomica (CEEA o Euratom). Per una descrizione dettagliata del processo di integrazione europea si rinvia a R. Adam, A. Tizzano, *Manuale di diritto dell'Unione europea*, Torino, 2014, p.17.

[53] L'accordo di Schengen è stato firmato il 14 giugno 1985 da Belgio, Francia, Germania, Lussemburgo e Paesi Bassi. A questo si aggiunge la convenzione di Schengen che completa l'accordo e definisce le condizioni e le garanzie inerenti all'istituzione di uno spazio di libera circolazione. Firmata il 19 giugno 1990 dagli stessi cinque paesi, è entrata in vigore nel 1995. L'accordo e la convenzione, nonché gli accordi e le regole connessi, formano insieme l'*«acquis di Schengen»*, che è stato integrato nel quadro dell'Unione europea nel 1999 ed è diventato legislazione dell'UE. Per un quadro maggiormente dettagliato consultare il sito *www.eur-lex.europa.eu/summary/glossary/schengen_agreement.html?locale=it.*

[54] Recentemente, alcuni Paesi dell'Unione hanno chiesto la sospensione dell'Accordo al fine di arginare il flusso dei richiedenti asilo politico in seguito alle minacce terroristiche dei gruppi facenti capo allo Stato Islamico, meglio noto come ISIS, prevedendo una chiusura delle frontiere, seppur temporanea, a causa delle continue minacce alla sicurezza interna.

[55] L. Ferrari Bravo, E. Moavero Milanesi, *Lezioni di Diritto Comunitario*, Napoli, 2002, p. 17 e ss.

[56] Si riferisce alla Risoluzione del Parlamento europeo del 12 aprile 1989 con la quale è stata adottata la "Dichiarazione dei diritti e delle libertà fondamentali" (in G.U.C.E n C 120/51 del 16 maggio 1989). Tale risoluzione appare utile anche ai fini della lettura della Carta di Nizza.

[57] V. Barabba, *Tra Fonti e Corti. Diritti e principi fondamentali in Europa: profili costituzionali e comparati degli sviluppi sovranazionali*, Padova, 2008, p. 112.

[58] La Corte si era espressa in senso negativo all'adesione alla CEDU nel parere n. 2/94 del 26 marzo 1996 e più recentemente con il parere n.2/13 pubblicato il 18 dicembre 2014. Per un'analisi dettagliata sulle decisioni della Corte si rinvia a C. Zanghi, *La mancata adesione dell'Unione Europea alla CEDU nel parere negativo della Corte di giustizia",* in *www.rivistaoidu.net/sites/default/files/9_Zangh%C3%AC%20CEDU.pdf,* marzo 2015.

sostanzia nei due obiettivi di fondo della direttiva: quello, appunto, non patrimoniale che si realizza nella salvaguardia dei diritti fondamentali dell'uomo, e quello prettamente "economico" della libera circolazione, nel caso specifico, dei servizi. Tale commistione è messa in rilievo anche da un altro aspetto della direttiva che la distingue dai precedenti interventi rivolti al rispetto delle regole del mercato europeo, ossia la centralità assunta dalla persona e della sua vita privata poiché è proprio attorno ad essa che si muove l'attività di raccolta e trasmissione dei dati personali: la rilevanza giuridica della persona non è quindi considerata qui come quella del consumatore che agisce nel mercato ma può definirsi come assoluta perché legata alla vita privata e alla personalità dell'individuo.[59] La libera circolazione dei dati, tuttavia, non poteva dirsi effettivamente realizzata se gli Stati membri non avessero potuto contare su un livello elevato e uniforme di protezione dei dati. Un equilibrio tra i due aspetti può dirsi raggiunto soltanto se si considera che il corretto funzionamento del mercato unico necessita della tutela dei diritti fondamentali. In tale senso, il contesto di riferimento della direttiva sulla protezione dei dati ricadeva in quello del Primo pilastro dell'Unione europea che riguardava le *Comunità europee* finalizzate alla realizzazione di un mercato comune europeo, oltre che l'unione economica e monetaria e altre competenze aggiunte nel corso del tempo al di là della politica del carbone e dell'acciaio e quella atomica, mentre le attività dell'Unione nei settori rientranti nel Secondo e Terzo pilastro non potevano beneficiare di un quadro generale sulla protezione dei dati personali[60].

Nonostante la direttiva fu adottata in un momento in cui nella maggior parte degli Stati membri erano già presenti legislazioni in materia con l'eccezione dell'Italia[61], essa, come ha espresso anche la Corte di Giustizia, si poneva lo scopo di *"rendere equivalente in tutti gli Stati membri il livello di tutela dei diritti e delle libertà delle persone riguardo al trattamento dei dati personali. […] Il ravvicinamento delle legislazioni nazionali applicabili in materia non deve avere per effetto un indebolimento della tutela da esse assicurata, ma deve, anzi, mirare a garantire un elevato grado di tutela nella Comunità. […] L'armonizzazione delle suddette legislazioni nazionali non si limita quindi ad un'armonizzazione minima, ma sfocia in*

[59] F. Macario, *op.cit.*, pp. 12-20.

[60] Il *Trattato di Maastricht* del 1992 aveva previsto la creazione dei tre Pilastri dell'Unione europea suddividendo le sue politiche in tre aree fondamentali: il primo rappresentato appunto dalle *Comunità europee* con le aree di riferimento sopra delineate; il secondo, la *Politica estera e di sicurezza comune;* il terzo, la *Cooperazione giudiziaria e di polizia in materia penale,* finalizzato alla costruzione di uno spazio europeo di libertà, sicurezza e giustizia in cui sia possibile una cooperazione contro la criminalità a livello sovranazionale. Per una disamina sul Trattato di Maastricht si rinvia a U. Villani, *Istituzioni di diritto dell'Unione europea,* 2 edizione riveduta e aggiornata, Bari, 2012, pp. 17-19.

[61] Soltanto la Grecia ha emanato una legge in questa materia dopo l'Italia. In Italia con l'adozione della legge n.675 del 1996 che sarà presa in considerazione nel capitolo successivo, darà attuazione interna alla direttiva comunitaria in questione.

un'armonizzazione che, in linea di principio, è completa."[62] Gli Stati membri avevano dunque limitata libertà nel dare attuazione alla direttiva a meno che non garantissero elevati livelli di protezione dei dati personali anche prima dell'adozione della normativa europea, lasciandogli tuttavia margini di adattamento per quanto riguarda deroghe in specifici settori nell'ottica del citato bilanciamento tra interessi contrapposti[63]. È da evidenziare come i 15 Stati appartenenti all'Unione europea al momento dell'adozione della direttiva del 1995 fossero anche parti contraenti della Convenzione del 1981 da un lato, evitando l'adozione di norme contraddittorie tra i due interventi e dall'altro rendendo effettiva la tutela della vita privata già contemplata nella Convenzione ma estendendone l'ambito di applicazione avvalendosi in particolare dell'art. 11 della stessa[64] che prevede la possibilità di utilizzare ulteriori strumenti di tutela quale l'istituzione all'interno degli Stati membri di autorità di controllo vigilanti sulla protezione dei dati personali, prevista poi nell'aggiornamento della Convenzione sopra detto[65] e attraverso la previsione di nuovi organismi istituiti per la tutela dei dati come *il Gruppo per la tutela delle persone col riguardo al trattamento dei dati personali*[66].

Delineando l'ambito di applicazione della direttiva, essa si applica ai dati trattati con mezzi automatici come le banche dati nonché a quelli contenuti in archivi non automatizzati come quelli tradizionali in formato cartaceo; non si applica, invece, al trattamento di dati effettuato da una persona fisica per l'esercizio di attività di tipo personale o domestico. Oltre a dare un'accurata definizione di *dati personali*[67] che sarà ripresa anche nella normativa italiana, ai fini della presente trattazione pare utile evidenziare come dedichi particolare attenzione alle *categorie particolari di dati* nella III Sezione, prevedendo all'art. 8 del testo della direttiva, il

---

[62] CGUE, cause riunite C-468/10 e C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) e Federación de Comercio Electrónico y Marketing Directo (FECEMD) c. Administración del Estado*, 24 novembre 2011, punti 28 e 29.

[63] L'art. 13 della direttiva prevede che gli Stati membri possono adottare disposizioni legislative intese a limitare il diritto di accesso e di informazione degli interessati al trattamento dei dati, qualora tali restrizioni siano una misura necessaria per: la sicurezza, la difesa, la pubblica sicurezza dello Stato; la prevenzione, la ricerca, l'accertamento e il perseguimento di infrazioni penali oltre che di violazioni della deontologia delle professioni regolamentate; la salvaguardia di un rilevante interesse economico o finanziario di uno Stato membro o dell'UE; la protezione della persona interessata o dei diritti e delle libertà altrui.

[64] L'art. 11 della Convenzione n. 108 che disciplina l'estensione della protezione prevede che: *"Nessuna disposizione del presente capitolo verrà interpretata come limitante o pregiudicante la facoltà di ogni Parte di accordare alle persone interessate una protezione più estesa di quella prevista dalla presente Convenzione".*

[65] Il riferimento è al Protocollo addizionale alla Convenzione stipulato nel 2001.

[66] Il Gruppo è stato istituito dall'art. 29 della direttiva 95/46, è un organismo consultivo e indipendente, composto da un rappresentante delle autorità di protezione dei dati personali designate da ciascuno Stato membro, dal Garante europeo della protezione dei dati, nonché da un rappresentante della Commissione. Il presidente è eletto dal Gruppo al suo interno ed ha un mandato di due anni, rinnovabile una volta. Per maggiori informazioni consultare *www.garanteprivacy.it/home/attivita-e-documenti/attivita-comunitarie-e-internazionali/cooperazione-in-ambito-ue/gruppo-di-lavoro-ex-articolo-29*.

[67] Art. 2, lettera a) della direttiva n. 95/46/CE definisce dati personali *"qualsiasi informazione concernente una persona fisica identificata o identificabile ("persona interessata"); si considera identificabile la persona che può essere identificata, direttamente o indirettamente, in particolare mediante riferimento ad un numero di identificazione o ad uno o più elementi specifici caratteristici della sua identità fisica, fisiologica, psichica, economica, culturale o sociale".*

più lungo dell'intero testo[68], i trattamenti riferibili a tali dati. In particolare, la direttiva vieta il trattamento da parte degli Stati membri di tutte quelle informazioni che riguardando la sfera più intima della persona che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale e quelle riguardanti lo stato di salute o la vita sessuale, non differenziandosi troppo da quanto era stato affermato in sede di Consiglio d'Europa. Tuttavia, con le opportune garanzie, la stessa disposizione, al secondo paragrafo, prevede delle deroghe al suddetto divieto quando:

"a) la persona interessata abbia dato il proprio consenso esplicito a tale trattamento, salvo nei casi in cui la legislazione dello Stato membro preveda che il consenso della persona interessata non sia sufficiente per derogare al divieto di cui al paragrafo 1, oppure
b) il trattamento sia necessario, per assolvere gli obblighi e i diritti specifici del responsabile del trattamento in materia di diritto del lavoro, nella misura in cui il trattamento stesso sia autorizzato da norme nazionali che prevedono adeguate garanzie, oppure
c) il trattamento sia necessario per salvaguardare un interesse vitale della persona interessata o di un terzo nel caso in cui la persona interessata è nell'incapacità fisica o giuridica di dare il proprio consenso; o
d) il trattamento sia effettuato, con garanzie adeguate, da una fondazione, un'associazione o qualsiasi altro organismo che non persegua scopi di lucro e rivesta carattere politico, filosofico, religioso o sindacale, nell'ambito del suo scopo lecito e a condizione che riguardi unicamente i suoi membri o le persone che abbiano contatti regolari con la fondazione, l'associazione o l'organismo a motivo del suo oggetto e che i dati non vengano comunicati a terzi senza il consenso delle persone interessate; o
e) il trattamento riguardi dati resi manifestamente pubblici dalla persona interessata o sia necessario per costituire, esercitare o difendere un diritto per via giudiziaria."

Altri casi di deroghe all'applicazione della disposizione in esame, sono previsti al terzo paragrafo, ossia *"quando il trattamento dei dati è necessario alla prevenzione o alla diagnostica medica, alla somministrazione di cure o alla gestione di centri di cura e quando il trattamento dei medesimi dati viene effettuato da un professionista in campo sanitario soggetto al segreto professionale sancito dalla legislazione nazionale, comprese le norme stabilite dagli organi nazionali competenti, o da un'altra persona egualmente soggetta a un obbligo di segreto equivalente".*

Infine, sempre per tali tipologie di dati, gli Stati sono autorizzati, previe opportune garanzie, ad apportare ulteriori deroghe per motivi di interesse pubblico rilevante, sulla base della

[68] Come è sottolineato in E. Giannanotonio, M.G. Losano, V. Zeno-Zencovich (a cura di), *La tutela dei dati personali. Commentario alla l.675/1996*, II edizione, Padova, 1999, pp. 273-276.

legislazione nazionale o di una decisione dell'autorità di controllo, lasciando margini di discrezionalità ai singoli Paesi.

In generale, la direttiva introduce il diritto ad ottenere informazioni da parte dell'interessato sul trattamento necessario per la prestazione del suo consenso e quello di accesso ai propri dati con possibilità di rettifica, cancellazione e congelamento dei dati e quello di opposizione al trattamento. Il controllo della corretta applicazione della direttiva è posto in capo ad un'apposita autorità dotata di poteri investigativi, di intervento e di promuovere azioni giudiziarie contro le violazioni delle varie disposizioni a tutela della *privacy*. Inoltre, la direttiva pone anche la possibilità di trasferire dati personali verso un Paese terzo avente un livello di protezione adeguato pur prevedendo espressamente delle deroghe[69]. Quello dell'adeguato livello di protezione dei dati all'estero, proprio in seguito ai continui attacchi principalmente alla *privacy* sul *web*, ha subìto proprio negli ultimi mesi importanti modifiche dopo che la Corte di Giustizia, lo scorso ottobre 2015, ha invalidato il cd. *Safe Harbor*, l'accordo che aveva permesso alle aziende USA di utilizzare gli stessi standard per la gestione dei dati personali negli Stati Uniti e in Europa adottato dopo il lasciapassare della Commissione europea che aveva ritenuto la presenza dell'*adeguato* livello di protezione dei dati negli Stati Uniti. La decisione della Corte di Giustizia e le sue conseguenze saranno affrontate ampiamente nel terzo capitolo.[70]

Nel maggio 2003, la Commissione europea ha trasmesso al Parlamento europeo la prima Relazione sull'applicazione della direttiva a cui ha fatto seguito una Risoluzione del Parlamento europeo[71]. È così stato posto alla luce come la direttiva abbia raggiunto i principali obiettivi che si era posta cioè eliminare gli ostacoli alla libera circolazione dei dati personali tra gli Stati membri e garantire livelli di protezione più ampi all'interno dell'Unione; tuttavia, entrambe le Istituzioni sono state concordi nell'affermare che non sia stata realizzata l'armonizzazione legislativa tra gli Stati membri auspicata. Le due istituzioni hanno indicato le criticità che non hanno permesso un'attuazione completa della direttiva quali un rispetto disomogeneo tra gli Stati del rispetto dei titolari del trattamento e la scarsa conoscenza dei diritti spettanti agli interessati. In seguito poi agli attacchi terroristici di matrice islamica a

[69] All'art. 26 sono previste le deroghe a tale disciplina: quando la persona interessata acconsenta al trasferimento nel caso della conclusione di un contratto; qualora il trasferimento risulti necessario per ragioni di interesse pubblico, ma anche qualora lo Stato membro abbia autorizzato norme d'impresa vincolanti o clausole contrattuali tipo.

[70] Come si vedrà nel prosieguo, la decisione della Corte deriva da un'iniziativa legale avviata da uno studente austriaco Max Schrems, che aveva fatto causa a Facebook in Irlanda, per violazione della privacy da parte di programmi di sorveglianza di massa della NSA. La sua iniziativa legale era stata inizialmente respinta dall'autorità per la privacy irlandese, dove ha sede principale Facebook proprio perché ricadeva sotto il cd. *Safe Harbor*; Schrems fece appello e alla fine portò il caso alla Corte di giustizia dell'Unione Europea. Il caso giurisprudenziale sarà affrontato nello specifico nel prosieguo della trattazione.

[71] Con lettera del 15 maggio 2003 la Commissione ha trasmesso al Parlamento la prima relazione sull'applicazione della direttiva sulla tutela dei dati consultabile su *www.privacy.it/cecA52004-104.html*.

partire dall'inizio degli anni 2000 e non ancora cessati[72], la Commissione ha riconosciuto la necessità di uniformare le legislazioni conciliando l'esigenza della *privacy* individuale con l'interesse pubblico della sicurezza interna degli Stati cosicché il Parlamento europeo nella sua Risoluzione ha sollecitato a proporre uno strumento giuridico vincolante sulla protezione della vita privata che potrebbe concretizzarsi con le prospettive aperte recentemente dal nuovo Regolamento europeo.

4.2 La direttiva sul commercio elettronico: la sicurezza dei dati con l'avvento delle nuove tecnologie e l'ampliamento della disciplina nel cd. Terzo pilastro

Il crescente sviluppo della società dell'informazione ha introdotto nuovi servizi di comunicazione elettronica rendendo sempre più semplice l'accesso alle reti digitali a disposizione di un numero sempre maggiori di individui. Questo aspetto ha da un lato, consentito agli utilizzatori delle nuove tecnologie, l'uso di possibilità maggiori soprattutto attraverso il *web*, dall'altro ha messo sempre più in pericolo la tutela della vita privata degli utenti sempre più "visibile" a chiunque. Dunque, gli obiettivi posti dalla direttiva "madre" sono apparsi come superati nell'ottica delle nuove tecnologie, così il Parlamento europeo e il Consiglio dell'Unione europea hanno adottato nel 2002 una direttiva, denominata *"e-privacy"* successivamente modificata da quella *data retention*[73] e invalidata nella pronuncia dell'aprile 2014 della Corte di Giustizia, della quale si tratterà nel terzo capitolo[74].

Non prevedendo all'interno della direttiva riferimenti a dati degni di una tutela rafforzata quali appunto quelli sensibili ma riferendosi più propriamente a termini "tecnici" introdotti dalle nuove tecnologie[75], la direttiva del 2002 integrando quella del 1995 si prefissava di armonizzare le legislazioni statali al fine di non creare ostacoli allo sviluppo delle reti di comunicazioni elettronica con l'obiettivo di tutelare i diritti e le libertà fondamentali delle persone fisiche e i legittimi interessi delle persone giuridiche nel settore delle reti pubbliche di comunicazione.

[72] Da considerare in tal senso, sono anche gli ultimi attacchi terroristici dei gruppi armati ricollegabili all'ISIS avvenuti lo scorso 13 novembre 2015 in molte zone della capitale francese.

[73] La direttiva di riferimento è quella 2002/58/CE del Parlamento europeo e del Consiglio del 12 luglio 2002 *relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche.* La direttiva del 2002 è stata adottata nell'ambito della riforma operata dal *Regulatory Package* formato da una direttiva quadro (21) e quattro direttive di settore (19, 20, 22 e 58), alle quali si aggiunge la 77/2002/CE relativa alla concorrenza nei mercati delle reti e dei servizi di comunicazione elettronica.

[74] L'8 aprile 2014, la Corte di Giustizia dell'Unione ha invalidato la Direttiva 2006/24/CE sulla conservazione dei dati, a seguito di un rinvio pregiudiziale presentato sia dalla High Court irlandese che dalla Corte costituzionale austriaca in merito alla validità di tale direttiva, con particolare riferimento ai diritti fondamentali del rispetto della vita privata e della protezione dei dati personali, sanciti nella Carta dei diritti fondamentali dell'Unione Europea.

[75] L'art. 2 della direttiva contiene l'elenco di una serie di definizioni: *utente, dati relativi al traffico, dati relativi all'ubicazione, comunicazione, chiamata, consenso dell'utente o dell'abbonato, servizio a valore aggiunto, posta elettronica.*

Anche questa direttiva aveva lo scopo di bilanciare il diritto dei cittadini al rispetto alla vita privata con la possibilità per gli Stati membri di adottare deroghe qualora esigenze di sicurezza pubblica, difesa, sicurezza dello Stato e applicazione legge penale lo avessero richiesto[76]. Prima della pronuncia invalidante la direttiva così modificata, nel tutelare la sicurezza dei dati personali, la direttiva imponeva al fornitore dei servizi di comunicazioni elettroniche di adottare misure tecniche e organizzative appropriate.

Il panorama europeo in materia è stato ampliato con l'adozione del Regolamento CE n. 45/2001, adottato sulla base dell'art. 286 del Trattato della Comunità europea come aggiornato dopo il Trattato di Amsterdam[77], che ha previsto la protezione dei dati personali anche per i trattamenti delle istituzioni e degli organismi comunitari[78] e l'istituzione dell'*European Data Protection Supervisor* (EDPS), il Garante europeo per la protezione dei dati personali: un'Autorità che ha il compito di garantire il rispetto del diritto alla vita privata nel trattamento dei dati personali da parte delle Istituzioni e degli organismi dell'Unione.

Proprio tale attenzione maggiore posta ai problemi di sicurezza dei dati personali sembrerebbe aver esteso gli interventi relativi alla protezione dei dati personali anche nell'ambito del Terzo Pilastro dell'Unione, mentre mancano ancora disposizioni in tal senso che si riferiscono alle attività rientranti nella PESC. Sulla base di ciò, sono state adottate diverse Convenzioni[79] che hanno previsto l'istituzione di Autorità nazionali di controllo in materia di dati personali supervisionati da un'Autorità comune con compiti di sorveglianza di determinati archivi. Tuttavia, le incessanti minacce di terrorismo hanno indotto l'Unione a superare l'idea di una protezione dei dati attraverso politiche settoriali quali le Convenzioni od interventi frammentati e disomogenei[80], e giungere ad un unico e generale sistema di protezione dei dati per le finalità di sicurezza, polizia e giustizia proprie del Terzo Pilastro[81]. Così nella *Spring Conference* del 2007, le Autorità nazionali della *privacy* hanno dato vita a un nuovo Gruppo di lavoro, il cd.

---

[76] Nel *Preambolo* della direttiva, si specifica infatti che gli Stati membri hanno la facoltà di effettuare intercettazioni legali di comunicazioni elettroniche, o di prendere altre misure per perseguire tali scopi, sempre nel rispetto della Convenzione europea di salvaguardia dei diritti dell'uomo e delle liberà fondamentali.

[77] Tale articolo, ora confluito nell'attuale art. 16 del TFUE, estendeva l'applicazione dei principi di protezione dei dati
anche ai dati personali trattati da parte delle Istituzioni e degli organi della Comunità europea.

[78] Il regolamento n. 45/2001 del Parlamento europeo e del Consiglio *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* è stato adottato il 18 dicembre 2000.

[79] In particolare la Convenzione Schengen, già citata, Europol ed Eurodac.

[80] Esempi di interventi settoriali e frammentati nell'ambito del terzo Pilastro possono essere ritrovati nelle recenti proposte sullo scambio di casellari giudiziari fra gli Stati, o gli scambi di dati sul DNA, impronte digitali e immatricolazione dei veicoli ai sensi della cosiddetta *"L'iniziativa di Prüm"*.

[81] F. Pizzetti, *op. cit.*, pp. 91-93.

Working Party on Policy and Justice (WPPJ)[82], che non ha però uniformato la disciplina come adesso si dirà.

Sempre in quest'ottica, nel novembre 2008 il Consiglio dell'Unione europea ha adottato una Decisione Quadro sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale[83], molto discussa in ambito europeo proprio dal WPPJ. Essa infatti è il primo strumento europeo adottato per la protezione dei dati nell'ambito del Terzo Pilastro. Pur non pregiudicando la sicurezza interna degli Stati, protegge i diritti e le libertà fondamentali delle persone fisiche quando i loro dati personali sono trattati, in modo automatizzato o meno, ai fini della prevenzione, indagine, accertamento o del perseguimento dei reati o dell'esecuzione delle sanzioni penali. Per quel che riguarda ciò che interessa nello specifico in questa sede, l'art. 6 della Decisione Quadro si riferisce ai dati sensibili il cui trattamento non è ammesso a meno che strettamente necessario e se la legislazione nazionale preveda adeguate garanzie.

La decisione indica tutta una serie di diritti che spettano all'interessato al trattamento: deve essere informato della raccolta o del trattamento di dati personali che la riguardano, qualora però siano stati trasmessi dati personali tra Stati membri, ciascuno Stato può chiedere che l'altro non informi la persona interessata. Quest'ultimo ha il diritto di richiedere conferma del fatto che dati che lo riguardano siano stati trasmessi, nonché le informazioni sui destinatari e sui dati che sono oggetto di trattamento, e conferma che siano state effettuate tutte le verifiche necessarie dei dati. In alcuni casi gli Stati membri possono restringere l'accesso alle informazioni da parte della persona interessata comunicandole per iscritto insieme ai motivi di fatto o di diritto sui quali la decisione si basa. Infine, può richiedere che i dati personali che la riguardano siano rettificati, cancellati o bloccati e qualsiasi rifiuto deve essere comunicato per iscritto informandola dell'opportunità di presentare un reclamo o un ricorso. Nel caso di un trattamento illegale dei dati, chiunque subisca un danno ha diritti al risarcimento e in caso di violazione dei diritti, l'interessato può fare ricorso giurisdizionale.

Tuttavia, è stato rilevato come, anche rispetto alla Convenzione del 1981 e alla direttiva "madre", la decisione non sembra assicurare un livello di tutela dei dati personali proprio relativamente a certi aspetti: in particolare, alla disciplina dei dati sensibili (dove il trattamento è ammesso soltanto se strettamente necessario e se la legislazione nazionale prevede adeguate garanzie), ma anche al diritto di accesso dell'interessato (l'elevata discrezionalità con cui gli

[82] Il WPPJ riunisce tutte le Autorità nazionali, tutte quelle operanti nel settore del Terzo Pilastro (Autorità Schengen, Europol, Eurodac) e l'EDPS. Esso vuole assicurare che il settore di sicurezza e giustizia sia accompagnato da un livello di tutela dei dati personali adeguato ai principi fondamentali.

[83] Si tratta della Decisione Quadro 2008/977/GAI del 27 novembre 2008 *sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale*.

Stati possono limitarlo per non compromettere le indagini) e al trasferimento dei dati verso paesi terzi (è molto generica la valutazione di adeguatezza del livello di protezione dei dati personali)[84]. È proprio in questo contesto che si opereranno le modifiche alla normativa di riferimento attuate con l'entrata in vigore del Trattato di Lisbona come si vedrà nel prosieguo.

4.3 L'impatto del Trattato di Lisbona in materia di *privacy* e la Carta dei diritti fondamentali: la nascita di uno "specifico" diritto alla protezione dei dati a carattere personale

È stato evidenziato sin dall'analisi della direttiva del 1995 come non fossero previste disposizioni all'interno dei Trattati istitutivi che si riferissero a diritti fondamentali e specificamente, per quel che interessa in questa sede, a un diritto alla *privacy* ma al contrario, come tutti i testi legislativi in materia fossero stati adottati su basi giuridiche principalmente volte ad affrontare l'armonizzazione del mercato interno[85]. Sicuramente il lavoro della Corte di giustizia è stato fondamentale in tal senso, chiarendo l'ambito di applicazione di tali disposizioni e privilegiando un'interpretazione che tenesse conto del diritto alla protezione dei dati anche al di là del esercizio concreto delle attività economiche.[86]

In tal senso il Trattato di Lisbona[87] ha apportato un miglioramento in materia poiché, abolendo la struttura dei tre Pilastri, ha esteso la protezione dei dati personali a tutti i settori dell'attività dell'Unione attraverso il suo riconoscimento all'interno del Trattato me prevede anche, come adesso sarà descritto, norme specifiche con riferimento ai settori della PESC e a quello della sicurezza, polizia e cooperazione giudiziaria. Dunque, il Trattato ha fornito un quadro giuridico comune per tutte le attività dell'Unione abolendo le divisioni tra attività "comunitarie" e "intergovernative" e rafforzando il ruolo di co-legislatore del Parlamento europeo, cambiamento che si riflette sulla materia della protezione dei dati personali.

In particolare è l'art. 16 del TFUE (ex art. 286 del TCE), che, nell'ambito del Titolo II intitolato *"Disposizioni di applicazione generale",* che stabilisce una specifica e completa base giuridica della materia. In particolare, esso precisa che:

---

[84] G.F. Ferrari (a cura di*), La tutela dei dati personali in Italia 15 anni dopo. Tempo di bilanci e bilanciamenti.*, Collana di Diritto dell'Economia a cura di P. Marchetti, Egea, p.31.

[85] Il riferimento normativo alla disciplina era rappresentato dall'art. 95 del Trattato della Comunità europea.

[86] A. Scirocco, *The Lisbon Treaty and the Protection of Personal Data in the European Union,* 19 settembre 2008, in *www.secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/Publications/Speeches/2008/08-09-19_Scirocco_Lisbontreaty_DP_EN.pdf.*

[87] Il trattato di Lisbona *che modifica il Trattato sull'Unione Europea e il Trattato che istituisce la Comunità Europea* è stato firmato a Lisbona il 13 dicembre 2007 dagli allora 27 Stati membri dell'Unione Europea ed entrato in vigore 1 dicembre 2009.

"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. Le norme adottate sulla base del presente articolo fanno salve le norme specifiche di cui all'articolo 39 del trattato sull'Unione europea."

Sono molti gli aspetti innovativi introdotti dalla norma: è previsto un diritto soggettivo alla tutela dei dati personali; un riferimento "costituzionale europeo" per le regole relative alla protezione dei dati; le norme attuative del dettato dei trattati devono essere adottate attraverso la procedura legislativa ordinaria, il che significa che Parlamento e Consiglio sono in una posizione di equi ordinazione. Tuttavia, quest'ultimo aspetto, in virtù di quel bilanciamento tra valori contrapposti, subisce una deroga nelle materie rientranti, prima di Lisbona, nel Secondo Pilastro, quella della PESC, come si evince nell'ultima parte dell'articolo: la procedura di adozione di norme specifiche in materia di protezione dei dati in quest'ambito saranno stabiliti dal Consiglio, non comportando il coinvolgimento del Parlamento; tuttavia anche in questo caso il rispetto di tali norme che anche in resta soggetto al controllo di autorità indipendenti[88]. Anche per quanto riguarda il settore della polizia cooperazione giudiziaria, il Trattato di Lisbona, attraverso due protocolli allegati, prevede una disciplina specifica nella materia della protezione dei dati personali. Il primo, il Protocollo n. 20 *sull'applicazione di alcuni aspetti dell'articolo 26 del trattato sul funzionamento dell'Unione europea al Regno Unito e all'Irlanda* che però non sembra aggiungere aspetti innovativi al quadro delle già citate eccezioni per interessi di sicurezza nazionale. Il secondo, il Protocollo n.21 *sulla posizione del Regno Unito e dell'Irlanda rispetto allo spazio di libertà, sicurezza e giustizia* specifica, invece, che la cooperazione giudiziaria e di polizia può giustificare norme specifiche di protezione dei dati, da adottare ai sensi dell'articolo 16 del TFUE e richiede l'adozione di alcuni interventi settoriali. I Protocolli hanno un forte valore politico e sono destinati a influenzare l'interpretazione delle

[88] L' art. 39 TFUE prevede che: *"Conformemente all'articolo 16 del trattato sul funzionamento dell'Unione europea e in deroga al paragrafo 2 di detto articolo, il Consiglio adotta una decisione che stabilisce le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale da parte degli Stati membri nell'esercizio di attività che rientrano nel campo di applicazione del presente capo, e le norme relative alla libera circolazione di tali dati. Il rispetto di tali norme è soggetto al controllo di autorità indipendenti.*" Tuttavia, dato che l'articolo 39 stabilisce deroghe solo per quanto riguarda il trattamento dei dati personali da parte degli Stati membri, la disposizione generale dell'articolo 16 sembra rimanere pienamente applicabile - con il coinvolgimento del Parlamento europeo - in caso di trattamento dei dati personali da parte delle istituzioni dell'Unione europea.

nuove disposizioni sui dati personali e lo sviluppo degli strumenti legislativi basati su di essi. Pur non facendo parte del Trattato, Lisbona ha riconosciuto alla Carta dei diritti fondamentali dell'Unione europea, proclamata già nel 2000[89], un valore giuridico vincolante soltanto nel 2009[90], che appare rilevante in questa sede perché ha contribuito a riconoscere un diritto *alla protezione dei dati a carattere personale.* Quest'ultimo si distingue dai "tradizionali" diritti ai quali era stata sempre ricondotta la *privacy* a partire dall'art. 8 CEDU interpretato dalla Corte di Strasburgo proprio in tal senso e rappresenta uno degli aspetti maggiormente innovativi nel *post*-Lisbona: in particolare si riferisce al diritto di ogni individuo *al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni* sancito all'art.7 della stessa Carta[91]. Venendo ad un'analisi dettagliata della disciplina considerata, è l'art. 8 della Carta a menzionare esplicitamente di un *diritto alla protezione dei dati a carattere personale*:

"1. Ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano.
2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica.
3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente."

Dalla lettura della disposizione in esame si evincono innanzitutto i suoi elementi essenziali: il trattamento effettuato in base a finalità legittime e secondo il consenso dell'interessato o secondo altro fondamento legittimo previsto dalla legge, il diritto di accesso e di rettifica dell'interessato ai propri dati. La Carta però, sempre in virtù del perseguimento di un interesse pubblico, prevede la possibilità di limitazioni a tale diritto attraverso le "garanzie" della loro previsione in base alla legge e il rispetto del contenuto essenziale di tali diritti[92]. Il diritto così

[89] La Carta è stata elaborata da una Convenzione composta da un rappresentante di ogni paese dell'UE e da un rappresentante della Commissione europea, nonché da membri del Parlamento europeo e dei Parlamenti nazionali. Fu proclamata ufficialmente a Nizza nel dicembre 2000 dal Parlamento europeo, dal Consiglio e dalla Commissione. Nel dicembre 2009, con l'entrata in vigore del trattato di Lisbona, è stato conferito alla Carta lo stesso effetto giuridico vincolante dei trattati. A tal fine, la Carta è stata modificata e proclamata una seconda volta nel dicembre 2007. Per maggiori informazioni consultare *www.eur-lex.europa.eu/legal-content/IT/TXT/?uri=URISERV%3Al33501*.

[90] È l'art. 6 del TUE a sancire che la Carta di Nizza abbia lo stesso valore giuridico dei Trattati.

[91] In realtà una simile distinzione era possibile ritrovarla già nelle direttive 95/46/CE, 97/66/CE (*sul trattamento dei dati personali e sulla tutela della vita privata nel settore delle telecomunicazioni* sostituita da quella del 2002), e 2002/58/Ce. Queste infatti distinguevano un diritto *alla protezione dei dati a carattere personale* da un diritto alla *riservatezza.* In E. Varani, *Il "nuovo diritto "alla privacy. Dalla Carta di Nizza al "Codice in materia di protezione dei dati personali"*, in *www.filodiritto.com/articoli/2012/04/il-nuovo-diritto-alla-privacy-dalla-carta-di-nizza-al-codice-in-materia-di-protezione-dei-dati-personali/*, 7 aprile 2012, pp. 2-3.

[92] Il riferimento è all'art. 54, paragrafo I della Carta: *"1. Eventuali limitazioni all'esercizio dei diritti e delle libertà riconosciuti dalla presente Carta devono essere previste dalla legge e rispettare il contenuto essenziale di detti diritti e libertà. Nel rispetto del principio di proporzionalità, possono essere apportate limitazioni solo laddove*

come è definito dalla Carta, da un lato, ha un effetto diretto in quanto i cittadini degli Stati membri dell'Unione, possono farli valere dai giudici nazionali e dalle rispettive autorità di protezione dei dati anche in assenza di misure specifiche di attuazione; dall'altro rafforza il ruolo di quelle Autorità che controllano il rispetto del diritto riconoscendo loro una "copertura costituzionale europea"[93].

Infine è utile evidenziare altri due aspetti messi in luce dall'art.6 del TUE: il primo delineato dal paragrafo 2 del TUE che prevede che l'Unione europea aderisca alla Convezione europea dei diritti dell'uomo. Tale previsione non solo sostanzia la tutela dei diritti fondamentali in seno all'Unione ma incide anche nei rapporti tra le Istituzioni compresa la Corte di Giustizia che sono tenute a rispettare le disposizioni presenti nella Convenzione. Il secondo aspetto previsto dal paragrafo 3 dello stesso articolo, il quale conferma che i diritti fondamentali quali sono garantiti dalla CEDU e quali risultano dalle tradizioni costituzionali comuni degli Stati membri, costituiscono principi generali del diritto dell'Unione. Questo "doppio legame" con la CEDU da parte dell'Unione è importante dal punto di vista della protezione dei dati personali perché conferma l'importanza dell'articolo 8 della CEDU e la giurisprudenza della Corte di Strasburgo nel quadro giuridico dell'Unione europea, migliorando nel contempo le garanzie istituzionali e procedurali.

Il Trattato di Lisbona anche attraverso la Carta di Nizza ha permesso di definire un quadro giuridico completo e generale in materia di protezione dei dati, ma, come si è detto, anche capace di considerare la specificità di alcuni settori. Tuttavia, la crescente domanda di tecnologia da un lato, e le possibilità offerte dall'era digitale, richiedono sforzi maggiori da parte delle istituzioni europee e degli Stati membri per coinvolgere i cittadini nelle scelte che ricadono nella loro *privacy.*

4.4 Le prospettive aperte dal nuovo pacchetto di riforma sulla *privacy*: il primo vero riferimento a un diritto alla riservatezza *online*

Nelle pagine precedenti è stato anticipato come la disciplina della *privacy* è in procinto di essere completamente riformata, nel territorio dell'Unione europea, dal pacchetto delle nuove regole in materia contenute nel nuovo Regolamento europeo sulla *privacy.* Il percorso di

siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui."

[93] Come sottolinea A. Scirocco, *op. cit.*: *"The use of the singular ("authority") rather than the plural ("authorities", used in the other Treaty provisions) does not seem to affect the possibility that the supervision might be carried out by more authorities, at European, national or sub-national level. The essential element is the independence, which should be a structural element of any single data protection authority".*

riordino ha avuto origine da un'iniziativa della Commissione europea[94], il 25 gennaio 2012, la quale aveva annunciato la pubblicazione di una proposta di riforma integrale della legislazione europea in materia di dati personali[95]. In linea anche con altri interventi delle Organizzazioni internazionali quali l'aggiornamento della Convenzione n.108 da parte del Consiglio d'Europa di cui si è detto nei paragrafi precedenti, la proposta nacque nell'ambito dell'iniziativa *"Agenda Digitale europea"* compresa nella più generale strategia decennale *"Europa 2020"*[96]. Dopo quasi quattro anni, lo scorso 15 dicembre 2015 è stato raggiunto un accordo sul pacchetto delle nuove regole, in seguito ai negoziati finali tra il Parlamento, la Commissione ed il Consiglio dell'Unione europea, il cd. *trilogo*, e dopo che la commissione LIBE[97] ha approvato nella sessione straordinaria del successivo 17 dicembre 2015 i testi concordati nei triloghi. Il giorno successivo, il COREPER[98] ha confermato i testi di compromesso finali relativi al regolamento e alla direttiva, che come si dirà nel prosieguo, sono i due provvedimenti che compongono il testo di riforma. Nei primi mesi del 2016, saranno sottoposti alla conferma da parte del Consiglio e del voto del Parlamento europeo[99]: se il pacchetto sarà definitivamente approvato, i 28 Stati membri dell'Unione avranno due anni a disposizione per recepire la Direttiva, mentre il Regolamento sarà immediatamente esecutivo applicandosi direttamente agli Stati, concedendo alle aziende nazionali due anni per potersi adeguare. Dunque, in tutti i Paesi dell'Unione le normative interne applicabili in materia di riservatezza saranno immediatamente sostituite dall'entrata in vigore del nuovo Regolamento, compreso il *Codice della privacy*, che come di vedrà nel capitolo seguente, rappresenta la normativa italiana attualmente in vigore in materia di *privacy*.

Analizzando adesso nello specifico in cosa consiste la riforma prospettata dalle nuove regole, questa si compone di due strumenti legislativi: un regolamento, che interesserà tutti i soggetti

---

[94]Tutte le informazioni relative all'iniziativa della Commissione sono consultabili su *www.ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm*.

[95] Commissione europea, *Proposta di regolamento del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (regolamento generale sulla protezione dei dati*), Bruxelles, 25 gennaio 2012.

[96] *Europa 2020* è la strategia decennale per la crescita e l'occupazione che l'Unione europea ha varato nel 2010. L'UE si è data cinque obiettivi quantitativi da realizzare entro la fine del 2020 che riguardano l'occupazione, la ricerca e sviluppo, il clima e l'energia, l'istruzione, l'integrazione sociale e la riduzione della povertà. Al fine di attuarli, sono state previste sette iniziative prioritarie che tracciano un quadro entro il quale l'UE e i governi nazionali sostengono reciprocamente i loro sforzi per realizzare le priorità di Europa 2020, tra cui anche quella dell'economia digitale. Per maggiori informazioni su Europa 2020 consultare *www.ec.europa.eu/europe2020/europe-2020-in-a-nutshell/index_it.htm.*

[97] È la Commissione per le libertà civili, la giustizia e gli affari interni del Parlamento europeo. Le informazioni e le attività della Commissione sono consultabili su *www.europarl.europa.eu/committees/it/libe/home.html*.

[98] Il Coreper è il Comitato dei rappresentanti permanenti previsto all' art. 240 del TFUE. Composto dai rappresentanti dei paesi dell'UE aventi il rango di ambasciatori degli Stati membri presso l'Unione europea e presieduto dal paese dell'UE che esercita la presidenza del Consiglio, è responsabile della preparazione dei lavori del Consiglio dell'Unione europea. Per maggiori informazioni sul comitato si rimanda al sito *www.eur-lex.europa.eu/summary/glossary/coreper.html?locale=it.*

[99] Il voto definitivo del Parlamento europeo potrebbe arrivare nel marzo 2016.

privati e parte di quelli pubblici e che sarà immediatamente applicabile e sostituirà la direttiva del 1995 sulla protezione dei dati personali; una direttiva, che riguarda l'uso dei dati personali nell'ambito della sicurezza e delle attività di polizia e di giustizia e che necessiterà del recepimento per diventare operativa nei vari Stati, finalizzata invece a sostituire la decisione quadro del 2008.

L'elemento centrale del pacchetto di riforma è dunque il Regolamento che mira a rafforzare il livello di protezione dei dati per le persone fisiche i cui dati personali sono oggetto di trattamento e incrementare le opportunità per le imprese nel mercato unico digitale attraverso una riduzione degli oneri amministrativi a loro carico. La necessità della previsione di un Regolamento in materia nasce dall'evoluzione dei concetti di *privacy* in tutte le sue declinazioni e di quella specifica di protezione dei dati personali rispetto alla diffusione del processo tecnologico. Tale aspetto è messo in rilievo dal fatto che la tecnologia attuale, infatti, consente tanto alle imprese private quanto ai soggetti pubblici di utilizzare dati personali nello svolgimento delle loro attività e, allo stesso tempo, i soggetti privati rendono sempre più disponibili e pubbliche le loro informazioni[100]. Dunque, pur rimanendo valido in termini di obiettivi e principi, il quadro giuridico attuale derivante dalla direttiva del 1995 non ha impedito la frammentazione delle modalità di applicazione della tutela dei dati nei diversi Stati membri né ha eliminato la percezione nel pubblico che le operazioni *online* comportino notevoli rischi. Così è divenuto sempre più necessario instaurare una disciplina più attuale e coerente in materia di protezione dei dati personali in tutto il territorio dell'Unione, rinvenibile nel Regolamento, che consentirà lo sviluppo dell'economia digitale nel mercato interno, garantirà un maggiore controllo delle persone fisiche sulle informazioni immesse in rete e rafforzerà la certezza giuridica per i soggetti economici e le autorità pubbliche[101]. Inoltre, la necessità della riforma è da ricercarsi anche nell'esigenza di una maggiore garanzia di sicurezza dei dati raccolti e trattati nell'*online* recentemente aumentate dalle continue minacce nei confronti della *privacy*[102]. Delineando nello specifico gli obiettivi del Regolamento, oltre al rafforzamento del diritto sancito sia dall'art.16 TFUE sia dall'art.8 della Carta di Nizza, esso intende, dunque, primariamente rafforzare i diritti della privacy *online*, favorire maggiori opportunità all'interno

[100] Sul punto si veda M. Iaselli, *Accordo raggiunto sul Regolamento Europeo in materia di protezione dei dati personali*, 23 dicembre 2015, su *www.altalex.com/documents/news/2015/12/23/accordo-raggiunto-sul-regolamento-europeo-in-materia-di-protezione-dei-dati-personali*, p. 2 in cui l'autore sottolinea come le nuove tecnologie abbiano trasformato non soltanto l'economia ma anche le relazioni sociali.

[101] Si veda ancora M. Iaselli, *ibidem.*

[102] Ad esempio, la presenza di programmi quali *trojans*, *cookies*, *malware* e *virus* mettono sempre più a rischio tutti quei dati concernenti i dettagli delle carte di credito e poco sicuri, sono anche i cd. *data security breach*, ossia quegli accessi non autorizzati da parte di pirati informatici ai database di aziende o di amministrazioni pubbliche contenenti le informazioni personali di migliaia di persone.

dell'economia digitale e incrementare la fiducia dei cittadini/utenti nei servizi offerti dal web[103]. Per la prima volta, il riferimento alla *privacy* è legato al contesto specifico del *web* e non più ricompreso in quello "generale" delle telecomunicazioni come avveniva con la direttiva 2002/58/CE, perché si comprende come il processo di digitalizzazione in atto cambi anche il modo di raccogliere e trattare i dati personali, compresi quelli legati alla sfera più intima dell'individuo, aspetti che non erano stati considerati dalla normativa attualmente in vigore[104]. Nello specifico, il testo del Regolamento, con le numerose modifiche apportate, prevede nuovi principi e diritti applicabili nei confronti degli interessati, ossia le persone fisiche i cui dati sono trattati, conferendo loro un maggiore controllo su di questi e definendo rispettivi obblighi a carico di titolari e responsabili del trattamento dei dati personali.

Innanzitutto, esso garantisce il cd. *diritto all'oblio,* che sarà analizzato nel terzo capitolo della presente trattazione nella particolare declinazione data dalla Corte di Giustizia in seguito ad una questione posta da un rinvio pregiudiziale[105], particolarmente vicino all'anglosassone *right to be let alone*: secondo questo, l'interessato ha il diritto ad ottenere la cancellazione dei dati che lo riguardano da parte del titolare del trattamento dopo un determinato periodo di tempo, nel caso in cui non vi siano ragioni che ne giustifichino la raccolta. Tale diritto nasce in rapporto con l'esercizio della cronaca giornalistica: un fatto privato può divenire oggetto di cronaca nel caso di interesse pubblico della notizia, in tale caso la collettività deve essere informata con tempestività, in modo di poter far conoscere l'accaduto in tempo reale e completezza. L'idea di fondo al diritto all'oblio, dunque, sta che dopo la conoscenza da parte del pubblico del fatto, cessa l'interesse pubblico e non vi sarebbe più un reale interesse della collettività quindi sarebbe inutile riproporre l'accadimento. Dunque, il diritto prevede che non dovrebbe essere riproposta una notizia vecchia e lesiva qualora non risponda più ad un'attuale esigenza informativa[106]. Tale diritto assume una particolare connotazione con l'avvento della rete per la possibilità enorme di raccogliere, scambiare e archiviare informazioni personali e dunque esercitare il diritto all'oblio. Tenendo conto di tali aspetti, il regolamento prevede un diritto alla cancellazione dei dati personali, il che consente, ad esempio, agli interessati di chiedere la

[103]Commissione Europea, *Why do we need an EU data protection reform?, www.ec.europa.eu/justice/data-protection/document/review2012/factsheets/1_en.pdf,* 2012.

[104] Come ha messo in rilievo il Commissario alla Giustizia Viviane Reding in occasione della presentazione del progetto di riforma al momento dell'entrata in vigore della Direttiva 95/46/CE, meno dell'un per cento dei cittadini europei faceva uso di internet. Oggi, invece, quasi la totalità dei cittadini europei dispone di un accesso alla rete, ove possono essere scambiate e trasferite enormi quantità di dati in semplici frazioni di secondo. Aspetto accentuato dall'avvento dei *social networks*, che però ha esposto la privacy degli utenti a nuove forme di controllo e di ingerenza. Il Comunicato stampa del Commissario è consultabile su *www.europa.eu/rapid/pressReleasesAction.do?reference=IP/12/46&format=HTML&aged=0&language=en&guiLanguage=en* aggiornato al 1 settembre 2012.

[105] Nel terzo capitolo, sarà analizzato il caso *Google Spain,* sul quale si è pronunciata la Corte di giustizia sul tema del diritto all'oblio.

[106] Così M. Iaselli, *op. cit.,* p. 4.

soppressione, senza ritardo, dei dati personali raccolti o pubblicati sui cd. *social network* quando la persona fisica in questione era ancora un minore, in una logica di "auto-protezione". Altro profilo innovativo previsto dal Regolamento è rappresentato dalla cd. *portabilità dei dati* che consente all'interessato sia di trasferire i propri dati tra sistemi elettronici diversi sia di farne usi ulteriori in formati elettronici diversi. Si permette così all'utente di avere un maggiore controllo sui propri dati raccolti e trattati dagli *Internet service provider (ISP)*[107]. Tale nuovo sistema facilita la trasmissione dei dati personali da un ISP all'altro: non solo saranno maggiormente garantiti i diritti in materia di protezione dei dati, ma sarà prevista anche una maggiore concorrenza tra prestatori di servizi *online.* Nell'ottica di un maggiore controllo rispetto ai dati, il regolamento, diversamente da quanto previsto dalla normativa attualmente applicabile, prevede anche un rafforzamento della disciplina riguardante il *consenso* individuale[108]. Se, difatti, attualmente in molti Stati membri il consenso è dato per implicito in numerose circostanze[109] ad eccezione però, come mostrato, per quello che riguarda il trattamento proprio dei dati sensibili, nella nuova previsione normativa è previsto che debba sempre essere specifico ed espresso in maniera esplicita[110]. Da questo punto di vista, il regolamento, prevede una particolare attenzione ai mezzi attraverso i quali ottenere il consenso dai minorenni, data la capillare diffusione delle tecnologie soprattutto tra i giovani: qualora infatti un sedicenne desideri utilizzare servizi in linea, l'ISP deve cercare di verificare l'effettivo consenso dei genitori. Tuttavia, tenendo conto delle differenze di disciplina applicabili nei diversi Stati membri, è stato prevista la possibilità di abbassamento di tale limite di età senza scendere al di sotto dei 13 anni. Si prevede anche un potenziamento dell'informativa resa all'interessato con la possibilità di rendere la procedura più semplice attraverso il ricorso a disegni, icone o altre forme grafiche, secondo una logica di trasparenza di cui si dirà; al contrario, non è più previsto il meccanismo della notificazione al Garante per comunicare dei trattamenti dei dati più delicati. Gli interessati godono inoltre di un diritto di porre reclamo all'autorità di controllo, nonché di un diritto ad un ricorso giurisprudenziale nonché un diritto ad ottenere il riesame da parte di un giudice nazionale delle decisioni adottate dalle rispettive autorità di controllo a prescindere dallo Stato membro in cui il responsabile del trattamento dei

[107] La direttiva 2000/31/CE *sul commercio elettronico* si occupa di definire forme minime e comuni di responsabilità degli ISP definendoli come i soggetti che forniscono servizi di connessione, trasmissione, memorizzazione dei dati. Il recepimento della normativa europea in Italia sul commercio elettronico sarà oggetto di uno specifico paragrafo del capitolo 2.

[108] Anche la cd. *profilazione,* ossia la creazione di profili degli utenti in base ai loro gusti o l'utilizzo dei loro dati personali a fini di marketing, può avvenire soltanto in base al consenso dell'interessato.

[109] Basti pensare che, ad esempio, si ritiene che un individuo che utilizzi un sito *web* abbi necessariamente aderito alla politica sulla privacy di tale medesimo sito, senza la necessità di un consenso esplicito.

[110] Da questo punto di vista, rispetto alla disciplina attuale, si avrà un'inversione dell'onere della prova ricadente sul responsabile del trattamento che dovrà fornire la dimostrazione che il titolare dei dati aveva dato il suo consenso esplicito al trattamento dei medesimi per specifiche finalità.

dati è stabilito.

Deve essere poi rispettato il principio di *accountability*[111], disponendo che il responsabile del trattamento debba garantire ed essere in grado di dimostrare che il trattamento dei dati personali sia conforme alla normativa del Regolamento. Tale principio è collegato ad un altro particolarmente rilevante e innovativo introdotto dalla normativa: il *principio della trasparenza* nell'accezione di una migliore informazione su quanto accade ai dati personali una volta condivisi in rete. Prevedendo un'informazione sulle politiche della *privacy* nei confronti delle persone fisiche, viene considerato fondamentale l'utilizzo di un linguaggio semplice e chiaro anche attraverso icone standardizzate. Ancora, collegati al principio di *accountability* sono quelli del cd. *privacy by design* e *privacy by default:* il primo prevede che la protezione dei dati sia integrata nell'intero ciclo di vita della tecnologia dalla fase della progettazione fino a quella dell'esecuzione del trattamento comprendente la sua distribuzione, utilizzo ed eliminazione finale; il secondo, invece, prevede che le impostazioni di tutela dei dati personali relativi ai servizi e ai prodotti debbano rispettare i principi generali della protezione dei dati. Il testo del Regolamento, poi, specifica anche quali siano gli obblighi generali dei responsabili del trattamento dei dati e dei soggetti che li trattano per loro conto, ossia gli incaricati al trattamento, in direzione di una previsione di maggiori responsabilità in capo a tali soggetti. Tra di questi figura l'obbligo di dimostrare che i trattamenti effettuati siano conformi alla normativa prevedendo l'obbligatorietà, in caso di trattamenti rischiosi, di una valutazione di impatto sulla protezione dei dati al fine di limitarne i rischi, ricadenti sui diritti e le libertà degli interessati (*Privacy Impact Assessment – PIA)* e della notificazione all'Autorità di controllo in caso di violazione di sicurezza che provoca, anche accidentalmente, la distruzione, la perdita, la modifica, la rivelazione non autorizzata o l'accesso a dati. Inoltre, le autorità pubbliche e le imprese che svolgono alcune operazioni di trattamento[112] dovranno nominare un responsabile della protezione dei dati, il cd. *Data Protection Officer,* figura presente già in alcuni Paesi europei[113] che potrà essere interno o esterno alle aziende, dotato di indipendenza e spettanti compiti di sorveglianza e controllo di attuazione e applicazione del regolamento. Qualora i responsabili o gli incaricati al trattamento violino le disposizioni sulla protezione dei dati

[111] Ancora, M. Iaselli, *op. cit.,* p.6 evidenzia come il concetto di *accountability*, è stato originariamente elaborato al fine di favorire il flusso dei dati internazionale ma può avere un'interpretazione più ampia applicabile al trattamento dei dati personali.

[112] Il responsabile del trattamento o l'incaricato del trattamento prevedono l'istituzione di un responsabile della protezione dei dati quando: il trattamento viene effettuato da un'autorità pubblica o da un organismo pubblico, da un'impresa con 250 o più dipendenti oppure quando le attività principali del responsabile del trattamento o dell'incaricato consistono in trattamenti che richiedono un controllo regolare e sistematico degli interessati per la loro natura, il loro oggetto o le loro finalità.

[113] La figura non è prevista attualmente dalla disciplina italiana ma l'ex Presidente dell'Autorità Garante per la Privacy, Francesco Pizzetti, intervenne a favore della sua istituzione nel 2006, in occasione dell'*European Privacy Officers Forum (EPOF)* che riunisce tutti i *Privacy Officers* che operano all'interno delle società multinazionali con sede in Europa.

personali, la nuova normativa prevede delle sanzioni fino a 20 milioni di EUR o al 4% del loro fatturato globale annuo, comminate dalle autorità nazionali di controllo. Tali sanzioni amministrative verranno imposte dalle autorità nazionali di controllo. Infatti, resta confermato l'obbligo di istituzione all'interno degli Stati membri di un'Autorità di controllo della normativa relativa ai dati personali come era stata prevista sin dall'adozione della direttiva 95/46/CE. Inoltre, prevede anche l'istituzione di un comitato europeo per la protezione dei dati, che dovrebbe comprendere rappresentanti di tutte le 28 autorità di controllo indipendenti e sostituire l'esistente comitato *ex* articolo 29 di cui si è parlato.

Il testo del nuovo Regolamento pone anche l'attenzione nel caso in cui vi sia un trasferimento di dati personali a Paesi terzi e organizzazioni internazionali. Al fine di garantire la massima tutela dei dati dei cittadini del territorio europeo, conferisce alla Commissione la responsabilità di valutare il livello di protezione di protezione offerto; qualora però manchi una decisione della Commissione in tal senso, sono previsti alcuni casi particolari in cui il trattamento dei dati è comunque concesso o esistano particolari garanzie[114]. Inoltre, le decisioni di adeguatezza dovranno essere riesaminate almeno ogni 4 anni. L'applicazione della normativa relativa ai trattamenti di dati svolti all'estero dovrà, tuttavia, tenere conto anche delle prospettive aperte dal *post- Safe Harbor* e dalle prossime mosse in tale direzione delle Istituzioni europee[115].

Occorre capire, dopo aver affrontato in linee generali il contenuto del nuovo Regolamento, se preveda e, in caso di esito positivo, che regime applicabile alle categorie *speciali* di dati, di cui si tratta. La risposta è positiva in quanto anche la nuova normativa conferma una disciplina specifica applicabile per quei dati che sono, per loro natura, particolarmente sensibili e idonei ad incidere in materia di diritti fondamentali e che dunque meritano di una protezione specifica. Nulla è innovato rispetto alla normativa attuale prevedendo che tali dati non possono essere trattati senza il consenso esplicito da parte dell'interessato; tuttavia deroghe specifiche possono essere previste nei confronti di esigenze specifiche e a quella "tradizionale" del trattamento rientrante tra le attività (legittime) poste in essere da associazioni o fondazioni il cui scopo è quello di consentire l'esercizio delle libertà fondamentali[116]. Deroghe al divieto di trattamento di tali categorie di dati possono essere consentite se previste dalla legge e fatte salve adeguate garanzie in modo di tutelare i dati personali e altri diritti fondamentali come la salute pubblica, la protezione sociale e la gestione dei servizi sanitari, finalizzata quest'ultima a garantire la

[114] Dalla lettura del testo di regolamento questi tali casi appaiono essere la presenza di clausole tipo di protezione dei dati, norme vincolanti d'impresa, clausole contrattuali.

[115] Come è stato anticipato nelle pagine precedenti, la sentenza *Schrems,* invalidante il regime previsto dal *Safe Harbour,* sarà trattata a conclusione del presente elaborato.

[116] Come si vedrà nel prossimo capitolo, fin dalla prima normativa adottata in Italia in materia di tutela dei dati sensibili, sono state previste deroghe specifiche qualora il trattamento sia effettuato da associazioni o fondazioni che svolgono attività legittime verso i diritti fondamentali.

qualità e costo-efficacia delle procedure per rispondere alle richieste di prestazioni e servizi nel sistema di assicurazione sanitaria, o per scopi storici, statistici e di ricerca scientifica. Con riferimento invece al secondo dei due strumenti legislativi previsti dal pacchetto di riforma in materia della *privacy*, questo è costituito dalla nuova direttiva che andrà a sostituire la decisione quadro 2008/977/GAI e che mira a tutelare il diritto delle persone fisiche alla protezione dei loro dati personali e allo stesso tempo a garantire un elevato livello di sicurezza pubblica. La direttiva si applicherà al trattamento dei dati sia nazionali che transfrontalieri da parte delle autorità competenti a fini di contrasto ossia: per la prevenzione, accertamento e perseguimento dei reati e la protezione e la prevenzione per la sicurezza pubblica. Non ricoprirà però l'attività delle istituzioni, organismi e agenzie dell'Unione né le attività che esulano dall'ambito di applicazione del diritto dell'Unione. La direttiva in questione prevederà una serie di principi e diritti applicabili agli interessati come anche obblighi nei confronti dei responsabili di detti trattamenti, sostanzialmente analoghi a quelli previsti dal Regolamento in materia di *privacy*. Garantisce, in primo luogo, che i dati vengano trattati in modo lecito, siano raccolti in base a finalità specifiche, esplicite e legittime e non siano eccessivi rispetto agli obblighi per i quali sono trattati. Inoltre, prevede anche il diritto di accesso, rettifica, cancellazione e limitazione del trattamento da parte dell'interessato con rispettivi obblighi degli Stati membri di fornire informazioni comprensibili. Con riferimento, invece, agli obblighi, anche la direttiva prevede che i responsabili del trattamento nominino un responsabile per la protezione dei dati incaricato di assistere le autorità competenti[117] e l'obbligo di effettuare una valutazione di impatto per alcuni casi di trattamento. Inoltre, il suddetto comitato consultivo europeo per la protezione dei dati svolgerà dei compiti anche relativamente alle attività contemplate dalla direttiva e sarà previsto un risarcimento nei confronti degli interessati per eventuali danni subiti per un trattamento che non rispetta la disciplina. Infine, anche con riferimento al trasferimento dei dati in un paese terzo, la direttiva riprende quanto già previsto dal testo del Regolamento: tali trasferimenti sono possibili solo se richiesti a fini di contrasto e qualora la Commissione abbia adottato una decisione sull'adeguatezza del livello di protezione offerto. In mancanza di queste, i trasferimenti possono avvenire soltanto in base ad alcune garanzie.

Dopo aver affrontato tutti i principali aspetti di cui si compone il pacchetto delle nuove regole in materia di *privacy,* che probabilmente entrerà in vigore nel marzo 2016 in seguito al voto definitivo del Parlamento europeo, occorrerà attendere l'eventuale adeguamento da parte dei 28 Stati membri dell'Unione per comprendere se effettivamente sarà capace di uniformare la disciplina dei dati personali all'interno del territorio europeo come, invece, non era riuscita la

[117] La direttiva prevede norme sull'assistenza reciproca tra le autorità competenti e obblighi di cooperazione tra di queste.

direttiva del 1995. A tal proposito giova sicuramente a favore la scelta dello strumento giuridico del *regolamento* da parte della Commissione europea, che il TFUE definisce come caratterizzato dalla massima incidenza negli Stati membri[118] ed una "supremazia" rispetto alla legislazione interna incompatibile, senza necessità di adozione di misure di recepimento. Con particolare riferimento a tale scelta infatti, non sono mancate perplessità in particolare da parte del Comitato Economico e Sociale che nel suo parere ha sottolineato come la Commissione avrebbe dovuto specificare in maniera più incisiva, alla luce del rispetto del principio di proporzionalità, il motivo della scelta di uno strumento così invasivo capace di limitare la discrezionalità degli Stati membri[119]. Nonostante ciò, è stato comunque adottato il regolamento che rappresenta il mezzo privilegiato ogniqualvolta le istituzioni europee si propongono di raggiungere un obiettivo di uniformazione legislativa all'interno dell'Unione. Contrariamente alla direttiva[120] infatti, strumento utilizzato per ottenere il ravvicinamento delle legislazioni, che fissa soltanto un obiettivo di "risultato" europeo lasciando discrezionalità agli Stati nei modi attraverso i quali raggiungerlo, che sicuramente comporta un adeguamento meno brusco alla normativa europea ma comportando anche evidenti rischi di differenziazioni tra le differenti leggi di attuazioni.

[118] Ai sensi del paragrafo 2 dell'art. 288 del TFUE *"Il regolamento ha portata generale. Esso è obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri."*

[119] Il parere del Comitato economico e sociale è consultabile su Parere del Comitato Economico e Sociale su *www.eesc.europa.eu/?i=portal.en.soc-opinions.22438*.

[120] Sempre ai sensi dell'art.288 del TFUE, paragrafo 3 invece *"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."*

Capitolo Secondo

Il nucleo duro della *privacy*: la normativa nazionale sul trattamento dei dati sensibili

1. Il diritto alla *privacy* nella Costituzione: un riconoscimento implicito

Prima di trattare come la normativa attuale italiana si sia occupata della disciplina dei cc. dd. *dati sensibili*, è opportuno domandarsi se vi sia un fondamento all'interno della Costituzione italiana della nozione di *privacy* intesa nella sua fattispecie complessa[121] e in particolare proprio del suo cd. *nucleo duro*[122] che come sottolinea Rodotà, *"[…] è ancora oggi costituito da informazioni riferite a fatti particolarmente intimi (ad esempio quelli riguardanti la salute o le abitudini sessuali): al suo interno, però, hanno assunto rilevanza sempre più marcata altre categorie, che pure non possono essere chiuse unicamente nella sfera privata (quali le opinioni politiche e sindacali, la razza o il credo religioso), protette, per evitare che dalla loro circolazione possano nascere situazioni di discriminazione."*[123] Non molto diversamente dagli altri Paesi europei[124], nella Costituzione italiana mancano riferimenti alla *privacy*, soprattutto perché al momento dell'entrata in vigore della Carta, costituiva un tema poco dibattuto[125]. A partire dagli anni Cinquanta, la giurisprudenza comincia ad affrontare sempre più frequentemente le questioni attinenti alla riservatezza, pronunciandosi su casi di opere cinematografiche e pubblicazioni relative a vicende personali di personaggi famosi che

[121] Si parla di fattispecie complessa del diritto in questione, sviluppatosi grazie al quadro europeo e internazionale e inteso quale diritto alla riservatezza, diritto all'identità personale e diritto alla protezione dei dati personali, tutti dotati di medesimo valore "costituzionale". Si rinvia a E. Varani, *Il "nuovo diritto "alla privacy. Dalla Carta di Nizza al "Codice in materia di protezione dei dati personali*, in *www.filodiritto.com/articoli/2012/04/il-nuovo-diritto-alla-privacy-dalla-carta-di-nizza-al-codice-in-materia-di-protezione-dei-dati-personali/*, 7 aprile 2012, p. 7-8.

[122] A tal proposito pare opportuno evidenziare come un primo riconoscimento alla tutela della riservatezza in Italia, seppur legislativo e non costituzionale, si è avuto proprio con riferimento a quelle informazioni che rivelano le opinioni politiche, sindacali e religiose, rientranti nel cd. *nucleo duro*, di alcune categorie di individui. Il riferimento è alla legge n. 300 del 1970 contenente lo *Statuto dei lavoratori*, in cui all'art. 8 prevede un divieto di raccolta delle opinioni politiche, sindacali e religiose da parte dei datori di lavoro. Sul tema del fondamento giuridico della *privacy* attraverso una tutela maggiormente garantistica accordata ai lavoratori si rimanda a S. Niger, *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali*, Padova, 2006 e S. Rodotà, *La privacy tra individuo e collettività*, in *Politica del diritto*, Bologna, 1974.

[123] S. Rodotà, *Tecnologie e diritti*, Bologna, 1995, p.105.

[124] Come in Italia, anche in Francia, Gran Bretagna e Germania il diritto alla *privacy* è nato soprattutto grazie agli interventi giurisprudenziali mentre in Spagna è previsto un richiamo all'art. 18 della Costituzione; tuttavia, anche in questo caso i giudici spagnoli hanno aumentato la portata di tale diritto.

[125] Per tali ragioni, la *privacy* viene fatta rientrare nei diritti di nuova formazione. In tal senso G. Gardini, *Le regole dell'informazione. Principi giuridici, strumenti, casi*, Milano, p. 239.

chiedevano ai giudici una tutela della propria riservatezza[126].

Nonostante il vuoto normativo, la giurisprudenza e la dottrina hanno ricavato un fondamento costituzionale del diritto da una lettura sistematica sia di disposizioni "generali" come quella previste dagli artt. 2 e 3 della Cost. sia di quelle finalizzate a tutele singole e specifiche. Attualmente, il quadro costituzionale è richiamato dall'art. 2, comma 1 del decreto legislativo n.196 del 2003, il quale prevede che i trattamenti dei dati si svolgano *"nel pieno rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali"*[127].

Date queste premesse, la *privacy* ha avuto un riconoscimento nel nostro ordinamento, anzitutto, attraverso l'art. 2 Cost. inteso come fattispecie aperta comprendente tutti i diritti che non sono esplicitati dalla Carta Costituzionale[128] - aspetto ancora più rilevante se si considera l'accento posto sulla particolare *sensibilità* di alcune informazioni personali come quelle trattate in questa sede. Il riferimento a tale articolo assume rilevanza rispetto al riconoscimento e alla tutela dei diritti inviolabili dell'uomo, per il rapporto che si instaura tra persona e formazioni sociali, evidenziato ancora di più oggi dal ruolo assunto delle tecnologie che accentuano la partecipazione politica e sociale; e, infine per la previsione di doveri inderogabili di solidarietà economica, politica e sociale. Dunque, attraverso il riconoscimento costituzionale all'art. 2, la *privacy* perde quel sospetto di forzatura del testo costituzionale in quanto finalizzato a soddisfare il fine superiore di apprestare effettiva tutela alla persona umana e alle sue esigenze fondamentali[129]. Anche l'articolo 3, riconoscendo l'uguaglianza giuridica e i diritti inviolabili, pone in rilievo il valore della persona umana. Infatti, la dottrina favorevole all'utilizzo dell'art. 3 come fondamento della riservatezza nella Carta Costituzionale, ha posto in rilevo la necessità della garanzia di una sfera privata inviolabile affinché la dignità e lo sviluppo della persona, siano effettivamente assicurati e non restino soltanto delle affermazioni di principio.[130]

---

[126] Si fa riferimento alle prime pronunce della Corte di Cassazione sul tema. La prima è la sentenza del 22 dicembre 1956, n. 4487 sul *caso Caruso;* la seconda è la n.990 del 20 aprile 1963 sulla *pubblicazione del libro "Il grande amore"*; e, la terza sul caso *Soraya Esfandiari* la n. 2129 del 27 maggio 1975.

[127] Come sottolinea A. Ghiribelli, *Il diritto alla privacy nella Costituzione italiana*, 30 novembre 2007, in *www.teutas.it/societa-informazione/comunicazioni-elettroniche/tutela-dei-dati-personali/92-il-diritto-alla-privacy-nella-costituzione-italiana.html*.

[128] Si vedano A. Barbera, *Commento all'art.2 della Costituzione*, in G. Branca (a cura di), *Commentario della Costituzione*, Bologna, 1975 e S. Niger, *op. cit.*,p. 43.

[129] Così M. Prosperi, *Il diritto alla riservatezza nell'ordinamento costituzionale (I parte)*, in *www.dirittosuweb.com/aree/rubriche/record.asp?cat=4&idrecord=575*.

[130] Per le critiche al fondamento della tutela della *privacy* all'art. 3 Cost. si rimanda a S. Fois, *Questioni sul fondamento costituzionale del diritto all'"identità personale"*, in AA.VV., *L'informazione e i diritti della persona*, Napoli, 1983, p. 167 e F. Bricola, *Prospettive e limiti della tutela penale della riservatezza*, in AAVV, *Il diritto alla riservatezza e la sua tutela penale, Atti del terzo simposio di studi di diritto e procedura penali*, Varenna, Villa Monastero, 5 – 7 settembre 1967/ promosso dalla Fondazione "Avv. Angelo Luzzani" di Como – Milano, 1970, p.84.

Attraverso la lettura combinata di tali disposizioni, viene riconosciuta alla *privacy* una rilevanza maggiore, in quanto rientrante nel *nucleo dei principi fondamentali* e pertanto non oggetto di revisione costituzionale[131].

Se tali disposizioni forniscono una copertura di tipo generale del diritto in questione, altre si riferiscono a sfere più specifiche della riservatezza o tutelano valori che potrebbero essere pregiudicati proprio da tale diritto. In particolare, si tratta dei riferimenti impliciti ricadenti: nell'art. 13 Cost. che riguarda l'inviolabilità della libertà personale e indirettamente anche a quella morale che sarebbe violata nei casi di interferenze nella vita privata dei soggetti; nell'art. 14 Cost., relativo alla protezione del domicilio, "luogo" all'interno del quale si manifesta la piena personalità dell'individuo e all'interno del quale quest'ultimo non debba subire interferenze esterne; nell'art. 15 Cost. sulla segretezza della corrispondenza che appare riferibile soprattutto alle comunicazioni elettroniche in quanto sono previste garanzie ogniqualvolta vi sia una limitazione di tale diritto[132]; e, infine all'art. 21 Cost. che concerne la libertà di manifestazione del pensiero che ha acquisito un peso sempre maggiore nella società dell'informazione. Occupandosi da un lato, del rapporto tra la libertà di informazione e il diritto alla *privacy* e, dall'altro, della definizione della libertà in questione sotto il profilo di informarsi ed essere informati, nell'era di internet la tecnologia ha infatti dato maggiori possibilità di reperire, accumulare e trattare le informazioni personali anche più intime senza limitazioni spaziali e temporali. Infatti, da un lato, è evidente come l'esercizio della libertà di manifestazione di pensiero possa entrare in conflitto con l'interesse della riservatezza in quanto ogni limite alla circolazione delle informazioni si traduce in un limite alla libertà sottesa all'art.21 Cost, ma dall'altro, considerando che nessuna libertà ha carattere assoluto, un individuo ha anche la possibilità di tacere, di manifestare il proprio pensiero soltanto in parte o di rivelarlo soltanto ad alcuni soggetti[133].

Riassumendo, se si considera preminente il riconoscimento della *privacy* all'interno delle disposizioni del primo tipo, si fa riferimento ad una base materiale più coerente in quanto la persona umana è considerata nella sua unitarietà con una "sovrapposizione" di tutti gli aspetti che la ricomprendono; se invece vengono poste in rilevo l'altro tipo di disposizioni, più "frammentate" nella Carta Costituzionale, c'è una proiezione della affermazione e valorizzazione di tali aspetti che si concretizzano in veri e propri beni. Nella prima legislazione italiana in materia, come si vedrà tra breve, prevarrà la seconda tesi sia perché la legge di

[131] A. Ghiribelli, *op.cit.*

[132] Infatti, l'art. 15 Cost. al comma 2 prevede che: *"La loro limitazione può avvenire soltanto per atto motivato dell'autorità giudiziaria [cfr. art. 111 c. 1] con le garanzie stabilite dalla legge."*.

[133] Sul punto si veda M. Prosperi, *Il diritto alla riservatezza nell'ordinamento costituzionale (II parte*), in *www.dirittosuweb.com/aree/rubriche/record.asp?cat=4&idrecord=578.*

riferimento enuncerà espressamente il diritto alla riservatezza e quello dell'identità personale, sia perché prevederà anche la nascita di un nuovo diritto sulla protezione dei propri dati[134].

2. Il lungo iter per l'approvazione della prima disciplina in materia: la legge 31 dicembre 1996 n. 675

Alla mancanza di un fondamento costituzionale del diritto in questione si aggiunse anche il ritardo, da parte dell'Italia, nel dotarsi di una disciplina organica nella materia nella sua particolare sua accezione di protezione dei dati personali, contrariamente ad altri Paesi europei, quali Francia e Germania che già a partire dagli anni Settanta si erano dati di una normativa apposita; tendenza progressivamente incrementata dalla diffusione dei nuovi mezzi tecnologici. Infatti, nonostante si rendesse sempre più necessaria una disciplina a causa proprio dell'ampliamento del numero dei *"detentori del nuovo potere informatico, consistente nel controllo sui singoli, reso possibile dall'acquisizione e dall'elaborazione di informazioni [..]*[135]*"*, l'inerzia italiana rispetto agli interventi suddetti negli altri Paesi europei, è durata per quasi quindici anni: tuttavia, nel settore delle banche dati è stato ritenuto applicabile il T. U. di Pubblica Sicurezza[136] che all'art. 8 regolava la raccolta e l'uso di informazione da parte della polizia e imponeva agli enti di denunciare alle Prefetture competenti gli "archivi magnetici" relativi a dati personali, disposizione abolita nel 1996. Prima di allora, il tema del trattamento dei dati personali era stata oggetto di attenzione sia da parte di molti giuristi italiani sia da parte di soggetti preposti alla formazione del procedimento legislativo[137]. Fu nel 1996 che si realizzò il primo intervento normativo in materia con la legge n. 675[138] sotto la spinta delle scadenze per il recepimento degli atti comunitari, in particolare proprio della direttiva *privacy* 95/46/CE[139]. Le novità più rilevanti della legge sono, anzitutto, la previsione della figura del *Garante per la*

---

[134] Zeno- Zencovich, *I diritti della personalità dopo la legge sulla tutela dei dati personali*, in *Studium Iuris*, 1997, p. 467.

[135] F. Fabris, *Il diritto alla privacy tra passato presente e futuro*, in *www.openstarts.units.it/dspace/bitstream/10077/3394/1/09_fabris.pdf*, 2009 n.2 (luglio-dicembre), pp.96-98.

[136] La legge del 1 aprile 1981, n. 121 contenente il *Nuovo ordinamento dell'Amministrazione della pubblica sicurezza*, GU n.100 del 10-4-1981 - Suppl. Ordinario.

[137]Cfr. Zeno- Zencovich, *Una lettura comparatistica della l. n 675/96 sul trattamento dei dati personali, in Riv. trim. dir. proc. civ.,* 1998, p. 735. L'autore, sul punto, specifica due schemi di disegni di legge in materia di tutela della riservatezza stilati dalla commissione Mirabelli costituita in seno al Ministero di Grazia e Giustizia ed il disegno di legge presentato dall'allora Ministro della giustizia Martelli ma che fu bloccato prima della sua approvazione finale.

[138] La legge del 31 dicembre 1996, n. 675 in materia di *Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali*, pubblicata in Gazzetta Ufficiale dell'8 novembre 1997 - Suppl. Ordinario n. 3. La legge è stata abrogata ai sensi dell'articolo 183, comma 1, lettera a), del Codice in materia dei dati personali.

[139] In senso contrario Zeno-Zencovich, *op. cit.,* 1998, pp. 734-735 che sostiene che *"pur non costituendo tecnicamente attuazione della direttiva 46/95 del 24 ottobre 1995, [..] , tuttavia ha in essa il suo punto di riferimento."*

protezione dei dati personali nonché la delega legislativa contenuta nella legge n. 676/1996 che ha permesso al Governo, negli anni successivi, di intervenire in senso correttivo per garantire una piena aderenza alle mutate esigenze di protezione[140]. La legge ha, inoltre, introdotto per la prima volta in Italia il principio per cui la riservatezza delle persone fisiche e giuridiche rappresenti un diritto assoluto e inviolabile meritevole di tutela attraverso la comminazione di sanzioni penali, civili e amministrative e perseguita attraverso l'uso congiunto degli strumenti del controllo e del consenso cd. *informato* con quello più limitato dell'autorizzazione; legata poi allo sviluppo della società dell'informazione, si è posto l'obiettivo di fornire al cittadino la possibilità di conoscere le informazioni che lo riguardano e in quale banche dati si trovano permettendogli di intervenire e di correggere le informazioni errate e difendere così la sua identità. Infatti l'art. 1 della legge, che riprende il modello redazionale dei testi normativi europei definendo l'ambito di applicazione della disciplina e i concetti più rilevanti, esplicita ciò che la legge mira a garantire, ossia il trattamento dei dati personali *"nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale".* Oltre ad avere positivizzato il concetto di *privacy*, la portata innovativa del provvedimento sta nell'aver inciso sull'intera categoria dei diritti della personalità: in particolare attraverso il riferimento alla *riservatezza* e dell'*identità personale*[141]. Al riguardo è stato rilevato da parte della dottrina come i due concetti non esauriscano gli aspetti della disciplina. Infatti, si coglie sicuramente dalla legge quanto la *riservatezza* sia stata stravolta dall'avvento dell'informatica per la crescente possibilità di raccogliere, scambiare e collegare grandi masse di dati riferibili all'interno degli archivi informatici ad un determinato soggetto, molto di più rispetto a quelli previsti da supporti cartacei e prevedendo una maggiore protezione soprattutto con riferimento al cd. *cuore della riservatezza*[142] . Inoltre, l'*identità personale* che aveva avuto una prima definizione da parte della Cassazione[143], ha adesso un primo riconoscimento legislativo prevedendo anche appositi strumenti di tutela[144]. Accanto a questi due aspetti della personalità, viene in rilievo per la prima

[140] In G. Gardini, *op. cit.*, 2009, pp. 246-247, dove l'autore sostiene che la tecnica della delega legislativa in senso autocorrettivo sia servita a mettere il legislatore al riparo da eventuali critiche, consapevole delle complessità e invasività della materia.

[141] Si veda F. Bilotta, *L'emersione del diritto alla privacy*, in A. Clemente (a cura di), *Privacy*, Padova, 1999, pp. 21-23.

[142] Il *cuore* della riservatezza, in una configurazione concentrica della stessa, è rappresentato proprio dai dati sensibili, i quali, come si dirà nel proseguo, necessitano di una "super protezione". Così Zeno- Zencovich, *op. cit.*, in Studium Iuris, 1997, pp. 467- 468.

[143] La Corte di Cassazione si è espressa nella sentenza 1985/3769, definendo l'identità personale come *"l'interesse di ciascuno a non vedersi all'esterno alterato, travisato, offuscato, contrastato il proprio patrimonio intellettuale, politico, sociale, religioso, ideologico, professionale, ecc. quale si è estrinsecato o appare, in base a circostanze concrete e univoche, destinato a estrinsecarsi nell'ambiente sociale".*

[144] La legge, all'art. 13, stabilisce i principi dell'esattezza, aggiornamento, pertinenza e completezza dei dati e definisce quali siano i diritti dell'interessato come quelli di ottenere l'aggiornamento, la rettifica e l'integrazione dei dati

volta un diritto "ai propri dati", un potere giuridico del soggetto sui dati che lo riguardano[145] acquisito tramite il *consenso*, che però può considerarsi pieno soltanto con riferimento al trattamento dei dati sensibili a causa delle numerose deroghe al principio. Inoltre, in tutte le "aree" della personalità, la legge ha innalzato le difese attraverso due disposizioni a contenuto sanzionatorio: la prima che ha esteso l'ipotesi di danno a seguito del trattamento dei dati la disciplina prevista dall'art. 2050 c.c., la seconda che prevede il risarcimento del danno non patrimoniale[146].

La legge ha, inoltre, ripreso molti aspetti della disciplina che erano stati fatti propri dalla direttiva europea, tra cui quelli maggiormente rilevanti: le definizioni di "trattamento"[147]e "dato personale", la previsione della suddetta Autorità preposta alla protezione dei dati personali, la cd. *notificazione,* i diritti dell'interessato e i rispettivi obblighi del titolare del trattamento. L'analisi specifica di tali aspetti dalla legge in esame saranno considerati in relazione alla protezione del citato *nocciolo duro della privacy* nel prossimo paragrafo.

2.1 Il primo riferimento ai dati sensibili nella normativa italiana

Come è stato evidenziato, la legge n. 675/1996 si era preoccupata di prevedere specifiche tutele per una particolare categoria di dati personali analogamente alle indicazioni provenienti dalla direttiva comunitaria. Infatti, al Capo IV rubricato *"trattamento dei dati particolari"* conteneva le disposizioni finalizzate a disciplinare il trattamento dei dati, tra gli altri, dei dati che erano stati individuati dall'art. 8 della suddetta direttiva: i dati sensibili (art. 22), oggetto della presente trattazione ma anche i dati giudiziari (art. 24) e gli altri dati particolari (art.24-*bis*). Anche in base all'indicazione europee, sin dalla prima effettiva regolazione in materia, vi era la convinzione che alcuni tipi di dati, per il loro contenuto, dovevano essere assoggettati a norme specifiche per la loro incisività nella sfera privata, nonostante parte della dottrina affermasse che fosse scorretto differenziare la disciplina in base ai dati trattati in quanto è soltanto in base al diverso utilizzo che si fa di detti dati e dal contesto giuridico-sociale nel quale sono calati che potrebbe porsi una distinzione tra le varie informazioni[148]. Superando tale impostazione, il legislatore del 1996 aveva compiuto la scelta, confermata nella normativa successiva, di delimitare all'interno della generale categoria dei dati personali, una più ristretta coincidente

[145] Zeno- Zencovich, *op. cit*., pp. 468-469.
[146] I riferimenti sono all'art. 18 e all'art.29, ultimo comma della legge.
[147] Si veda Secondo P. Zanelli, *La Legge N. 675 del '96: una strategia integrata di protezione per la privacy*, in *Contratto e Impresa*, 1997, p. 3 che sostiene che la nozione di "trattamento" previsto all'art. 1 della legge appare ampia, ai limiti della onnicomprensività, mostrando come il legislatore voglia estendere al massimo l'ambito di applicazione della normativa.
[148] In tal senso, si veda F. Maschio, *I dati sensibili*, in A. Clemente, *op. cit.* , pp. 213-217.

con il cd. *nucleo duro della privacy,* comprendente tutte quelle informazioni incidenti nella sfera più intima dell'individuo e che riguardano il tradizionale bisogno di segretezza[149]. Lo stesso legislatore, ha mantenuto anche la divisione, all'interno dei dati sensibili, di "informazioni" differenti basate sulle funzioni che queste assolvono e sulla loro natura: rientrano nella prima categoria, i dati relativi a una determinata sfera di azione del soggetto e quelli relativi ad alcune sue caratteristiche, stati o condizioni; della seconda, invece, fanno parte quelle informazioni che per la loro natura sono predisposte alla vita relazionale dell'individuo e perciò sono destinate ad essere condivise con altri soggetti, differentemente da altre[150].

Tali aspetti furono ripresi dall'art. 22, primo comma della legge che definiva tutto quello che rientrava nel concetto di dato sensibile[151] ossia: *"I dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale, possono essere oggetto di trattamento solo con il consenso scritto dell'interessato e previa autorizzazione del Garante."* Nel secondo comma, l'art. 22 prevedeva che la decisione adottata, con la quale il Garante poteva anche prescrivere misure e accorgimenti obbligatori, doveva essere comunicata entro il termine di trenta giorni decorsi i quali la mancata pronuncia equivale a rigetto. Il mancato rispetto del provvedimento adottato dal Garante veniva punito con la reclusione da tre mesi a due anni ai sensi dell'art. 37. Come ha sottolineato Rodotà[152], la "super protezione" attribuita al trattamento di tali dati deriva dalla doppia garanzia dell'autorizzazione e consenso, che sussiste anche nella disciplina attuale[153] e per tale ragione essi costituiscono il *nocciolo duro della privacy*[154].

In primo luogo, dalla lettura del primo comma di tale articolo, si nota come abbia una portata più espansiva dell'art. 8 della direttiva comunitaria perché non tutela soltanto il trattamento dei dati "che rivelano" le informazioni sensibili ma anche quelli "idonei a rilevare" ossia quelli che

---

[149] In tale senso A. De Cupis, *I diritti della personalità,* A. Cicu e F. Messineo e continuato da L.Mengoni *Trattato di diritto civile e commerciale*, IV, Milano, 1982, p.350, definisce tale sfera quella ricadente in *"certi particolari settori e manifestazioni della vita personale che la persona vuole maggiormente sottrarre all'altrui conoscenza conservando su di essi un segreto".*

[150] Per una disamina su tale distinzione all'interno dei dati sensibili si rimanda a R. Pardolesi (a cura di), *Diritto alla riservatezza e circolazione dei dati personali,* Volume primo, Milano, 2003, pp. 513-514.

[151] In V. Zeno-Zencovich, *Commento sub art. 22,* in E. Giannanotonio, M.G. Losano, V. Zeno-Zencovich (a cura di), *La tutela dei dati personali. Commentario alla l.675/1996,* II edizione, Padova, 1999, p.276, in cui l'autore sottolinea che tutte le legislazioni straniere contengono disposizioni particolari sui dati sensibili e quella che maggiormente si avvicinava all'art. 22 della legge italiana si trovi all'art. 7 della legge spagnola del1992.

[152]P. Zanelli, *op. cit.,* p. 3.

[153] Infatti, l'art. 26, comma 1 del *Codice della privacy* prevede ancora che *"I dati sensibili possono essere oggetto di trattamento solo con il consenso scritto dell'interessato e previa autorizzazione del Garante, nell'osservanza dei presupposti e dei limiti stabiliti dal presente codice, nonché dalla legge e dai regolamenti."*

[154] Parlano di tale "nocciolo duro" anche G. Buttarelli, *Banche dati e tutela della riservatezza,* Milano, 1995, p. 375 e V. Zeno-Zencovich, *Commento sub art. 22,* in *op. cit.*, 1999, p.274.

anche indirettamente o attraverso processi induttivi o presuntivi sono in grado di rivelare il bene protetto[155], come il nome o il cognome ma anche lo stato di famiglia. Alcuni, hanno persino individuato nella disciplina prevista all'art. 22, la diretta attuazione dell'art. 3 comma 2 della Costituzione, in quanto permetterebbe di rimuovere gli ostacoli che non permettono al cittadino di sviluppare appieno la sua personalità[156].

A integrare, poi, e chiarire il concetto di dato sensibile poi, è intervenuto più volte il Garante attraverso una serie di autorizzazioni relative a determinate categorie di titolari o di trattamenti[157] tra cui quelle più rilevanti quella sul trattamento dei dati sensibili sul luogo di lavoro e quella sul trattamento dei dati idonei a rilevare lo stato di salute e la vita sessuale[158] : in tali autorizzazioni sono previste regole applicabili alle modalità di trattamento dei dati sensibili e ai limiti imposti ai titolari di detti trattamenti[159]. Accanto poi a tali autorizzazioni, il Garante ha previsto anche una serie di decisioni in ordine a questioni relative all'applicazione del trattamento dei dati sensibili[160].

2.1.1 Le condizioni per la liceità del trattamento: il consenso scritto

La tutela rafforzata finalizzata alla citata "super protezione" di tali dati, prevista tutt'ora, avviene attraverso un *obbligo di forma* ed un *controllo "sociale"* per mezzo del Garante, al fine di garantire la persona contro il rischio di subire discriminazioni e/o limitazioni delle libertà personali costituzionalmente inviolabili[161].

Infatti, il primo comma della legge definiva le condizioni per il trattamento di tali dati: il *consenso scritto* dell'interessato e la previa autorizzazione del Garante. Entrambi necessari ma non sufficienti giacché la presenza di uno non escludeva l'altro.

Con riferimento al consenso, che è stata definita come la chiave di volta della disciplina, il Capo IV, volendo maggiormente tutelare tali categorie di dati, non derogava all'art. 11 che si riferiva alla disciplina del consenso per il trattamento di categorie comuni dei dati ma

---

[155] Così J. Monducci, *Diritti della persona e trattamento dei dati particolari*, Milano, 2003, pp. 2-7 sostiene che il legislatore non ha voluto dare un'interpretazione restrittiva della disposizione su tale aspetto, altrimenti avrebbe "ricopiato" disposizioni più ampie contenute in atti comunitari o internazionali quali l' art. 6 della Convenzione n. 108 del Consiglio d'Europa e l'art. 8 della più volte citata direttiva o da quelle contenute in disposizione da lui stesso formulate in passato come l'art. 7 dell'ordinamento dell'amministrazione di pubblica sicurezza.

[156] Cfr. R. Pardolesi (a cura di), *op. cit.*, pp. 514-524.

[157] Il decreto legislativo n.123 del 9 maggio 1997 contenente *Disposizioni integrative e correttive della legge del 31 dicembre 1996 n.675* ha previsto la possibilità di rilasciare d'ufficio tali autorizzazioni.

[158] La prima è l'autorizzazione generale n. 1/97, la seconda è la n. 2/97 successivamente modificate. Le altre riguardavano il trattamento dei dati sensibili da parte degli organismi di tipo associativo e delle fondazioni, dei liberi professionisti, da parte di "diverse categorie di titolari" e da parte di investigatori privati.

[159] V. Zeno-Zencovich, *Commento sub art. 22*, in *op. cit.*, 1999, pp. 280-281.

[160] Si fa riferimento ad alcuni comunicati che si riferivano soprattutto al trattamento di dati concernenti la salute.

[161] R. Pardolesi (a cura di), *op. cit.*, p. 513.

prevedeva una sua integrazione, mantenuta anche nella disciplina attuale: in tal senso, il consenso era considerato valido solo dopo aver avuto conoscenza delle informazioni all'art. 10; prestato espressamente, in forma specifica e per iscritto.

Con riguardo al primo aspetto, l'interessato al trattamento deve essere informato prima dell'inizio del trattamento circa: le sue finalità e modalità, le conseguenze di un rifiuto di rispondere, i soggetti o le relative categorie cui i dati possono essere diffusi e l'ambito di diffusione dei propri dati, i diritti e le generalità. Sempre l'art. 10, prevedeva che l'informativa poteva essere data oralmente o per iscritto a meno che l'interessato non fosse già a conoscenza delle informazioni. Con riferimento al cd. *consenso informato,* rileva come, grazie alla legge n. 675, sia stato introdotto anche in Italia un diritto paragonabile a quel *diritto all'autodeterminazione informativa* introdotto in Germania nel 1983 in una sentenza della Corte Costituzionale e inteso quale *"diritto del singolo di decidere in linea di principio autonomamente sulla cessione e sull'impiego dei suoi dati personali",* sancito poi dalla legge sulla protezione dei dati personali tedesca adottata nel 1990[162].

Il consenso deve essere poi *libero* ossia la volontà non deve essere viziata contrariamente dal caso in cui sia prestato in presenza di errore, violenza o dolo[163]; *espresso,* rendendo illegittimo il trattamento dei dati personali eseguito sulla base di un consenso presunto; e, infine *formulato specificamente* intendendosi che debba essere manifestato in relazione allo specifico trattamento, a specifiche operazioni dello stesso[164]. L'art. 22, integrando la disciplina dell'art. 11 e definendo una formula *"sacramentale",* rafforzava la tutela proprio con riferimento al consenso in quanto prevedeva *ad substantiam* la forma *scritta,* al fine di realizzare la certezza dell'atto, oltre che a prevedere la sua forma espressa da parte dell'interessato come accade per le categorie comuni di dati personali; contrariamente ad altri casi, in cui la legge non prevedeva neppure che l'interessato dovesse prestare il consenso[165].

[162] Così P. Zanelli, *op. cit.,* p. 7. In particolare, il principio dell'autodeterminazione informativa (informationelles Selbstbestimmmungsrecht) è stato coniato da una sentenza del Tribunale costituzionale tedesco in cui veniva riconosciuto come diritto fondamentale del cittadino. Tale diritto prevede un controllo sulle proprie informazioni personali, dunque accentuato dalla possibilità di effettuare trattamenti automatizzati e trovava il proprio fondamento costituzionale nel diritto alla personalità attribuito a tutti gli individui.

[163] Riccardo Imperiali, Rosario Imperiali, *La tutela dei dati personali, Vademecum sulla privacy informatica,* Il Sole 24 ore, 1997.

[164] Per un'analisi dettagliata della disciplina del consenso presente nella legge si rimanda a J. Monducci, *op. cit.,* pp. 10- 25.

[165] L'art. 12, lettera (f della legge n. 675 non prevedeva il consenso dell'interessato per lo svolgimento delle attività economiche.

2.1.2 Le condizioni per la liceità del trattamento: la previa autorizzazione del Garante

Adeguandosi a quanto disposto dalla direttiva comunitaria secondo cui i dati sensibili possono essere trattati solo con il consenso della persona interessata *"salvo nei casi in cui la legislazione dello stato membro preveda che il consenso non sia sufficiente",* la legge italiana seguendo l'orientamento di altri Paesi, aveva previsto anche il requisito autorizzatorio[166] per i dati sensibili, dotati di superiore capacità lesiva di quelli comuni. Secondo la disciplina, rimasta peraltro applicabile, prima dell'inizio di ogni attività di trattamento di tali dati, infatti, il titolare del trattamento ha l'obbligo di richiedere il rilascio di autorizzazioni attraverso l'invio della domanda su supporto cartaceo, informatico o telematico e utilizzando i modelli preposti dal Garante, quindi a meno che il Garante non voglia emanare "autorizzazioni generali" di cui si tratterà successivamente, il potere di iniziativa del provvedimento appartiene alla parte privata[167]. Tale provvedimento potrà essere di accoglimento o di rigetto e dovrà essere adottato e comunicato dal Garante entro 30 giorni dalla richiesta. Qualora il Garante ritenga che sia già stata rilasciata un'autorizzazione generale in materia non sarà tenuto ad adottare alcun provvedimento né comunicare al titolare che l'autorizzazione richiesta sia stata già rilasciata: infatti, le autorizzazioni ai sensi dell'art. 22 sono state ricondotte a quelle specifiche, mentre quelle generali erano state introdotte dal decreto legislativo n. 123/97.

Nel rilasciare tale autorizzazione, il Garante gode di una piena discrezionalità amministrativa al fine di soddisfare gli interessi all'art.1 della legge n.675/1996 alla cui tutela è preposta[168]. Anche l'autorizzazione concessa dal Garante, come la prestazione del consenso da parte dell'interessato, è finalizzata a tutelare l'interesse individuale di quest'ultimo nonostante la nozione di Autorità indipendente richiami quella di interesse collettivo e generale[169]. Il Garante, infatti, nel valutare la sussistenza delle condizioni per il rilascio ti tale provvedimento, deve contemperare l'esigenza del rispetto della riservatezza e delle libertà fondamentali degli interessati con l'interesse dell'aspirante titolare: nel fare ciò gode di ampia discrezionalità nella valutazione, potendo anche condizionare il rilascio dell'autorizzazione al rispetto di determinate prescrizioni. Al decorrere del termine previsto dalla legge senza alcun provvedimento adottato, il silenzio equivale a rigetto[170].

---

[166] L'autorizzazione è uno specifico atto amministrativo attraverso il quale il Garante garantisce all'aspirante titolare del trattamento dei dati sensibili la possibilità di trattare i dati sensibili, nei limiti delle disposizioni del provvedimento.

[167] Sempre entro 30 giorni dall'avvio del procedimento, il Garante può rilasciare anche un'autorizzazione temporanea qualora lo richiedano le circostanze

[168] J. Monducci, *op. cit.*, p. 28.

[169] D'Alberti, *Autorità indipendenti (diritto amministrativo),* in *Enciclopedia giuridica*, 1995, 1.

[170] J. Monducci, *op. cit.*, pp.25-31.

Bisogna poi evidenziare un ulteriore aspetto messo in rilevo dalla legge n. 675/1996 che si collega all'autorizzazione prevista per i trattamenti effettuati su tutte le categorie di dati personali, e che acquista maggiore rilevanza con riferimento a quelli sensibili: la notificazione al Garante. Tale disciplina era prevista all'art. 7 della legge e con una modifica introdotta dal decreto legislativo n. 467/2001, finalizzata a ridurre il numero delle notificazioni al Garante chiariva che tale meccanismo poteva essere previsto soltanto *"se il trattamento, in ragione delle relative modalità o della natura dei dati personali, sia suscettibile di recare pregiudizio ai diritti e alle libertà dell'interessato, e nei soli casi e con le modalità individuati con il regolamento di cui all'articolo 33, comma 3".* Nel caso di trattamento dei dati sensibili però non deve confondersi tra l'autorizzazione e la notificazione: la seconda deve essere effettuata, da parte del titolare, per tutti i trattamenti al contrario dell'autorizzazione che riguarda solo il regime dei dati sensibili. Una non segue necessariamente l'altra ma senza l'una e l'altra non può aver luogo il trattamento. Come si vedrà nel prossimo paragrafo, la disciplina prevista per la notificazione ha subìto un cambiamento di rotta con l'entrata in vigore del Codice della *privacy*.

2.1.3 Le deroghe alla disciplina delineata dall'art. 22

Vennero previste delle deroghe alla disciplina del consenso scritto dell'interessato e della previa autorizzazione del Garante applicabili al trattamento dei dati sensibili, introdotte con successive modifiche apportate alla disposizione in esame.[171]

Il legislatore con l'introduzione del comma 1-*bis* dell'art.22 aveva previsto infatti che la disciplina del comma 1 non si applicasse *"ai dati relativi agli aderenti alle confessioni religiose i cui rapporti con lo Stato siano regolati da accordi o intese ai sensi degli articoli 7 e 8 della Costituzione, nonché relativi ai soggetti che con riferimento a finalità di natura esclusivamente religiosa [..]"*: aveva voluto così contemperare l'esigenza di tutela della *privacy* con quella di non porre ostacoli al libero esercizio del culto religioso, garantito dalla Costituzione. Tale disciplina non si applicava, all'art. 1-*ter*, altresì *"ai dati riguardanti l'adesione di associazioni od organizzazioni a carattere sindacale o di categoria ad altre associazioni, organizzazioni o confederazioni a carattere sindacale o di categoria."* Le opinioni e l'aderenza a tali associazioni sono state considerate dal legislatore aventi natura pubblica e le stesse associazioni hanno un interesse a divulgarle il più possibile in modo da non rappresentare un rischio per le libertà tutelate dalla disposizione.

Invece, il comma 3 dell'art. 22 ha poi previsto che la disciplina non si applicasse ai soggetti

[171] Le modifiche furono apportate dai decreti legislativi dell'11 maggio 1999 n.135 e del 28 dicembre 2001 n. 467.

pubblici, escludendo per questi, ad eccezione di quelli economici, la necessità del consenso e dell'autorizzazione del Garante che poteva avvenire *"solo autorizzato da espressa disposizione di legge, nella quale siano specificati i dati che possono essere trattati, le operazioni eseguibili e le rilevanti finalità di interesse pubblico perseguite."* Doveva trattarsi di un'espressa norma di legge che doveva individuare i dati oggetto del trattamento e definire e circoscrivere le finalità di interesse pubblico che si volevano soddisfare con quel dato trattamento.

Ancora, altra deroga alla necessità del consenso per alcune tipologie di dati sensibili, era prevista anche dal quarto comma dello stesso art. 22 ma in ogni caso con la previa autorizzazione del Garante. In particolare alla lettera b) prevedeva tale disciplina per tutelare uno dei principi costituzionali supremi, quello del diritto alla salute legittimando al trattamento qualora vi fosse impossibilità fisica o giuridica dell'interessato a prestare il consenso.

Pur esulando dall'ambito di riferimento del presente elaborato, sempre nel Capo IV della legge erano previsti oltre ai riferimenti dei dati sensibili, anche quelli *giudiziari* e quelli *particolari nell'esercizio della professione giornalistica.* È, tuttavia, opportuno evidenziare rispetto a questi ultimi, *ex* art. 25, che anche in questo caso il legislatore aveva posto l'esigenza di bilanciare il diritto alla riservatezza del nucleo duro con quello del diritto di cronaca dei giornalisti. La modifica alla legge aveva infatti previsto l'eliminazione del sistema protettivo basato sul binomio consenso/autorizzazione, prevedendo il rispetto dell'intera categoria dei dati sensibili ad un codice deontologico, poi effettivamente adottato[172].

3. Il Codice in materia di protezione dei dati personali

La legge n. 675/1996 era intervenuta in un momento in cui lo sviluppo delle tecnologie aveva permesso una diffusione dell'utilizzo dell'informatica ad un numero sempre crescente di utenti rispetto al passato. Nei circa sette anni di vigenza, il quadro tecnologico mutò ulteriormente, grazie alle crescenti possibilità telematiche, le nuove tecniche di digitalizzazione nonché le possibilità di tracciare i movimenti delle persone incidendo sulla loro libertà di movimento[173]: per tali ragioni, la legge del 1996 fu considerata come obsoleta e dunque abrogata dal *Codice per la protezione dei dati personali*[174] attualmente in vigore. In linea con una tendenza di

[172] Il codice deontologico *relativo al trattamento dei dati personali nell'esercizio dell'attività giornalistica* fu approvato dopo una serie di dibattiti e rinvii il 29 settembre 1998.

[173] Esempi sono le tecniche di riconoscimento facciale oppure le informazioni relative all'ubicazione di cellulari e persone attraverso reti digitali o satellitari.

[174] Il decreto legislativo del 30 giugno 2003, n. 196 fu emanato in base alla legge delega del 24 marzo 2001 n.127. Pubblicato in G.U. il 29 luglio 2003 ed entrato in vigore il 1 gennaio 2004, ha introdotto nell'ordinamento italiano il *Testo Unico* in materia di privacy.

codificazione e sistematizzazione della disciplina giuridica di quegli anni[175], il principale aspetto innovativo del *Codice* sta nel passaggio ad una legge *dinamica* dato il ruolo attivo di esecuzione e controllo da parte del Garante[176] e non più *statica*, legata alla tutela della riservatezza attraverso le norme dell'ordinamento. Emerge, inoltre, il diritto alla protezione dei dati personali, già "costituzionalizzato" nel contesto europeo nell'art. 8 della Carta di Nizza[177]. Il legislatore delegato aveva previsto l'adozione di un Testo Unico in materia di *privacy* da attuarsi attraverso un coordinamento tra le norme allora vigenti in materia, apportandogli modificazioni e integrazioni e al fine di assicurargli una *"migliore attuazione"*[178]*:* la previsione di un T. U. indusse il Governo a istituire una commissione di esperti presso il Dipartimento della funzione pubblica. Non rientrando nella categoria dei cd. *Testi Unici misti* contenenti anche norme regolamentari, il T.U. assunse la denominazione di *Codice in materia di protezione dei dati personali.* Rappresentò, infatti, la prima esperienza di codificazione e coordinamento normativo di tutte le disposizioni ricadenti in materia e non solo: in quanto fu il frutto di *"un'opera di armonizzazione e di adeguamento ai principi elaborati nel corso degli anni dalla dottrina e modellando le norme più significative secondo le interpretazioni più sicure della giurisprudenza pratica e delle decisioni rese dal Garante per la protezione dei dati personali"*[179]. A tal proposito, in riferimento proprio ad alcune pronunce del Garante, le attuali definizioni di *titolare, responsabile e incaricati* al trattamento dei dati personali presenti nel *Codice*[180] rappresentano il recepimento di taluni indirizzi dell'Autorità[181].

Il *Codice,* articolato in tre parti e 24 titoli per un totale di 186 articoli, si estende in realtà ben oltre attraverso alcuni allegati che ne costituiscono parte integrante: i codici di deontologia[182] in

---

[175] Oltre al *Codice della privacy,* nel 2003 venne anche adottato con decreto legislativo n. 259, il cd. *Codice delle comunicazioni elettroniche.*

[176] Le disposizioni riguardanti l'istituzione, organizzazione dell'Ufficio e i poteri del Garante sono contenute nel Titolo II, Parte III del *Codice;* tuttavia, è possibile rinvenire ulteriori norme che attribuiscono all'Autorità poteri specifici in relazioni a situazioni particolari.

[177] Si veda V. Zeno- Zencovich, *Ragioni ed obiettivi del Codice,* in F. Cardarelli, S. Sica, V. Zeno Zencovich (a cura di), *Il codice dei dati personali: temi e problemi,* Milano, 2004, pp. 3-5.

[178] Art. 1, comma 4 della legge delega n.127/2001.

[179] G. P. Cirillo, *Il nuovo codice in materia di trattamento dei dati personali. Il diritto alla protezione dei dati e gli schemi di riferimento relativi alla tutela dei diritti fondamentali della persona e dei cd. diritti dell'interessato,* in G. Santaniello (a cura di), *La protezione dei dati personali,* in *Trattato di diritto amministrativo,* diretto da Santaniello G., Volume trentaseiesimo, Padova, 2005, p.3.

[180] Rispettivamente definiti all'art. 4 lettera f), g) e h) del Codice.

[181] Con riferimento alla nozione di *titolare* e *responsabile,* il Garante aveva ampliato concettualmente le due figure già previste dalla legge n.675/1996 nel Parere del 9 dicembre 1997, in *Boll.,* n.2, 44 e 45; al contrario, la figura dell'*incaricato* che non aveva trovato un'esplicita definizione nella legislazione precedente, fu previsto nella Nota del Garante dell'8 giugno 1999, in *Boll.,* n. 9, 58, che l'aveva distinto dal *responsabile* del trattamento.

[182] Si fa riferimento soprattutto ai codici di deontologia sul trattamento dei dati personali: nell'esercizio dell'attività giornalistica; per scopi storici; a scopi statistici. Ma anche ai codici di deontologia e buona condotta per i trattamenti di dati personali per scopi statistici e scientifici; per i sistemi informativi gestiti da soggetti privati in tema di crediti al consumo, affidabilità e puntualità nei pagamenti; per i trattamenti di dati personali effettuati per svolgere investigazioni difensive; per il trattamento dei dati personali effettuato a fini di informazione commerciale.

quanto il Codice attribuisce una particolare importanza alla capacità di autodeterminazione dei destinatari della disciplina; il cd. *"Disciplinare tecnico"* sulle misure minime di sicurezza ad integrazione degli art. 33-36 del Codice[183]; e, infine anche se non allegate, le autorizzazioni generali per vari settori di attività, che oggetto di un successivo paragrafo, si riferiscono soprattutto al trattamento dei dati sensibili in particolari settori. Nella Prima Parte, il *Codice* contiene le disposizioni generali ossia le finalità, i principi alla base della legge, le definizioni degli istituti e la disciplina generale; nella Seconda, sono invece previste disposizioni particolari per specifici settori ad integrazione o in deroga a quelle della Prima Parte; infine, la Terza disciplina il meccanismo della tutela dell'interessato da attivarsi per i trattamenti illeciti dei dati personali[184] e l'assetto sanzionatorio penale e amministrativo. Dunque, il sistema è caratterizzato da una linearità di fondo: all'inizio sono previsti alcuni principi generali della materia e di diritti spettanti agli interessati (rispettivamente il Titolo I e il Titolo II del Codice) che si applicano a tutti i settori e con riferimento a ciascuna tipologia di soggetto; prevede, poi, con maggiore dettaglio le regole generali per tutti i trattamenti dei dati (Titolo III ma anche Titolo IV, V, VI, VII) in cui opera una distinzione tra i trattamenti effettuati da soggetti pubblici (Capo II) e quelli effettuati da soggetti privati (Capo III); per poi terminare con gruppi di norme che si distinguono per il relativo ambito di applicazione e da particolari funzioni svolte da soggetti specifici[185](Parte II)[186]. La logica fatta propria del Codice non è dunque solo riproduttiva di quella della legge del 1996 ma apporta molti elementi di novità dal punto di vista contenutistico.

In primo luogo, introduce la figura del *"diritto alla protezione dei dati personali",* preannunciato dal Garante nel 2002[187], non menzionata dalla legge n.675/1996 e adesso disciplinata espressamente agli art. 1 e 2 del Codice. Il diritto alla protezione dei dati personali viene riconosciuto solennemente come diritto fondamentale e autonomo. L'art. 1 prevede che *"chiunque[188] ha diritto alla protezione dei dati personali che lo riguardano"*[189] mentre all'art. 2 è espressamente qualificato come uno dei diritti e delle libertà fondamentali con cui si estende la garanzia costituzionale. Seguendo tale impostazione, il Codice intende passare da una tutela

[183] Sempre negli allegati sono previsti anche quello relativo ai trattamenti non occasionali effettuati o in ambito giudiziario o per fini di polizia e la Tavola di corrispondenza dei riferimenti previgenti al codice in materia di protezione dei dati personali.

[184] Tale sistema di tutela ha il cardine nell'Ufficio del Garante.

[185] Tra queste ultime, quelle concernenti il trattamento dei dati personali in ambito sanitario, giudiziario o pubblico, o quelle relative al sistema bancario, finanziario e assicurativo e quelle in materia di comunicazioni elettroniche.

[186] Si veda S. Kirschen, *Codice della privacy, tradizione ed innovazione*, in R. Panetta (a cura di), *Libera circolazione dei dati e protezione dei dati personali*, Milano, 2006, pp. 33-34.

[187] Il Garante aveva definito tale diritto nella Relazione annuale del 2002. Tale Relazione è consultabile su *www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/128281*.

[188] In riferimento sia alle persone fisiche sia a quelle giuridiche sia agli enti.

[189] Comma così modificato, da ultimo, dall'art. 14, comma 1, della legge 4 novembre 2010, n. 183, che ha soppresso il secondo periodo del comma aggiunto dall'art. 4, comma 9, della legge 4 marzo 2009, n. 15.

finalizzata a proteggere la persona dalle ingerenze nella sua sfera privata all'attribuzione all'*interessato*[190] di maggiori poteri decisionali con riferimento all'impiego e alla destinazione delle sue informazioni personali: a tal proposito questo diritto non opera solo come un obbligo negativo ossia a tutela di condotte lesive e invasive di una controparte pubblica o privata, ma anche come una delle cd. *obbligazioni positive* poste a carico dei Paesi che aderiscono alla Convenzione europea dei diritti dell'Uomo[191], al fine di conferire tutela effettiva ai diritti fondamentali e in particolare al diritto *al rispetto della vita privata e familiare.* Proprio la connotazione di diritto fondamentale che il *Codice* garantisce al diritto in questione, è da mettere in rilievo: non essendoci una menzione espressa in Costituzione di tale situazione soggettiva, il legislatore l'ha ricondotto allo sviluppo delle tecnologie informatiche e alla consapevolezza dei pericoli da essa creati[192]. Alcuni autori parlano pertanto di un "*effetto paracostituzionale"* degli articoli. 1 e 2 del *Codice*, pur avendo il carattere formale di norma ordinaria, dato che specifica ed implementa nel diritto interno garanzie, che come si è detto, sono state consolidate a livello europeo[193].

Secondo tale impostazione, il legislatore sembra aver voluto distinguere il diritto alla protezione dei dati personali dalle altre situazioni giuridiche soggettive quali la *riservatezza* e l'*identità personale* già previsti dalla legge n.675/1996, confermando l'autonoma rilevanza del primo all'interno dei diritti fondamentali della persona, dato che appare evidente come il primo copra un ambito fenomenico più esteso rispetto, ad esempio, a quello della tutela della sfera privata del diritto alla riservatezza. Tuttavia, non mancano posizioni contrarie in tal senso, che sottolineano come la previsione del *diritto alla protezione dei dati personali* all'interno del Codice non innovi rispetto alle altre situazioni nominate.[194]

Ultima considerazione da fare è che la previsione di tale nuovo diritto era stato in realtà già riconosciuto e anticipato dall'art. 8 della Carta dei diritti fondamentali dell'Unione europea che prevede *un diritto alla protezione dei dati a carattere personale.* È proprio nella Carta che *"[..]*

---

[190] Sul punto il Codice si differenzia dalla legge n. 675/96 che all'art. 1 differenziava tra la protezione dei diritti e delle libertà fondamentali della persona fisica e di altri diritti degli enti collettivi, mentre l'art. 2 del *Codice* parla indistintamente ai diritti e alle libertà fondamentali dell'interessato.

[191] Così G. Buttarelli, *Profili generali del trattamento dei dati personali,* in G. Santaniello (a cura di), *op. cit.,* p. 76.

[192] G. Resta, *Il diritto alla protezione dei dati personali,* in in F. Cardarelli, S. Sica, V. Zeno Zencovich (a cura di), *op. cit.,* pp. 31-32.

[193] Si veda ancora G. Resta, *ibidem,* p. 41. In senso contrario, A. Bardusco, *Commento all'art. 1,* in AA. VV., *Codice della privacy. Commento al decreto legislativo 30 giugno 2003, n.196,* I, Milano, 2004, p.12 e ss., che sostiene *"[..] per quando solennemente enunciato esso rimane un principio dotato sì di forza normativa; ma pur sempre a livello di legge ordinaria."*

[194] Si veda G. P. Cirillo, *ivi*, p. 25 che sostiene che *"[..] l'impressione di chi scrive è che, nonostante la proclamazione del nuovo diritto, in punto di tutela, le cose non siano cambiate rispetto alla vigenza della legge n.675/1996. [..]"*. Per una disamina dettagliata sul rapporto tra i vari diritti della personalità si rimanda a C. Lo Surdo, *Gli strumenti di tutela del soggetto "interessato" nella legge e nella sua concreta applicazione,* in R. Pardolesi (a cura di), *Diritto alla riservatezza e circolazione dei dati personali,* Volume I, Milano, 2003, p. 617 e ss.; V. Cuffaro, V. Ricciuto (a cura di), *La disciplina del trattamento dei dati personali*, Torino, 1997, p. 225 e ss.

si opera una distinzione tra il rispetto della propria vita privata e familiare (art. 7) e il diritto alla protezione dei dati personali (art.8). [..] Nel diritto al rispetto della vita privata e familiare si manifesta soprattutto il momento individualistico, il potere si esaurisce sostanzialmente nell'escludere interferenze altrui. [..] La protezione dei dati, invece, fissa regole sulle modalità di trattamento, si concretizza nei poteri di intervento."[195]In sostanza, il legislatore italiano recepisce questa impostazione, riconoscendo all'interessato un pieno diritto soggettivo a sindacare, già al *gestore* dei dati, vari aspetti sulle modalità di raccolta e utilizzo delle proprie informazioni.

La protezione dei dati personali introduce il secondo aspetto innovativo introdotto dal *Codice*: la sua connotazione di diritto fondamentale induce a ritenere che ogni sua limitazione debba rispettare i canoni di ragionevolezza e proporzionalità e non possa intaccarne il contenuto essenziale[196]. L'art. 3 infatti introduce il *principio di necessità nel trattamento dei dati*[197] che si riferisce espressamente ai contesti informatici e telematici che *"sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi.* L'utilizzo di questi ultimi, secondo la disposizione, deve avvenire soltanto quando siano indispensabili per il raggiungimento di finalità determinate, legittime, esplicite e per il periodo necessario al raggiungimento di queste ultime, nonché l'affermazione della necessaria pertinenza e non eccedenza delle informazioni raccolte[198]. Dunque, nell'impostazione della disposizione, i *software* devono essere configurati in modo tale da preferire l'uso di dati anonimi piuttosto che quelli personali o quelli che consentono un'identificazione diretta dell'interessato[199]: in questo modo, si intende favorire una programmazione di sistemi informativi più attenta ai profili sostanziali della protezione dei dati personali. Inoltre, l'importanza di tale principio è stata sottolineata dall'Autorità Garante nell'adozione delle nuove, sette autorizzazioni generali al trattamento dei dati sensibili e giudiziari, di cui si tratterà in un successivo paragrafo.

Da un punto di vista sistemico, invece, il *Codice*, contrariamente alla legge n. 675/1996 contiene una ripartizione che tiene conto della diversa natura dei soggetti, pubblici e privati, titolari dei trattamenti dei dati personali e una distinzione tra regole generali e regole specifiche anche in base a tale parametro: in questo modo, il decreto legislativo, tiene conto, diversamente

---

[195] S. Rodotà, *Tra i diritti fondamentali ed elasticità della normativa: il nuovo Codice sulla privacy,* in *Eur. Dir. Priv.*, 2004, p. 2.

[196] Il principio si ricava dall'art. 52, primo comma della Carta di Nizza:" *Eventuali limitazioni all'esercizio dei diritti e delle libertà riconosciuti dalla presente Carta devono essere previste dalla legge rispettare il contenuto essenziale di tali diritti e libertà."*

[197] Il principio rappresenta una versione arricchita del cd. *principio di minimalizzazione* presente all'art. 3° nel *Bundesdatenschutzgesetz* tedesco nel 2001.

[198] Si veda S. Kirschen, *op. cit.*, pp. 69-70.

[199] R. Acciai, S. Melchionna, *Le regole generali per il trattamento dei dati personali,* in R. Acciai (a cura di), *Il diritto alla protezione dei dati personali. La disciplina sulla privacy alla luce del nuovo Codice*, Rimini, 2004, p.71.

da quanto accadeva in precedenza, della peculiarità del settore pubblico e delle funzioni che esso svolge caratterizzate da "interferenze" con la tutela dei dati personali.[200] Come in passato, all'art. 18 viene ribadito come i soggetti pubblici possano trattare i dati personali solo *"per lo svolgimento delle funzioni istituzionali":* ancora una volta, il legislatore conferma che la qualità pubblica del soggetto non gli conferisce alcun potere speciale, in quanto occorre sempre una norma per poter svolgere queste funzioni[201].

Il *corpus* normativo del Codice ricomprende poi tutti gli aspetti salienti della disciplina già presenti nella legislazione precedente, con l'apporto di qualche modifica: i diritti dell'interessato, l'informativa da parte del titolare, il conseguente consenso dell'interessato, il trasferimento dei dati in Paesi terzi, l'obbligo di notificazione e il sistema sanzionatorio in caso di trattamento illecito. Questi saranno considerati nel prossimo paragrafo con riferimento al trattamento dei dati oggetto del presente elaborato, ossia quelli sensibili.

3.1 Una nuova disciplina dei dati sensibili nel Codice

Il *Codice della privacy* sul modello delineato dalla legge n.675/1996 riprende la struttura concentrica delle tipologie di dati: al centro emergono i dati sensibili, mentre nei cerchi più esterni quelli "comuni", delineando una graduatoria di valori e di mezzi protettivi a seconda della natura dei dati.[202] Anche il *Codice* recepisce la nozione di *nocciolo duro* della riservatezza sul quale ci si è già soffermati, presente nella normativa comunitaria e ancora prima da quella del Consiglio d'Europa. A ben vedere, tali norme avevano a loro volta ripreso disposizioni che si rifacevano a dati sensibili nelle legislazioni straniere: la prima si rinveniva nell'art.4 della legge svedese del 1978, ma quella che maggiormente si avvicina alla disciplina italiana in materia è contenuta all'art. 7 della legge spagnola del 1992 che condiziona al consenso espresso e scritto da parte dell'interessato, la liceità del trattamento dei dati che rivelano l'ideologia e la religione.[203]

Per tanto, anche nel *Codice* il *nucleo duro* è costituito non solo dalle informazioni che esprimono una particolare esigenza di riservatezza in quanto attinenti a fatti particolarmente intimi della vita privata dell'individuo, come i dati che rivelano lo stato di salute e le abitudine sessuali ma anche quelle informazioni che seppure non rientrano in tale sfera, devono comunque godere di una particolare tutela al fine di evitare che dalla loro circolazione possano

[200] Il Capo II, Titolo III, Parte I del *Codice* contiene le *Regole ulteriori per i soggetti pubblici* che non riguardano gli enti pubblici economici.
[201] In tal senso S. Kirschen, *op. cit.*, pp. 38-39.
[202] R. Gamberale, *Trattamento dei dati sensibili,* in R. Panetta (a cura di), *op. cit.,* p.1071.
[203] Per ulteriori esempi di legislazioni straniere in materia di dati sensibili si rinvia ancora a R. Gamberale, *ibidem,* p.1072.

nascere delle situazioni discriminatorie nei confronti dei soggetti ai quali si riferiscono, come quelli relativi alla razza, alle opinioni politiche e sindacali o al credo religioso. Con riferimento a questi ultimi, alcuni parlano addirittura, di *"paradossale circostanza"* data dal fatto che dati tipicamente pubblici *"[..] ricevono il massimo di protezione privata"*[204]. Quindi i dati sensibili rivelano aspetti non esclusivamente materiali o informativi ma piuttosto indicano aspetti diversi della personalità: ogniqualvolta ci si trova dinanzi a tali tipi di informazioni, il soggetto al quale essi si riferiscono non può che essere una persona fisica[205].

Non sono stati oggetto di particolare attenzione, da parte del legislatore italiano, contrariamente ad altri Paesi, alcune informazioni come i provvedimenti disciplinari o i dati raccolti per scopi di assistenza sociale[206]. Né le informazioni, con riferimento ai rapporti economici, finalizzate a rilevare la situazione patrimoniale e finanziaria del soggetto interessato: anche il Garante era intervenuto sul punto sostenendo che i dati riguardanti le retribuzioni e le indennità corrisposte dai concessionari di pubblici servizi *"[..] soddisfano l'interesse pubblico alla conoscenza della prassi in atto presso soggetti che operano, di regola, secondo norme privatistiche ed in base a logiche di mercato, ma svolgono attività aventi una particolare connotazione pubblicistica."*[207]

Inoltre, ad un livello intermedio di "sensibilità", ci sono poi i *dati giudiziari*[208] che, come vedremo nei prossimi paragrafi, hanno ricevuto all'interno del *Codice* una disciplina, da parte dei soggetti pubblici, sostanzialmente analoga a quella dei dati sensibili.

Nell'impianto normativo precedente al *Codice*, la disciplina sul trattamento dei dati sensibili era contenuta all'art. 22 della legge n. 675/1996 con le successive modifiche intervenute[209]: in un'unica norma era contenuta la definizione di *dato sensibile* e gli adempimenti che erano tenuti a rispettare tanto i soggetti pubblici tanto quelli privati nel trattamento di tale categoria di dati. La prima differenza del *Codice* sta nell'aver collocato la definizione di dato sensibile,

---

[204] Così G.B. Ferri, *Relazione al Convegno di Alghero del 19-20 settembre 1997, cit.* in V. Cuffaro, V. Ricciuto (a cura di), *op. cit.*, p.302 che sottolinea come questo tipo di informazioni vengono considerate sotto l'etichetta della *privacy* che per molti aspetti non avrebbero nulla in comune se non un legame estrinseco e occasionale.

[205] Si veda C. Rigotti, *Il nuovo testo unico sulla privacy*, Trento, 2003, p. 18.

[206] Con riferimento ai primi, il decreto reale olandese del 19 febbraio 1993 che disciplina i dati sensibili, all'art. 1 si riferisce anche a quelli aventi natura disciplinare; con riferimento ai secondi, invece, la legge olandese tutela i dati a sfondo psicologico, quella finlandese quelli concernenti servizi sociali, aiuti economici, assistenza sociale o altri servizi correlati e, infine quella islandese pone un divieto di trattamento dei dati riguardanti le difficoltà di inserimento sociale.

[207] Così il Garante per la protezione dei dati personali nel suo Comunicato del 17 settembre 1997, consultabile su *www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1055114*, sostiene che devono essere riservate quelle informazioni diverse dalla redistribuzione-tipo e relative a circostanze familiari quali l'esistenza di determinate ritenute previdenziali ed assistenziali, cessioni di stipendio, deleghe per iscrizioni ad associazioni sindacali.

[208] L' art. 4, comma 1, lettera e) definisce i dati giudiziari come *"i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del d.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale".*

[209] Si fa riferimento al decreto legislativo n.135/1999 e del n.467/2001 modificativi e integrativi della legge n. 675/1996.

sostanzialmente coincidente con quella precedente, all'art. 4[210] dello stesso che contiene le *definizioni* applicabili alla materia distinguendosi da quella più "generale" di dati personali[211]: sono elencati tassativamente tutti i dati che rientrano in tale categoria. La seconda, più rilevante, sta nell'aver distinto e disciplinato separatamente il trattamento di tali categorie di dati da parte dei soggetti pubblici e privati,[212] come sarà esaminato nei paragrafi seguenti.

3.1.1 Il trattamento dei dati sensibili da parte dei soggetti pubblici

Una disciplina parzialmente nuova introdotta dal decreto legislativo n.196 del 2003 è quella della differenziazione del regime previsto per il trattamento di dati sensibili (art. 20) e giudiziari (art.21), non prevista dalla norma comunitaria di recepimento[213]. Anche se l'analisi sulla disciplina del trattamento dei dati giudiziari esula dall'ambito del presente elaborato, è opportuno rilevare come le due disposizioni si distinguano in pochi punti[214] e che i tre presupposti che autorizzano il trattamento dei dati sensibili da parte dei soggetti pubblici, che adesso vedremo coincidere con le *rilevanti finalità di interesse pubblico, tipi di dati e di operazioni,* sono i medesimi che legittimano il trattamento da parte dei stessi soggetti dei dati giudiziari.

Prima di illustrare i principi applicabili al trattamento dei dati sensibili da parte di tali soggetti, occorre fare una considerazione preliminare. L'art. 18 in apertura del Capo II specifica che le disposizioni in esame si applicano a tutti i soggetti pubblici con eccezione degli enti pubblici economici per i quali, invece, è previsto il regime applicabile ai soggetti privati che sarà analizzato nel prossimo paragrafo. La disposizione chiarisce poi che i soggetti pubblici, fatte salve le disposizioni riguardanti medici e organismi sanitari non debbano richiedere il consenso dell'interessato: questo non rappresenta un requisito per il trattamento e non deve essere né richiesto o sollecitato dalle pubbliche amministrazioni. Inoltre, tali soggetti possono trattare dati

---

[210] All' art. 1, comma 4, lettera d), i dati sensibili sono definiti come *"i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale."*

[211] Alla lettera b), del citato art. 4 comma 1 del *Codice* sono definiti come *"qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale".*

[212] I primi rispettivamente agli articoli 20-22, i secondi, per i quali si riprende sostanzialmente la disciplina previgente, agli art. 26-27 del *Codice*.

[213] Infatti, tale differenziazione in base alla natura soggettiva degli enti preposti al trattamento non era prevista dall'art. 8 della citata direttiva 95/46/CE.

[214] L'art. 21 del *Codice* equipara l'*espressa disposizione di legge* dove vengono specificati i tipi di dati che vengono trattati, le operazioni eseguibili e le finalità di interesse pubblico perseguibili prevista anche dall'art. 20, ad un *provvedimento del Garante* che abbia lo stesso contenuto; quando poi, la legge specifichi le finalità di rilevante interesse pubblico ma non le tipologie di dati e le operazioni eseguibili, si applica la stessa disposizione dei dati sensibili prevista all'art. 20, comma 2.

soltanto per lo svolgimento delle funzioni istituzionali intese come *"[..] attività rivolte al perseguimento degli interessi collettivi, e può trovare fondamento, oltre che nella legge anche in atti di indirizzo emanati dagli organi di governo dell'Ente, a condizione che si tratti di atti assunti legittimamente"* [215].

Passando alla disciplina in esame, l'art. 20 riproduce l'art. 22, comma 3 e 3-*bis* della legge n. 675/1996 introducendo però delle modifiche: il primo comma prevede che il trattamento di tali dati da parte dei soggetti pubblici *"è consentito solo se autorizzato da espressa disposizione di legge nella quale sono specificati i tipi di dati che possono essere trattati e di operazioni eseguibili e le finalità di rilevante interesse pubblico perseguite."* La dottrina ha risolto il problema interpretativo riguardante il concetto di *finalità di interesse pubblico:* la presenza di tale interesse è valutata implicitamente da parte del legislatore nel momento in cui riconosce al soggetto pubblico la facoltà di trattare di dati sensibili e di effettuare le conseguenti operazioni su di essi[216]: tuttavia, è stato sostenuto da più parti che il legislatore nazionale non possa godere di un'illimitata discrezionalità nell'individuazione delle finalità rilevanti per effetto della collocazione del diritto alla protezione dei dati personale, quale diritto fondamentale nella Carta di Nizza[217]. Il secondo comma, prevede che quando la disposizione di legge specifichi solo la finalità di rilevante pubblico ma non i tipi di dati e di operazioni eseguibili, *"il trattamento è consentito solo in riferimento ai tipi di dati e di operazioni identificati e resi pubblici a cura dei soggetti che ne effettuano il trattamento, in relazione alle specifiche finalità perseguite nei singoli casi e nel rispetto dei principi di cui all'articolo 22, con atto di natura regolamentare adottato in conformità al parere espresso dal Garante ai sensi dell'articolo 154, comma 1, lettera g), anche su schemi tipo."* Con riferimento a suddetto caso, occorre sottolineare l'innovazione del Codice rispetto alla disposizione precedente derivante dal citato decreto legislativo n.135/1999. In primo luogo, il legislatore ha chiarito definitivamente attraverso *quale* atto i soggetti individuano i tipi di dati e di operazioni eseguibili: secondo l'art. 20 del *Codice*, deve avere *natura regolamentare*[218]. Nella vigenza della precedente legge, invece, la Presidenza del Consiglio aveva inviato una nota[219] a tutti i Ministeri, precisando che tale attività dovesse avvenire con atti di natura ricognitiva e non regolamentare. Era in più casi intervenuto

[215] Così G. Modesti, *Commento breve al D.LGS.VO N. 196/2003. Codice in materia di protezione dei dati personali*, in *www.diritto.it/archivio/1/20807.pdf*, ottobre 2002, s, p.18.
[216] R. Gamberale, *op. cit.*, p. 1098.
[217] Così F. Cardarelli, *Il Codice dei dati personali*, in F. Cardarelli, S. Sica, V. Zeno Zencovich (a cura di), *op. cit.*, p.238.
[218] L'art. 181, comma 1 lettera a) del *Codice* prevede che i soggetti pubblici che non avevano, al momento dell'introduzione della disposizione, adottato il regolamento di competenza, avrebbero dovuto adottarlo entro il 28 febbraio 2007.
[219] Il riferimento è alla Circolare n. DAGL/643 Pres. 1998 del 1 dicembre 1999 consultabile su *www.governo.it/la-presidenza-del-consiglio-dei-ministri*.

il Garante e in particolare nel gennaio 2002[220], segnalando la necessità da parte del Governo di adottare interventi opportuni in materia di dati sensibili e giudiziari da parte di soggetti pubblici, aveva espresso che le operazioni eseguibili da tali soggetti su detti dati dovevano avvenire attraverso un atto regolamentare e non di tipo amministrativo interno, garantendo una maggiore autorevolezza e stabilità. A tale aspetto si ricollega seconda innovazione apportata dal *Codice* rappresentata dal fatto che tali atti devono essere adottati in conformità al parere reso dal Garante rilasciato sui relativi schemi o anche su schemi tipo.[221] Il terzo comma dell'art. 20 definisce poi una terza modalità di trattamento dei dati sensibili da parte dei soggetti pubblici, quando non è previsto da espressa disposizione di legge: essi *"possono richiedere al Garante l'individuazione delle attività, tra quelle demandate ai medesimi soggetti dalla legge, che perseguono finalità di rilevante interesse pubblico e per le quali è conseguentemente autorizzato, ai sensi dell'articolo 26, comma 2, il trattamento dei dati sensibili. Il trattamento è consentito solo se il soggetto pubblico provvede altresì a identificare e rendere pubblici i tipi di dati e di operazioni nei modi di cui al comma 2."*[222] È evidente come in tali casi l'autorizzazione sostituisca la necessità del parere del Garante, previsto al comma precedente, solamente se individui anche i tipi di dati e le operazioni eseguibili su di essi oltre che le attività di tali soggetti[223]. Il comma 3 rimanda a successivo art. 26 del *Codice*[224] che stabilisce le modalità e le procedure che il Garante rilascia su richiesta dei soggetti privati che debbano trattare di dati sensibili, quando tale trattamento non rientri nelle autorizzazioni standard adottate dall'Autorità. La disposizione considera il rapporto tra la *legge* e l'autorizzazione del Garante: solo quest'ultimo può intervenire per individuare attività di rilevante interesse pubblico, qualora manchino espresse previsioni normative[225]. L'articolo 20 si chiude con il comma 4 che prevede poi che *"l'identificazione dei tipi di dati e di operazioni di cui ai commi 2 e 3 è aggiornata e integrata periodicamente".* Relativamente a questo aspetto, è opportuno evidenziare che può accadere che con l'introduzione di nuove tecnologie, lo svolgimento di una determinata attività che si riferisca ai dati sensibili, possa essere realizzata anche attraverso il

[220] È il Provvedimento del 17 gennaio 2002, in *Bollettino del Garante*, n.24,40.
[221] In tale modo si vuole agevolare l'omogeneità degli atti regolamentari delle pubbliche amministrazioni. Così R. Gamberale, *op. cit.*, p. 1100.
[222] In realtà, tale disposizione era già presente al comma 3-*bis* dell'art.22 nella previgente disciplina e il Garante, in base a tale disposizione, aveva individuato una serie di attività di rilevante interesse pubblico che la legge demanda ai soggetti pubblici e adesso elencate all'art. 73 del Codice.
[223] Così F. Cardarelli, *op. cit.*, p. 244.
[224] L'art. 26, al comma 2 prevede che *"Il Garante comunica la decisione adottata sulla richiesta di autorizzazione entro quarantacinque giorni, decorsi i quali la mancata pronuncia equivale a rigetto. Con il provvedimento di autorizzazione, ovvero successivamente, anche sulla base di eventuali verifiche, il Garante può prescrivere misure e accorgimenti a garanzia dell'interessato, che il titolare del trattamento è tenuto ad adottare."*
[225] In E. Barilà, C. Caputo, *Il trattamento dei dati sensibili da parte dei soggetti pubblici nel D.Lgs. 11 maggio 1999, n.135,* in *Tar,* 1999, II, p.156, l'autore rileva come non appaiano condivisibili le perplessità avanzate rispetto alle modalità di intervento del Garante sia rispetto alla sua potenziale ingerenza nelle competenze legislative sia in ordine alle potenziali forme di sindacato sulle modalità di esercizio della discrezionalità amministrativa.

trattamento di *dati anonimi*[226]*:* con la previsione all'art. 20, invece, si vuole invece comprendere nel termine "aggiornamento" di eliminare quel tipo di dati e operazioni su di essi[227].

Di primaria importanza, al fine di comprendere le disposizioni concernenti i dati sensibili come anche quelli giudiziari, è l'art. 22 del *Codice* che coordina e integra le varie disposizioni del citato decreto legislativo n.135 del 1999 sulle modalità di trattamenti di tali tipi di dati che era intervenuto a modificare la legge del 1996. La disciplina attuale ribadisce l'obbligo per i soggetti pubblici di prestare particolare attenzione alla possibilità di arrecare danni per l'interessato in modo da *"prevenire violazioni dei diritti, delle libertà fondamentali e della dignità dell'interessato"* (art. 22, comma 1) e il rifermento agli obblighi per i soggetti pubblici nel trattamento di dati sensibili e giudiziari nell'informativa resa agli interessati (art.22, comma 2). Al comma 3 e 9, invece, sviluppa, il *principio di proporzionalità* nel trattamento di tali dati e lo collega a quello dell'*indispensabilità dei dati* stessi, e non più solo della *necessità* o *essenzialità* come prevedeva la previgente disciplina[228], del loro uso rispetto ad attività che potrebbero essere svolte ricorrendo a dati anonimi o quelli personali di diversa natura[229]. Lo scopo è quello di armonizzare le disposizioni in materia, anche considerando le autorizzazioni generali che il Garante ha rilasciato nei confronti di soggetti privati in materia di dati sensibili. L'art. 22 continua riprendendo tutti i punti salienti già presenti nel suddetto decreto legislativo: la raccolta dei dati sensibili e giudiziari presso l'interessato (comma 4); i particolari obblighi ricadenti sui soggetti pubblici titolari del trattamento (comma 5); l'utilizzo di tecniche di cifratura o di codici identificativi o altre soluzioni quando i dati in esame siano contenuti in elenchi, registri o banche dati (comma 6); maggiori cautele previste per i dati idonei a rivelare lo stato di salute e la vita sessuale (comma 7 e 8); il divieto di utilizzo dei dati sensibili e giudiziari nell'ambito di test psico-attitudinali (comma 10). È, poi a chiusura dell'articolo, al comma 12 che innova rispetto alla legislazione precedente: dispone che tutte le disposizioni enunciate *"recano principi applicabili, in conformità ai rispettivi ordinamenti, ai trattamenti disciplinati dalla Presidenza della Repubblica, dalla Camera dei deputati, dal Senato della Repubblica e dalla Corte costituzionale."*[230]

---

[226] La definizione di *dato anonimo* è presente al suddetto art. 4 comma 1 lettera m) del decreto legislativo n.196/2003 come il *"dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile".*

[227] R. Gamberale, *op. cit.*, pp. 1101-1102.

[228] In particolare all'art. 3, comma 1 del decreto legislativo n.135/1999.

[229] Sul punto si veda S. Foà, *Il trattamento dei dati personali per finalità di rilevante interesse pubblico,* in in G. Santaniello (a cura di), *op. cit.,* p. 345.

[230] Infatti, l'art. 2 comma 1, lettera c) del decreto legislativo n.135/1999 escludeva detti soggetti dall'applicazione delle sue disposizioni.

3.1.2 Il trattamento dei dati sensibili da parte dei soggetti privati

L'art. 26 del *Codice,* intitolato *"Garanzie per i dati sensibili"* disciplina, invece, il trattamento dei dati sensibili da parte dei soggetti privati e degli enti pubblici economici, espressamente esclusi dalla disciplina appena considerata. L'articolo successivo si occupa, separatamente e quindi diversamente da quanto previsto per il sistema applicabile ai soggetti pubblici, le *garanzie per i dati giudiziari*. Oltre alla sopra citata definizione di dato sensibile[231], la norma riprende l'impianto normativo previgente anche se con la previsione di alcuni interventi di razionalizzazione e di adeguamento alla direttiva 95/46/CE. In virtù della "delicatezza" di questi dati[232], anche nella normativa vigente sono considerati, al primo comma, i due presupposti primari per garantire il trattamento in condizioni di massima sicurezza: il *consenso scritto* dell'interessato e l'*autorizzazione* del Garante. Non solo, perché la disposizione aggiunge *"nell'osservanza dei presupposti e dei limiti stabiliti dal presente codice, nonché dalla legge e dai regolamenti.":* obbligo che si impone ai soggetti privati ma che si ritiene applicabile anche ai soggetti pubblici.

Il secondo comma, che riguarda le modalità di rilascio di un'autorizzazione da parte del Garante non rientrante in quelle cd. *generali*[233], resta sostanzialmente analogo all'impianto precedente se non sui tempi di rilascio di tale provvedimento da parte dell'Autorità: non più trenta ma quarantacinque giorni dal ricevimento della stessa e il silenzio equivarrà sempre a rigetto con la possibilità di poter prescrivere successivamente misure e accorgimenti a garanzia dell'interessato.

Un regime di esclusione di entrambi i presupposti legittimanti al trattamento dei dati sensibili da parte dei soggetti privati è previsto al terzo comma in cui si riprende sostanzialmente la disciplina previgente. Derogando al comma 1 dell'art.26, il legislatore del 2003 ha confermato l'esigenza di contemperare la tutela della *privacy* con quella di altri interessi valevoli di medesima tutela[234] e in particolare quello del libero svolgimento dell'esercizio del culto religioso, costituzionalmente garantito[235] e quello della libera partecipazione ad associazioni od organizzazioni sindacali e di categoria[236]. Riproducendo i commi 1-*bis* e 1-*ter* dell'art. 22 della

---

[231] Si rinvia alla nota 208 sulla definizione di dato sensibile.

[232] In G. Gardini, *op. cit.*, p.251.

[233] Come nell'impianto precedente, il riferimento è alle autorizzazioni rilasciate singolarmente ai soggetti privati quando il trattamento dei dati sensibili non rientra in nessuna delle fattispecie regolate dalle autorizzazioni generali o standard.

[234] Per la nozione di *bilanciamento di interessi* si rinvia al primo capitolo.

[235] L'art. 8 Cost. prevede che *"Tutte le confessioni religiose sono egualmente libere davanti alla legge.*
Le confessioni religiose diverse dalla cattolica hanno diritto di organizzarsi secondo i propri statuti, in quanto non contrastino con l'ordinamento giuridico italiano. I loro rapporti con lo Stato sono regolati per legge sulla base di intese con le relative rappresentanze".

[236] Nei casi previsti, il comma 3 dell'art. 26 prevede la non applicazione del comma 1 al trattamento: " *a) dei dati relativi agli aderenti alle confessioni religiose e ai soggetti che con riferimento a finalità di natura*

precedente legge n.675/1996, si è voluto riconfermare l'esonero dalla disciplina in virtù del particolare rilievo costituzionale di alcuni titolari del trattamento nel primo caso e della minore pericolosità del relativo trattamento nel secondo[237]. Con particolare riferimento al caso del regime applicabile alle confessioni religiose, riprendendo quanto previsto originariamente dalla direttiva 95/46/CE e poi introdotto con le integrazioni all'art. 22 della precedente disciplina, l'art. 26 del *Codice* ha posto fine alla questione discriminatoria "[..] *che tante polemiche aveva determinato, facendo venire meno la condizione della previa regolamentazione dei rapporti tra le confessioni religiose e lo Stato italiano ed equiparando, in tal modo, le disposizioni previste per tutte le confessioni religiose"*[238]. Proprio con riferimento alle confessioni religiose, una disposizione transitoria all'interno del *Codice* prevede che con rispetto a quelle che prima della sua entrata in vigore abbiano già adottato le *garanzie* richieste nell'ambito del rispettivo ordinamento, queste possono perseguire le attività di trattamento dei dati nel rispetto delle suddette garanzie[239].

Inoltre, il terzo comma prevede un nuovo caso di deroga alla disciplina normale non previsto precedentemente, che è stato successivamente aggiunto, per "*i dati contenuti nei curricula, nei casi di cui all'articolo 13, comma 5-bis"*[240]*:* ossia nei casi in cui l'informativa non è dovuta all'interessato o alla persona presso la quale sono raccolti i dati quando questi abbiano trasmesso spontaneamente i *curricula* ai fini dell'eventuale instaurazione del rapporto di lavoro[241].

Il successivo comma 4 prevede una terza tipologia di regole applicabili al trattamento dei dati sensibili ossia quando possono essere effettuati attraverso l'esonero del consenso ma nel rispetto dell'*autorizzazione* del Garante. Il primo caso è quello dei trattamenti di dati effettuati da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, a carattere politico, filosofico, religioso o sindacale, compresi partiti e movimenti politici: analogamente

---

esclusivamente religiosa hanno contatti regolari con le medesime confessioni, effettuato dai relativi organi, ovvero da enti civilmente riconosciuti, sempre che i dati non siano diffusi o comunicati fuori delle medesime confessioni. Queste ultime determinano idonee garanzie relativamente ai trattamenti effettuati, nel rispetto dei principi indicati al riguardo con autorizzazione del Garante;

b) dei dati riguardanti l'adesione di associazioni od organizzazioni a carattere sindacale o di categoria ad altre associazioni, organizzazioni o confederazioni a carattere sindacale o di categoria".

[237] J. Monducci, *op. cit.*, Milano, 2003, p.42.

[238] Così R. Gamberale, *op. cit.*, p. 1106.

[239] Si rinvia all'art. 181, comma 6 del decreto legislativo n.196/2003.

[240] La lettera b-*bis)* è stata aggiunta dall'art. 6, comma 2, lett. a), numero 4), del decreto legge 13 maggio 2011, n. 70, convertito, con modificazioni, dalla legge 12 luglio 2011, n. 106.

[241] L'art. 13 comma 5-*bis* del *Codice* prevede che; *"L'informativa di cui al comma 1 non è dovuta in caso di ricezione di curricula spontaneamente trasmessi dagli interessati ai fini dell'eventuale instaurazione di un rapporto di lavoro. Al momento del primo contatto successivo all'invio del curriculum, il titolare è tenuto a fornire all'interessato, anche oralmente, una informativa breve contenente almeno gli elementi di cui al comma 1, lettere a), d) ed f)."*

alla disciplina applicabile ai dati comuni[242], anche per questi trattamenti viene evidenziata l'esigenza di maggiore garanzia e trasparenza nell'espressa determinazione delle modalità di utilizzo dei dati da parte di detti organismi rendendole note all'interessato attraverso l'informativa. Esonero dall'obbligo di consenso è previsto anche quando il trattamento sia necessario per la salvaguardia della vita o dell'incolumità fisica di un terzo, analogamente a quanto previsto per i dati diversi da quelli sensibili[243] , specificando che qualora l'interessato non possa prestare consenso per impossibilità fisica, per incapacità di agire o per incapacità di intendere o di volere: tale consenso sarà prestato da chi esercita legalmente la potestà, ovvero da un prossimo congiunto, da un familiare, da un convivente o, in loro assenza, dal responsabile della struttura presso cui dimora l'interessato. Il terzo caso, previsto alla lettera c), esclude la necessità del consenso qualora i dati sensibili vengano trattati per lo svolgimento di investigazioni difensive o per esigenze di tutela di un diritto in sede giudiziaria[244]. Da evidenziare, perché introdotta dal *Codice*, è la previsione secondo cui qualora tali dati siano idonei a rivelare lo stato di salute e la vita sessuale, *"il diritto deve essere di rango pari a quello dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile"*, riprendendo nuovamente l'istituto del corretto *bilanciamento* tra interessi contrapposti introdotto dalla giurisprudenza.

Tuttavia, la novità più rilevante quanto alle cause di esclusione del consenso è quella prevista dalla lettera d) quando sia *"necessario per adempiere a specifici obblighi o compiti previsti dalla legge, da un regolamento o dalla normativa comunitaria per la gestione del rapporto di lavoro, anche in materia di igiene e sicurezza del lavoro e della popolazione e di previdenza e assistenza*". Tale innovazione si iscrive nel principio di semplificazione che il Codice ne attribuisce pieno valore[245] come mostra la previsione all'art. 2 del *Codice* [246] ed è rilevante proprio perché nella disciplina previgente vi era la necessità del consenso scritto da parte del lavoratore anche quando l'acquisizione dei suoi dati personali fosse necessaria all'adempimento degli obblighi conseguenti al contratto di lavoro o alla gestione dei rapporti di lavoro: la nuova previsione invece *"semplifica non poco la posizione dell'imprenditore rispetto al regime di default, rendendo inutile il consenso dell'interessato."*[247] Comunque, tale principio deve agire

[242] Essa è prevista all'art. 24, comma 1, lettera h) del *Codice.*
[243] Si rinvia all'art.24, comma 1, lettera e) del *Codice.*
[244] Il riferimento alle investigazioni difensive è presente nella legge n. 397/2000 contenente *"Disposizioni in materia di indagini difensiva"* che prevede all'art. 11 un'informativa simile a quella dell'art.13 del *Codice* con cui deve essere coordinata.
[245] Per un'analisi dettagliata dell'applicazione del principio di semplificazione nel *Codice* si rinvia a G. Santaniello, *La semplificazione delle regole nel codice della privacy,* in *Protezione dei dati personali,* in *www.interlex.it/675/santaniello10.htm*, 3 marzo 2004.
[246] Per il quale si rinvia al paragrafo 3 del presente capitolo.
[247] G. Rasi, *Valutazioni del datore di lavoro sul dipendente e privacy: l'intervento del legislatore,* in *Il Sole-24Ore – Guida al lavoro,* 8 agosto 2003, 16.

nei limiti previsti dall'autorizzazione del Garante e può subire deroghe dai codici di deontologia e di buona condotta allegati al *Codice.*

L'art. 26 si conclude con il riferimento ai dati che necessitano di una tutela ancora maggiore ossia quelli idonei a rivelare lo stato di salute, i quali non possono essere diffusi[248] secondo la formula perentoria e assoluta prevista al comma 5[249]. Mentre la previgente disciplina consentiva la diffusione di tali dati in caso di necessità ai fini della prevenzione, accertamento o repressione dei reati[250], la modifica apportata dal *Codice* è giustificata dalla particolare "sensibilità" di tali dati che incidono sulla concezione di dignità dell'individuo e potrebbero essere utilizzati maggiormente per fini discriminatori, come si vedrà tra breve[251].

3.1.3 Consenso, autorizzazione, notificazione al Garante e altre disposizioni applicabili al trattamento dei dati sensibili

Contrariamente al regime relativo ai soggetti pubblici i quali non hanno un obbligo di richiedere il consenso all'interessato[252] purché il trattamento sia effettuato nell'ambito dello svolgimento delle proprie funzioni istituzionali, questo è invece necessario per i soggetti privati e gli enti pubblici economici e previsto all'apertura del Capo III contenente le *Regole ulteriori per privati ed enti pubblici economici* all'art.23 del *Codice.* L'impianto legittimante il consenso è il medesimo della previgente disciplina anche per quanto concerne il trattamento dei dati sensibili, per tanto si rimanda al paragrafo relativo all'analisi specifica di tali aspetti: riassumendo, alle regole applicabili ai dati comuni, ossia il fatto di dover essere *espresso*, *libero*, *documentato per iscritto* e *informato* nonché può riguardare l'intero trattamento o anche più operazioni dello stesso; nel caso poi, di trattamento di dati sensibili, si aggiunge anche che il consenso debba essere *manifestato in forma scritta*[253] sempre a garanzia di una tutela rafforzata. Un cenno deve essere fatto al cd. *consenso informato* già presente nella legge del 1996 che diviene elemento portante sui quali regge il *Codice* e che rimanda all'art. 13 dello stesso. Infatti tra i suddetti requisiti, il consenso risulta validamente prestato se sono state fornite all'interessato *preventivamente* adeguate informazioni[254], oralmente o per iscritto, su: *a) le finalità e le modalità del trattamento cui sono destinati i dati;*

[248] L'art. 4, comma 1, lettera m) del *Codice* definisce la diffusione come "*il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione"*.
[249] Il comma 5 prevede infatti che *"I dati idonei a rivelare lo stato di salute non possono essere diffusi."*
[250] La previsione si trovava all'art. 23 comma 4 della legge n.675/1996.
[251] Così R. Gamberale, *op. cit*., p. 1110.
[252] La previsione è all'art. 18, comma 4 del *Codice,* salvo la disciplina applicabile agli esercenti delle professioni sanitarie e gli organismi sanitari pubblici.
[253] Art. 23, comma 4 del *Codice.*
[254] Rappresentano gli elementi che necessariamente deve contenere l'informativa.

b) la natura obbligatoria o facoltativa del conferimento dei dati;

c) le conseguenze di un eventuale rifiuto di rispondere;

d) i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, e l'ambito di diffusione dei dati medesimi;

e) i diritti di cui all'articolo 7;

f) gli estremi identificativi del titolare e, se designati, del rappresentante nel territorio dello Stato ai sensi dell'articolo 5 e del responsabile. Quando il titolare ha designato più responsabili è indicato almeno uno di essi, indicando il sito della rete di comunicazione o le modalità attraverso le quali è conoscibile in modo agevole l'elenco aggiornato dei responsabili. Quando è stato designato un responsabile per il riscontro all'interessato in caso di esercizio dei diritti di cui all'articolo 7, è indicato tale responsabile.[255]

È opportuno notare, allora, come il legislatore italiano abbia voluto aderire a quel particolare sistema di regolamentazione conosciuto come *opt-in system*, secondo cui ogni individuo deve autorizzare *preventivamente* il trattamento dei dati che lo riguardano, che è più garantistico[256] rispetto al modello nordamericano[257].

Anche con riferimento alla *previa autorizzazione* del Garante per poter trattare dati sensibili, nulla è innovato[258] rispetto alla precedente disciplina.

Con riguardo invece alla *notificazione* il nuovo testo sovverte il principio che era stato fatto proprio dalla legge n.675/1996, secondo cui vi era un obbligo generale di notifica al Garante, al fine di segnalare le tipologie e le modalità di trattamento dei dati che si intende eseguire, da parte di tutti i soggetti titolari dal trattamento con esclusione dei casi tassativamente previsti all'art. 7 della legge del 1996. Al contrario, il Testo Unico prevede che la notifica *preventiva* debba essere effettuata solo in casi espressamente previsti dall'art. 37: questi riguardano per la maggior parte casi di trattamento di dati sensibili[259]. L'idea di fondo dell'obbligo di notifica sta

[255] Il riferimento è all'art. 13, comma 1 del *Codice.*

[256] G. Gardini, *op. cit.,* pp. 253-254.

[257] Nell'ordinamento nordamericano è adottato, invece, il cd. *opt-out system* per cui il consenso dell'interessato al trattamento si ritiene *implicito* a meno di espressa opposizione da parte dell'interessato.

[258] Nel prossimo paragrafo saranno analizzate nel dettaglio le Autorizzazioni rilasciate dal Garante in materia di dati sensibili.

[259] L'art. 37, comma 1 del *Codice* prevede infatti che la notificazione debba avvenire solo per i trattamenti che riguardano: *a) dati genetici, biometrici o dati che indicano la posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica; b) dati idonei a rivelare lo stato di salute e la vita sessuale, trattati a fini di procreazione assistita, prestazione di servizi sanitari per via telematica relativi a banche di dati o alla fornitura di beni, indagini epidemiologiche, rilevazione di malattie mentali, infettive e diffusive, sieropositività, trapianto di organi e tessuti e monitoraggio della spesa sanitaria; c) dati idonei a rivelare la vita sessuale o la sfera psichica trattati da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, a carattere politico, filosofico, religioso o sindacale; d) dati trattati con l'ausilio di strumenti elettronici volti a definire il profilo o la personalità dell'interessato, o ad analizzare abitudini o scelte di consumo, ovvero a monitorare l'utilizzo di servizi*

proprio nella maggiore pericolosità del trattamento nel senso di arrecare pregiudizio a terzi per cui è evidente che l'elencazione non può essere tassativa ed immutabile[260]. A tal proposito, il comma 2 dell'art. 37 prevede che il Garante possa individuare "*altri trattamenti suscettibili di recare pregiudizio ai diritti e alle libertà dell'interessato"*, con proprio provvedimento. Novità introdotta con l'entrata in vigore del decreto legislativo, è che la notifica al Garante possa essere presentata solo per via telematica per essere *"validamente effettuata"* ai sensi dell'art. 38.

Meritano, infine, di essere accennati alcuni degli elementi centrali per il trattamento dei dati personali "generali" e applicabili anche per quelli sensibili: i principi applicabili ai trattamenti dei dati, i diritti degli interessati al trattamento, i casi di trasferimento dei dati verso altri Paesi ed il sistema sanzionatorio previsto per la violazione delle disposizioni sul trattamento dei dati.

In primo luogo, l'art. 11 definisce quali siano i *principi applicabili a qualsiasi trattamento di dati.* Essi devono essere: trattati in modo *lecito* e *secondo correttezza; raccolti e registrati per scopi determinati, espliciti e legittimi,* ed utilizzati in altre operazioni del trattamento *non incompatibili* con essi; *esatti* e *aggiornati; pertinenti, completi e non eccedenti rispetto alle finalità* per le quali sono raccolti o successivamente trattati; *conservati* in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

Con riferimento, invece, ai *diritti dell'interessato* rispetto ai propri dati, la disciplina è contemplata nel Titolo II, Parte I del *Codice* e come detto sopra, devono essere richiamati dal titolare nell'informativa: a tale riguardo non è sufficiente un richiamo all'art.7, ma è opportuno richiamare l'intero testo normativo[261]. Tali diritti rivestono particolare importanza perché rappresentano situazioni giuridiche individuate e per le quali viene predisposto un sistema di tutela specifico e composito[262], riprendendo quanto già disposto dall'art. 13 della legge n.675/1996 ed ora previsti dall'art. 7 e seguenti[263]. I diritti previsti possono essere racchiusi in tre categorie: *il diritto a conoscere se un trattamento è stato iniziato; l'esercizio di un controllo sulla qualità dei dati* che si traduce poi nel *diritto ad ottenere la cancellazione dei dati, la loro trasformazione in forma anonima, la rettificazione, l'aggiornamento, il blocco e l'integrazione dei dati medesimi; il diritto di opposizione* per motivi legittimi, anche quando il trattamento sia

---

di comunicazione elettronica con esclusione dei trattamenti tecnicamente indispensabili per fornire i servizi medesimi agli utenti; e) dati sensibili registrati in banche di dati a fini di selezione del personale per conto terzi, nonché dati sensibili utilizzati per sondaggi di opinione, ricerche di mercato e altre ricerche campionarie; f) dati registrati in apposite banche di dati gestite con strumenti elettronici e relative al rischio sulla solvibilità economica, alla situazione patrimoniale, al corretto adempimento di obbligazioni, a comportamenti illeciti o fraudolenti."

[260] Così C. Rigotti, *op.cit.*, p.41.

[261] Così C. Rigotti, *ivi.*, p.52.

[262] G.P. Cirillo, *op. cit.*, p.40.

[263] Si rinvia a S. Fiorenzano, *Commento all'art.7,* in G.P. Cirillo (a cura di), *Il Codice sulla protezione dei dati personali*, Milano, 2004 per un'analisi dettagliata dell'art. 7 del *Codice.*

conforme alle finalità di raccolta dei dati.[264] L'aspetto di novità rispetto alla legge del 1976 è data dal fatto che le situazioni giuridiche del nuovo testo legislativo aumentano, prevedendo, in primo luogo, al comma 2, lettera e) dell'art. 7 il diritto di conoscere i soggetti cui possono essere comunicati i dati o che ne possano venire a conoscenza, dando piena attuazione anche a quanto disposto dalla direttiva 95/46/CE[265]. In secondo luogo, la nuova disposizione, al comma 4, lettera b) definisce il diritto di opporsi al trattamento effettuato *"a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale"* ossia di *marketing*[266]. Il *Codice,* dunque, prevede ancora di più rispetto al passato, garanzie nei confronti dell'interessato al trattamento: tali diritti *"costituiscono innegabilmente espressione di un più generale diritto della persona sui propri dati"*[267].

Se invece ci si riferisce al trasferimento dei dati in altri Paesi, occorre distinguere se questo avvenga verso Paesi appartenenti o meno all'Unione europea. Nel primo caso, le legislazioni degli Stati membri, adottate in attuazione della direttiva comunitaria 95/46/CE, sono considerate come *equivalenti* in relazione all'adeguata tutela in materia di protezione dei dati personali: pertanto detto trasferimento non è soggetto a particolari restrizioni previsto dall'art. 42 del *Codice.* Qualora, invece, il trasferimento dei dati personali avvenga nei confronti di Paesi non appartenenti all'Unione europea, questo è possibile solo quando: ricorra una delle condizioni previste dall'articolo 43 del *Codice* oppure quando sia autorizzato dal Garante sulla base di adeguate garanzie per i diritti dell'interessato ai sensi dell'articolo 44 del *Codice*. Al di fuori di questi casi, l'art.45 del *Codice* prevede che detto trasferimento sia vietato quando l'ordinamento del Paese di destinazione o di transito dei dati personali non assicuri un livello adeguato di tutela delle persone[268].

Infine, nella Parte III, Titolo III del *Codice* sono previste le *sanzioni* amministrative e penali da applicarsi nei vari casi di violazioni delle disposizioni sul trattamento dei dati personali, comprendenti anche i casi in cui ci siano illiceità del trattamento di quelli sensibili. Sono previste sanzioni amministrative nei casi di: omessa o inidonea informativi per trattamenti che non contengono dati sensibili, illegittima cessione dei dati, violazione delle prescrizioni in ordine alla comunicazione di dati in ambito sanitario, omessa o incompleta notificazione, omessa informazione o esibizione dei documenti al Garante. Invece, sono previste sanzioni

[264] La tripartizione dei diritti dell'interessato è considerata da A. Scalisi, *Il diritto alla riservatezza,* Milano, 2002, p. 248.

[265] All'art. 12, la direttiva comunitaria prevede infatti la disciplina concernente il diritto di accesso.

[266] La nuova disposizione ha escluso il riferimento all'informativa del trattamento che era prevista all'art. 13, comma 1, lettera e) della legge n.675/1996.

[267] M. Messina, *I diritti dell'interessato,* in F. Cardarelli, S. Sica, V. Zeno-Zencovich, *op.cit.*, p.68.

[268] Come si vedrà nel capitolo successivo, tale disposizione acquista una rilevanza particolare in seguito alla sentenza della Corte di Giustizia invalidante il *Safe Harbor.*

penali ogni qualvolta ci sia: un trattamento da parte di soggetti pubblici per scopi non istituzionali, violazione da parte di un soggetto pubblico delle regole di comunicazione dei dati personali comuni, trattamento dei dati senza il prescritto consenso, violazione delle regole di trattamento imposte ai gestori di servizi di comunicazione elettronica, violazione dei divieto di comunicazione e diffusione, trattamento di dati sensibili e giudiziari in violazione delle garanzie specificamente previste, violazione dei divieti di trasferimento di dati all'estero, false dichiarazioni o notificazioni rese al Garante, omessa azione delle misure minime di sicurezza, inosservanza dei provvedimenti dei Garante e inosservanza dello Statuto dei lavoratori. [269]

3.1.4 Il trattamento dei cc. dd. dati supersensibili

Pare opportuno porre l'attenzione su *alcuni* dei dati rientranti nella categoria dei dati sensibili e di cui pertanto si è già accennato, che però assumono un'importanza del tutto particolare. Accanto a quelli *"idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico, o sindacale",* vi sono anche quelli relativi alla salute e alla sfera sessuale: tali dati prendono la denominazione di dati *supersensibili*. Previsti già dalla normativa del 1996, il *Codice* conferma tale impostazione basandosi sulla considerazione che siano riferiti alla sfera privata dell'individuo in quanto tale, contrariamente agli altri che lo relazionano ad un "gruppo sociale". Come è stato anticipato dall'analisi della disciplina applicabile ai soggetti pubblici, l'art. 22 prevede che tali tipi dati debbano essere *"conservati separatamente da altri dati personali trattati per finalità che non richiedono il loro utilizzo. I medesimi dati sono trattati con le modalità di cui al comma 6 anche quando sono tenuti in elenchi, registri o banche di dati senza l'ausilio di strumenti elettronici.";* mentre al comma 8 riferendosi soltanto a quelli sullo stato di salute, si prevede che non possono essere diffusi. Disposizione peraltro ripresa anche nel caso di trattamento da parte dei soggetti privati ed enti pubblici economici[270]. Ancora, nel caso di trattamento dei dati *supersensibili* da parte di tali ultimi soggetti, come è stato anticipato nelle pagine precedenti, è prevista una deroga al regime dell'acquisizione del consenso pur con la previa autorizzazione del Garante ma a condizione che nel caso di tali dati, *"il diritto deve essere di rango pari a quello dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o*

[269] Nella Parte III del Codice si trovano le disposizioni concernenti le forme di tutela garantite all'interessato ed il regime sanzionatorio.
[270] Il riferimento è al comma 5 dell'art. 26 del *Codice.*

libertà fondamentale e inviolabile"[271]. Altre disposizioni del *Codice* finalizzate a garanzie maggiori per i dati relativi alla salute e/o alla vita sessuale sono ancora quelle previste:

- all'art. 33, comma 1 lettera h) che prevede nel caso di alcuni trattamenti di dati *supersensibili* effettuati con strumenti elettronici, debbano essere adottate tecniche di cifratura o di codici identificativi da parte di organismi sanitari;
- all'art. 37, comma 1 rientrando nei casi espressamente previsti per il trattamento notificato al Garante qualora siano finalizzati alla procreazione assistita, alla prestazione di servizi sanitari per via telematica relativi a banche di dati o alla fornitura di beni, indagini epidemiologiche, rilevazione di malattie mentali, infettive e diffusive, sieropositività, trapianto di organi e tessuti e monitoraggio della spesa sanitaria;
- all'art. 39 comma 1 nei casi in cui il titolare debba dare comunicazione preventiva al Garante quando il trattamento di dati idonei a rivelare lo stato di salute sia *"previsto dal programma di ricerca biomedica o sanitaria di cui all'articolo 110, comma 1, primo periodo*";
- al Capo I sull' *Accesso dei documenti amministrativi,* previsto all'interno del Titolo IV, un'intera disposizione riguarda le regole applicabili al trattamento in ambito pubblico dei dati idonei a rilevare lo stato di salute o la vita sessuale: in tali casi, "*il trattamento è consentito se la situazione giuridicamente rilevante che si intende tutelare con la richiesta di accesso ai documenti amministrativi è di rango almeno pari ai diritti dell'interessato, ovvero consiste in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile."*[272]
- nell'ambito del Titolo V del *Codice* relativo ai *Trattamenti in ambito sanitario* sono previste una serie di disposizioni finalizzate ad una tutela più incisiva per i dati trattati: all'art. 76 sono previste le regole che si applicano agli esercenti le professioni sanitarie e gli organismi sanitari pubblici, i quali anche nell'ambito di un'attività di rilevante interesse pubblico trattano i dati personali idonei a rivelare lo stato di salute pur senza consenso dell'interessato o la previa autorizzazione del Garante[273]; l'art' 84, al comma 1, prevede, invece, che i *"dati personali idonei a rivelare lo stato di salute possono essere resi noti all'interessato o ai soggetti di cui all'articolo 82, comma 2, lettera a), da parte di esercenti le professioni sanitarie ed organismi sanitari, solo per il tramite di un medico designato dall'interessato o dal titolare. Il presente comma non si applica in riferimento ai dati personali forniti in precedenza dal medesimo interessato."*; l'art. 85, al comma 3, considera ai fini dell'identificazione che ai *"tipi di dati*

[271] Il citato art. 26, comma 4, lettera c).
[272] Ci si riferisce all'art. 60 del *Codice.*
[273] L'art. 76, comma 1 prevede infatti i casi in cui tali soggetti possono trattare dei dati idonei a rilevare lo stato di salute anche *"a) con il consenso dell'interessato e anche senza l'autorizzazione del Garante, se il trattamento riguarda dati e operazioni indispensabili per perseguire una finalità di tutela della salute o dell'incolumità fisica dell'interessato;*
b) anche senza il consenso dell'interessato e previa autorizzazione del Garante, se la finalità di cui alla lettera a) riguarda un terzo o la collettività."

idonei a rivelare lo stato di salute e di operazioni su essi eseguibili è assicurata ampia pubblicità, anche tramite affissione di una copia o di una guida illustrativa presso ciascuna azienda sanitaria e presso gli studi dei medici di medicina generale e dei pediatri di libera scelta."; ancora, l'art. 91 consente il trattamento dei dati idonei a rivelare lo stato di salute o la vita sessuale eventualmente registrati su carte anche non elettroniche, soltanto se necessario ai sensi dell'articolo 3, nell'osservanza di misure ed accorgimenti prescritti dal Garante nei modi di cui all'articolo 17; infine l'art. 91 prevede che quando il trattamento di dati idonei a rivelare lo stato di salute sia contenuto in banche di dati, schedari, archivi o registri tenuti in ambito sanitario, deve avvenire sempre nel rispetto dell'articolo 3 anche presso banche di dati, schedari, archivi o registri già istituiti alla data di entrata in vigore del *Codice* e in riferimento ad accessi di terzi previsti dalla disciplina vigente alla medesima data;

- all'art. 139 che prevede l'adozione di un codice di deontologia da parte del Consiglio nazionale dell'ordine dei giornalisti, di cui si è detto, tenendo conto di accorgimenti a garanzia degli interessati nei casi dei dati idonei a rivelare lo stato di salute e la vita sessuale. In tal direzione, il Codice di deontologia dei giornalisti non ha trascurato la prevalente importanza dei dati *supersensibili* dedicando ad essi due disposizioni: l'art. 10 relativo alla *tutela delle persone malate* e l'art. 11 relativo alla *tutela della sfera sessuale della persona.*

3.1.5 Le autorizzazioni generali del Garante in materia di dati sensibili e giudiziari

L'istituzione di un'Autorità nazionale posta a garanzia della protezione dei dati personali trova la sua origine nelle norme comunitarie ed in particolare nella direttiva 95/46/CE[274], recepita nella normativa italiana a partire dalla legge n.675/1999, che ha previsto l'istituzione del Garante per la protezione dei dati personali[275]. Infatti, alcuni autori sottolineano come il recepimento del modello comunitario da parte del legislatore italiano si inserisce in una generale tendenza ad adattare l'ordinamento interno a quello europeo "[..] *mediante l'attribuzione di funzioni di regolazione in ambiti rilevanti per la realizzazione del mercato unico ad organismi indipendenti anziché ad apparati dell'amministrazione statale tradizionale"*[276]. La disciplina attualmente vigente[277] conferma l'impianto precedente con

[274] Si rinvia al primo capitolo sull'evoluzione della normativa comunitaria in materia di *privacy*.
[275] Le disposizioni dedicate alla figura del *Garante* nella precedente disciplina si rinvenivano agli art. 29-30 della legge n.675/1996.
[276] Citazione in A. Putignani, *Il garante per la protezione dei dati personali*, in A. Clemente (a cura di), *op. cit.*, p.653 in cui si evidenzia come le amministrazioni statati siano ritenuti meno adatti a trattare di materie investite dall'attuazione delle politiche comunitarie.
[277] Prevista dagli art. 153-156 del *Codice.*

l'attribuzione all'Autorità di piena autonomia[278] e all'art. 154 del *Codice* sono previsti i principali compiti che gli vengono attribuiti anche da norme internazionali e comunitarie.

Venendo alla materia in esame, proprio ai sensi della lettera d), comma 1 dell'art. 154 del *Codice*, il Garante per la protezione dei dati può adottare provvedimenti previsti dalla normativa in materia di dati personali[279], tra cui, in particolare, autorizzazioni generali per il trattamento dei dati sensibili. Esse non rientrano nella categoria di quelle rilasciate dalla stessa Autorità in seguito ad una specifica richiesta da parte del titolare di cui si è detto sopra che rappresenta una delle condizioni legittimanti il trattamento di dati sensibili insieme al consenso. Infatti, il Garante, sotto espressa previsione del legislatore, ha ritenuto troppo gravoso e pericoloso l'obbligo di richiedere autorizzazioni specifiche al trattamento di dati sensibili e aveva previsto la necessità di prevedere autorizzazioni generali per interi settori o categorie di dati e dei trattamenti autorizzati, già nella previgente disciplina. Infatti il decreto legislativo n.127/1997[280] all'art. 4 aveva previsto la possibilità da parte del Garante di emanare provvedimenti generali in quei casi entro il 30 novembre 1997 che era intervenuto sull'art. 41, comma 7 della legge del 1996[281]. In base a tale disposizione, furono emanate sette autorizzazioni *standard* ossia a carattere collettivo, di cui si dirà a breve, e basate su tre elementi[282]: la semplificazione degli adempimenti da parte del titolare, in quanto essi senza una richiesta si trovano necessariamente a trattare alcuni dati di carattere sensibile; l'armonizzazione delle prescrizioni con una riduzione del lavoro del Garante; la valutazione di interessi socialmente rilevanti. È stato, infatti, da più parti mostrato come il metodo delle autorizzazioni sia rispondente alle esigenze del settore e dotato di efficacia operativa[283].

Attualmente, la materia è stata completamente sostituita dal vigente art. 40 del *Codice* che si occupa specificamente delle autorizzazioni generali prevedendo che *"Le disposizioni del presente codice che prevedono un'autorizzazione del Garante sono applicate anche mediante il rilascio di autorizzazioni relative a determinate categorie di titolari o di trattamenti, pubblicate*

---

[278] G. P. Cirillo, *La tutela in via amministrativa del trattamento dei dati personali,* in G. Santaniello (a cura di), *op.cit.,* p.717, sostiene come la piena autonomia sia da intendersi la preminenza sugli operatori pubblici e privati del settore e supremazia rispetto al potere amministrativo in senso stretto e "indipendenza di giudizio e di valutazione".

[279] Art. 154, comma 1, lettera d).

[280] Si fa riferimento al decreto legislativo 9 maggio 1997, n.123 contenente *Disposizioni integrative e correttive della legge 31 dicembre 1996 n.675.*

[281] L'art. 41 contenente le *Disposizioni transitorie* al comma 7, così come era stato modificato prevedeva: *"Le disposizioni della presente legge che prevedono un'autorizzazione del Garante si applicano limitatamente alla medesima autorizzazione e fatta eccezione per la disposizione di cui all'articolo 28, comma 4, lettera g), a decorrere dal 30 novembre 1997. Le medesime disposizioni possono essere applicate dal Garante anche mediante il rilascio di autorizzazioni relative a determinate categorie di titolari o di trattamenti.*
In sede di prima applicazione della presente legge, le informative e le comunicazioni di cui agli articoli 10, comma 3, e 27, comma 2, possono essere date entro il 30 novembre 1997."

[282] Si veda R. Gamberale, *cit.,* in R. Panetta (a cura di), *op.cit.,* p.1082.

[283] Si veda G. Santaniello, *Le autorizzazioni per categoria relative al trattamento dei dati sensibili,* Relazione al Convegno Paradigma, Milano 10-11 febbraio 1998.

nella Gazzetta Ufficiale della Repubblica italiana". Così, a partire dal 1997 le autorizzazioni generali sono state rinnovate di volta in volta, tecnica che ha consentito che le disposizioni in esse presenti assumessero maggiore stabilità: in esse, si scorge infatti un nucleo di disposizioni comuni coincidenti con i principi alla base del trattamento[284].

Recentemente, il Garante ha rinnovato le autorizzazioni al trattamento dei dati sensibili e giudiziari che saranno efficaci dal 1° gennaio 2015 fino al 31 dicembre 2016, in sostituzione di quelle in scadenza al 31 dicembre 2014: le nuove autorizzazioni rispecchiano per molti aspetti quelle già adottate e apportano le necessarie integrazioni derivanti da modifiche normative intervenute nei settori considerati. In ciascuna autorizzazione sono individuate le finalità dei trattamenti, le categorie dei dati trattati, degli interessati, dei destinatari della comunicazione e diffusione e sulla limitazione del periodo di conservazione degli stessi.

Le autorizzazioni generali applicabili nei trattamenti di dati sensibili in particolari settori, attualmente in vigore [285]sono:

- La n. 1/2014 *al trattamento dei dati sensibili nei rapporti di lavoro:* include nel proprio ambito tutti i soggetti che si avvalgono di prestazioni lavorative effettuate da altri. Tra i soggetti autorizzati a tale trattamento rientrano i datori di lavoro, quelli che si avvalgono da tali prestazioni non caratterizzate da vincolo di subordinazione[286] nonché gli organismi paritetici che gestiscono osservatori in materia di lavoro e il medico competente. Inoltre, l'autorizzazione non si riferisce a tutti dati sensibili ma solo ad alcune categorie[287].
- La n. 2/2014 *al trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale*: essa riguarda gli esercenti le professioni sanitarie e le figure professionali del settore che necessariamente vengono a conoscenza di tali tipologie di dati. I trattamenti in questione devono tutelare l'incolumità fisica e la salute di un terzo e della collettività; i dati in questione sono solo ed esclusivamente i dati pertinenti e necessari all'espletamento degli obblighi, compiti o al perseguimento delle finalità proprie dei soggetti autorizzati, facendo riferimento, in caso di soggetti collettivi, alle relative norme statutarie;
- La n. 3/2014 *al trattamento dei dati sensibili da parte degli organismi di tipo associativo e delle fondazioni:* prende in considerazione i trattamenti di dati sensibili svolti dalla maggior

[284] In tal senso R. Acciai, *Le garanzie per i dati sensibili e giudiziari,* in R. Acciai (a cura di) *Il Diritto alla protezione dei dati personali- la disciplina sulla privacy alla luce del nuovo codice,* Rimini, 2004, p.136 e ss.

[285] L'elencazione delle autorizzazioni è consultabile su *www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3632998.*

[286] Si fa riferimento ai liberi professionisti e lavoratori autonomi.

[287] Ci si riferisce ai dati idonei a rivelare le convinzioni religiose, filosofiche o di altro genere; l'adesione ad associazioni od organizzazioni a carattere religioso; concernenti la fruizione di permessi e festività religiose o di servizi di mensa; relativi all'obiezione di coscienza; idonei a rivelare le opinioni politiche, l'adesione ai partiti, sindacati, associazioni od organizzazioni a carattere politico o sindacale; concernenti l'esercizio di funzioni pubbliche e di incarichi politici.

parte dei soggetti collettivi con particolare riferimento a finalità culturali, religiose, politiche, sindacali. In base a tale autorizzazione, possono essere trattati dati diversi da quelli dell'autorizzazione n.2 o quelli idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o altro genere, opinioni politiche, adesione ai partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofiche, politico o sindacale. Inoltre, può comprendere anche trattamenti di dati necessari per perseguire le finalità statutarie o per adempiere ad obblighi di legge, della normativa comunitaria, dei regolamenti o dei contratti collettivi.

- La n. 4/2014 *al trattamento dei dati sensibili da parte dei liberi professionisti:* si riferisce alle operazioni di trattamento di dati utilizzati da soggetti iscritti in albi o elenchi per ragioni di ordine comportamentale legate alle diverse professioni.
- La n. 5/2014 *al trattamento dei dati sensibili da parte di diverse categorie di titolari:* è rilasciata per trattamenti effettuati in diversi settori economici, in cui tuttavia, il trattamento di dati sensibili è più frequente e di maggiore necessità: in particolare, nelle attività bancarie, creditizie, assicurative, di gestione dei fondi, del settore turistico, del trasporto; sondaggi e ricerche; attività di elaborazione dati; attività di selezione del personale; mediazione a fini matrimoniali. Ma anche la mediazione finalizzata alla conciliazione delle controversie civili e commerciali e i servizi digitali, settori non previsti precedentemente.
- La n. 6/2014 *al trattamento dei dati sensibili da parte degli investigatori privati:* essa è rilasciata esclusivamente per i soggetti che esercitano attività di investigazioni private.
- La n. 7/2014 *al trattamento dei dati a carattere giudiziario da parte di privati, di enti pubblici economici e di soggetti pubblici:* si riferisce ai soggetti, persone fisiche e giuridiche, enti e associazioni od organismi che hanno a che fare queste tipologie di dati.

Diversamente da quelle previste 1997, nel 2014 il Garante ha rilasciato altre due autorizzazioni secondo il modello dell'art. 40 del *Codice:*

- La n. 8/2014 *al trattamento dei dati genetici*: la nozione di *dato genetico*[288] è introdotta nel nostro ordinamento proprio dal Codice, dedicando il Capo V alle disposizioni su di essi. Dunque, l'autorizzazione si riferisce a tutti i soggetti che hanno a che fare con tali dati nello svolgimento delle loro attività lavorative come: gli esercenti le professioni sanitarie, gli organismi sanitari pubblici e privati, laboratori di genetica medica, alle persone fisiche o giuridiche, agli enti o agli istituti di ricerca, alle associazioni e agli altri organismi pubblici e

[288] La stessa autorizzazione n. 8/2014 definisce dato genetico *"il risultato di test genetici o ogni altra informazione che, indipendentemente dalla tipologia, identifica le caratteristiche genotipiche di un individuo trasmissibili nell'ambito di un gruppo di persone legate da vincoli di parentela".*

privati aventi finalità di ricerca, agli psicologi, ai consulenti tecnici e ai loro assistenti, ai farmacisti, ai difensori, anche a mezzo di sostituti, consulenti tecnici e investigatori privati autorizzati, agli organismi di mediazione pubblici e privati, agli organismi internazionali ritenuti idonei dal Ministero degli affari esteri e alle rappresentanze diplomatiche o consolari per il rilascio delle certificazioni.

- La n. 9/2014 *al trattamento dei dati personali effettuato per scopi di ricerca scientifica:* essa è rilasciata alle università, agli altri enti o istituti di ricerca e società scientifiche, nonché ai ricercatori che operano nell'ambito di dette università, enti, istituti di ricerca e ai soci di dette società scientifiche; agli esercenti le professioni sanitarie e agli organismi sanitari nei limiti di cui all'art. 2, comma 2, del codice di deontologia e buona condotta per i trattamenti di dati personali per scopi statistici e scientifici. L'autorizzazione specifica che non riguarda i casi in cui gli scopi della ricerca che possono essere realizzati attraverso il trattamento di dati anonimi e di dati riferiti ad interessati che sia possibile contattare al fine di rendere l'informativa e acquisirne il consenso.

Dunque, tali autorizzazioni sono provvisorie ed a tempo determinato, efficaci per un periodo di 24 mesi. Come è stato rilevato, tali provvedimenti hanno lo scopo di eliminare per il periodo di riferimento l'obbligo della richiesta dell'autorizzazione al Garante, imposto ai titolari che effettuano il trattamento di dati sensibili nei casi menzionati.

Capitolo Terzo

La tutela dei dati sensibili *online* nel contesto italiano ed europeo: la normativa relativa agli *Internet Service Provider* e la sua applicazione da parte della giurisprudenza

1. Il ruolo degli ISP nel trattamento dei dati personali e sensibili

Nei capitoli precedenti è stato rilevato come sia la normativa europea sia quella italiana di recepimento in materia di *privacy* abbiano previsto, fin dalle origini, una disciplina per categorie "speciali" di dati separata da quella generale dei dati comuni, in virtù della loro incidenza negli aspetti più intimi nella sfera privata dell'individuo con la previsione un regime maggiormente garantistico per questi[289]. In tal senso, il Codice dedica, come è stato ampiamente mostrato, numerose disposizioni finalizzate alla tutela dei dati sensibili: nella Parte I contenente le *Disposizioni generali*, al Titolo III sono presenti sia quelle applicabili ai soggetti pubblici sia quelle relative ai soggetti privati ed enti pubblici economici, prevedendo due regimi diversi a seconda del titolare del trattamento dei dati sensibili[290].

La necessità di una tutela più intensa per tali dati è richiesta soprattutto nell'era digitale[291] in cui Internet, citando le parole di una sentenza di primo grado di un caso giurisprudenziale che sarà analizzato nei seguenti paragrafi[292], rappresenta molto spesso, in assenza di specifiche regolamentazioni, *"la sconfinata prateria dove tutto è permesso"*. Inoltre, proprio in rete il flusso dei dati personali scorre molto più velocemente e le regole tradizionali concernenti il rispetto della *privacy* in tutti i suoi aspetti previste dalla normativa spesso sono ignorate[293].

---

[289] In tal senso, nel capitolo precedente, è stato precisato come il *Codice della privacy* affidi al previo consenso da parte dell'interessato, manifestato in forma scritta *ad substantiam* pena la sua la validità, e l'autorizzazione da parte del Garante, rappresentino le adeguate garanzie ai fini del trattamento dei dati sensibili.

[290] Nel Capo II sono presenti le disposizioni relative all'applicazione di regole specifiche da parte dei soggetti pubblici; al Capo III, invece, quelle per i soggetti privati ed enti pubblici economici. Si rinvia al terzo paragrafo del secondo capitolo per una disamina sulle differenze tra i due regimi nel trattamento dei dati sensibili.

[291] Cfr. D. Finocchiaro, *Privacy e protezione dei dati personali. Disciplina e strumenti operativi*, Bologna, 2012, pp. 56-60 e pp. 205-209 e R. Popoli, *Social network e concreta protezione dei dati sensibili: luci ed ombre di una difficile convivenza*, Il Diritto dell'informazione e dell'informatica, Anno XXiX - Fasc.6, 2014. Le autrici sottolineano come l'esigenza di garanzie di tutela più forti nell' *online* derivi dal fatto che, maggiormente di quanto accade nell'*offline*, il trattamento illecito dei dati sensibili è potenzialmente idoneo ad arrecare un pregiudizio più lesivo alla persona i cui dati si riferiscono. Così, ad esempio, il danno che può derivare dall'utilizzo delle informazioni riguardanti la salute di una persona in rete è più rischioso data la maggiore capacità diffusiva dei contenuti all'interno del *web* nonché il raggiungimento più immediato di un elevato numero di utenti.

[292] Si fa riferimento alla sentenza del Tribunale di Milano, sez. IV penale, 12 aprile 2010, n.1972 sul caso *Google ViviDown.*

[293] C. Filippi*, Le nuove regole per i servizi di comunicazione elettronica: l'attuazione della direttiva 2002/58. La tutela della riservatezza su Internet e reti telematiche*, in G. Santaniello (a cura di), *La protezione dei dati*

Dunque, seppur sono immediatamente visibili i vantaggi offerti della rete[294], altrettanto evidente è la moltiplicazione dei rischi legati alla tutela della riservatezza in rete in tutti i suoi aspetti legati soprattutto alla previsione di nuovi profili di responsabilità, nei confronti dei dati degli utenti del *web*, posti a carico di alcuni soggetti non previsti nell'*offline* ma che assumono un ruolo centrale nell'*online*: i cd. *Internet service provider* (denominati con l'acronimo ISP) ossia i soggetti che forniscono i servizi di connessione, trasmissione, memorizzazione dati anche mettendo a disposizione spazi di memoria per ospitare i siti[295]. Peraltro, il ruolo assunto da tali figure non è soltanto legato agli aspetti più prettamente economici delle nuove tecnologie, nelle quali i prestatori di servizi *online* forniscono la connessione alla rete, ma, al contrario, coinvolge anche valori più strettamente connessi alle libertà e ai diritti fondamentali della persona[296]: specificamente, le attività degli ISP nei confronti degli utenti, prima di tutte quella dell'accesso alla rete, sono al fondamento della partecipazione dell'individuo alla società e dunque attuativi dei principi di democrazia e sovranità popolare e rappresentano uno strumento utile per esercitare le libertà fondamentali[297]. Ciò ha determinato, prima a livello europeo e poi a quello interno, come si vedrà nel prosieguo, la necessità di prevedere oltre ad una disciplina generale sulla responsabilità da fatto illecito[298] e le ordinarie in materia di responsabilità civile, anche norme specifiche relative al tema della responsabilità degli ISP nel caso di violazioni commesse attraverso i servizi che essi forniscono agli utenti. Dunque, gli illeciti connessi sul web non sono soltanto idonei a imputare una responsabilità in capo ai loro autori materiali ma anche ai prestatori di servizi: illeciti che possono essere di varia natura e difficilmente catalogabili ma che possono essere accumunati dal fatto di essere commessi o consumati attraverso la diffusione o l'utilizzazione dei dati o informazioni dai quali possano derivare violazioni del diritto alla riservatezza, del diritto d'autore, diritto all'onore e alla

---

personali, in Trattato di diritto amministrativo, diretto da Santaniello G., Volume trentaseiesimo, Padova , 2005, p. 617.

[294] Sul punto, si veda, G. Napoli*, Responsabilità dell'Internet Service Provider nella giurisprudenza civile*, in G. Cassano, G. Scorza, G. Vaciago (a cura di), *Diritto dell'internet. Manuale operativo. Casi, legislazione e giurisprudenza*, Padova, 2013, p.463 in cui l'autrice evidenzia come Internet sia capace di condividere e consultare un numero inestimabile di informazioni e di risorse, ovunque queste siano allocate *"facendo sì che gli individui stabiliti ai capi opposti del globo possano facilmente contattarsi e scambiarsi opinioni con banali gesti, ormai istintivi e quotidiani nonché imprescindibili per chiunque".*

[295] Sulla definizione di ISP si veda P. Falletta, *La responsabilità degli Internet Service Provider*, in P. Falletta, M. Mensi, *Il diritto del web. Casi e materiali*, Padova, 2015, p.142.

[296] Sul ruolo non soltanto economico degli ISP si veda M. Gambini, *Gli hosting providers tra doveri di diligenza professionale e assenza di un obbligo generale di sorveglianza sulle informazioni memorizzate,* in *www.costituzionalismo.it/articoli/401/,* 27 dicembre 2011.

[297] Si fa riferimento all' art. 1 Cost. sulla sovranità popolare; all' art. 21 sulla libera manifestazione di pensiero; agli artt. 9 e 33 Cost. sulla libertà di cultura e della ricerca scientifica; all' art. 18 Cost. sulla libertà di associazione; all'art. 15 sulla libertà di corrispondenza; all'art. 41 sulla libertà di iniziativa economica.

[298] Nell'ordinamento italiano, l'art. 2043 del c.c. prevede il regime di responsabilità per fatto illecito: *"Qualunque fatto doloso o colposo, che cagiona ad altri un danno ingiusto, obbliga colui che ha commesso il fatto a risarcire il danno."* Prima dell'entrata in vigore della disciplina vigente in materia di commercio elettronico, nel nostro ordinamenti i casi di responsabilità dei fornitori di servizi veniva ravvisata esclusivamente in questa disposizione.

reputazione[299]. Delineando adesso nello specifico le diverse figure di prestatori di servizi e la rispettiva disciplina applicabile prevista per ognuno di questi, occorre partire dalla normativa di riferimento, ossia la direttiva europea n. 2000/31/CE conosciuta come direttiva *e-commerce*[300] finalizzata ad assicurare la libera prestazione dei servizi *online* nell'Unione europea, creando una base comune di regole per il commercio elettronico in tutto il territorio dell'Unione. La direttiva è stata poi recepita in Italia con il decreto legislativo n. 70 del 2003[301], sostanzialmente riproduttivo della normativa comunitaria[302]. Il principio generale che accompagna il regime di responsabilità dei prestatori dei servizi previsto dalla normativa in materia è quello della *neutralità*[303] secondo cui il prestatore dei servizi non è ritenuto responsabile per il contenuto delle informazioni immesse dagli utenti né di eventuali illeciti commessi da terzi, purché sussistano determinate condizioni. Tale aspetto è previsto all'art. 17 del decreto legislativo n. 70 del 2003 che prevede una clausola generale sia di esclusione dall'obbligo di sorveglianza degli ISP sui contenuti e le informazioni che circolano sulla rete da lui gestita, sia di ricerca attiva dei fatti che indichino la presenza di illiceità. Fatte salve le circostanze, previste al comma 2, che il prestatore sia comunque tenuto: *"ad informare senza indugio l'autorità giudiziaria o quella amministrativa avente funzioni di vigilanza, qualora sia a conoscenza di presunte attività o informazioni illecite riguardanti un suo destinatario del servizio della società dell'informazione; a fornire senza indugio, a richiesta delle autorità competenti, le informazioni in suo possesso che consentano l'identificazione del destinatario dei suoi servizi con cui ha accordi di memorizzazione dei dati, al fine di individuare e prevenire attività illecite".* Infatti, la stessa disposizione al comma 3 prevede una responsabilità civile del prestatore di servizi nel caso in cui non sia intervenuto prontamente ad impedire l'accesso al contenuto nonostante la richiesta da parte dell'autorità competente oppure se, avendo avuto conoscenza del carattere illecito o pregiudizievole per un soggetto terzo del contenuto di un servizio al quale assicura l'accesso, non abbia provveduto ad informare l'autorità suddetta. La

[299] Sul punto G. Napoli, *op. cit.*, p.464.

[300] Direttiva 2000/31/CE del Parlamento europeo e del Consiglio dell'8 giugno 2000 *relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno ("Direttiva sul commercio elettronico")*; pubblicata in G.U. n. L 178 del 17.07.2000, 1-16.

[301] Decreto legislativo 9 aprile 2003, n. 70 *Attuazione della direttiva 2000/31/CE relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno;* pubblicato in G. U. n. 61 del 14.04.2003.

[302] Per un confronto tra il regime di responsabilità degli ISP previsto nell'Unione europea e negli Stati Uniti si rimanda a C. Gattei, *Considerazioni sulla responsabilità dell'Internet provider,* in *www.interlex.it/regole/gattei2.htm*., 23 novembre 1998,

[303] In senso contrario si veda O. Pollicino, *Tutela del pluralismo nell'era digitale: ruolo e responsabilità degli Internet service provider,* in *www.giurcost.org/studi/pollicino1.pdf*, 2014, nel quale l'autore sottolinea come l'evoluzione della fisionomia degli ISP porti ad una distanziazione rispetto alla loro accezione, delineata dalla direttiva, di una neutralità operativa, dato il ruolo sempre più attivo che assumono rispetto ai contenuti degli utenti. L'aspetto relativo al ruolo attivo degli ISP sarà messo in rilievo anche nelle questioni sollevate nei casi giurisprudenziali che saranno affrontati nelle prossime pagine.

normativa vigente, tanto quella europea quanto quella italiana, prevedono diversi regime di responsabilità a secondo del servizio prestato. Il decreto legislativo n. 70 del 2003 ne prevede nello specifico tre:

- l'attività di *mere conduit*, ossia di mero trasporto e disciplinata dall'art. 14, la quale consiste nella trasmissione sulla rete di informazioni fornite o nella semplice fornitura dell'accesso alla rete. Entrambi profili di attività includono la memorizzazione automatica, intermedia e transitoria delle informazioni trasmesse, a condizione che questa serva solo alla trasmissione sulla rete e che abbiano una durata limitata alle finalità della trasmissione stessa o dell'accesso. In questo caso, l'intermediario è ritenuto responsabile soltanto se non abbia dato egli stesso origine alla trasmissione o non selezioni il destinatario di suddetta trasmissione;
- l'attività di *caching* ossia di memorizzazione temporanea delineata dall'art. 15 che consiste nel trasmettere su una rete i dati forniti da un destinatario del servizio. Anche per questo tipo di attività non è prevista una responsabilità generale dell'ISP a meno che quest'ultimo non modifichi le informazioni; si conformi alle condizioni di accesso e alle norme di aggiornamento del settore stesso; non interferisca con l'uso lecito della tecnologia; oppure intervenga prontamente a rimuovere le informazioni che ha memorizzato o disabiliti l'accesso qualora venga a conoscenza che le informazioni siano state rimosse dal luogo dove si trovavano inizialmente sulla rete o che l'accesso sia stata disabilitato, o ancora che l'autorità competente disponga la rimozione o disabilitazione dell'accesso;
- l'attività di *hosting* ossia la memorizzazione permanente delle informazioni fornite dai destinatari, disciplinata dall'art. 16 del decreto. In questo caso, al prestatore di servizi non è imputata nessuna responsabilità delle informazioni memorizzate a richiesta di un destinatario, salva la circostanza che non sia a conoscenza dell'illiceità delle informazioni e, per quanto attiene alle azioni risarcitorie, non sia al corrente di fatti o circostanze che rendano manifesta l'illegalità dell'attività o dell'informazione e, una volta messo al corrente, agisca nell'immediato per rimuovere le informazioni o disabilitare l'acceso.

Le disposizioni in esame definiscono in negativo, *ad excludendum*, le condizioni alle quali gli ISP non rispondano civilmente per gli illeciti commessi[304]: tali condizioni sono analoghe, come si è detto, nella normativa europea e quella italiana in materia[305] di commercio elettronico, anche se nella seconda è precisato che l'ISP risponda nel caso di mancata rimozione dei contenuti illeciti qualora non ottemperi a richieste specifiche dell'autorità pubblica.

[304] Si veda ancora G. Napoli, *op. cit.,* p.466.
[305] Sul punto si rimanda a P. Falletta, *op. cit.,* p.150

1.1 Il contributo della giurisprudenza sulla responsabilità degli ISP

Il quadro normativo delineato è stato integrato dal contributo dei giudici europei ed italiani che hanno precisato quale fosse il regime di responsabilità applicabile in capo ai prestatori di servizi. Soffermando l'attenzione sui principali interventi giurisprudenziali in materia, la Corte di Giustizia, chiamata a pronunciarsi in seguito ad un rinvio pregiudiziale sulla legittimità di una norma che predisponeva un sistema di filtraggio in capo ai prestatori di servizi al fine di tutelare il diritto di autore in rete[306], imponeva ai giudici e alle autorità nazionali competenti di garantire il giusto equilibrio tra la tutela del diritto alla proprietà intellettuale e la libertà di impresa. Nel caso di specie, tale bilanciamento per la Corte sarebbe stato compromesso dalla previsione di un sistema di filtraggio a carico dei prestatori dei servizi in quanto oltre all'obbligo di prevedere un sistema informatico costoso, sarebbe stato in violazione dell'art. 15 della direttiva *e-commerce*[307]che, con contenuto analogo all'art.17, prevede l'assenza di un obbligo di sorveglianza. Ancora, la Corte continuava sostenendo che tale sistema avrebbe leso anche il diritto alla tutela dei dati personali e la libertà di informazione dei clienti degli ISP previsti agli artt. 8 e 11 della Carta dei diritti fondamentali dell'Unione europea: infatti la previsione di detto sistema da un lato avrebbe portato alla conoscenza degli indirizzi IP degli utenti che costituiscono dati personali protetti, dall'altro, non potendo distinguere tra contenuti leciti e illeciti, avrebbe potuto bloccare anche le informazioni rientranti nel primo tipo incidendo sulla libertà di informazione.

Anche i giudici italiani hanno posto l'attenzione sui casi di esonero della responsabilità degli ISP sia sul suddetto divieto di un obbligo generale di sorveglianza sia rispetto a motivi oggettivi e soggettivi di esclusione. Con riferimento al primo caso, il Tribunale di Roma[308] aveva aggirato inizialmente la previsione di tale divieto, ammettendo che in caso di accertate ipotesi di illecito sullo spazio *web* degli ISP, questi fossero obbligati a predisporre un sistema di sorveglianza dei contenuti onerosi e generalizzati, al fine di impedire in futuro qualsiasi altra violazione dei diritti nei confronti di terzi. Ma, in altre pronunce, si è evidenziata la circostanza che non vi sia un obbligo di controllo preventivo sui contenuti immessi e che dunque, non esiste *"[…] un obbligo di legge codificato che imponga agli ISP un controllo preventivo*

[306] Corte di Giustizia delle Comunità europee, terza sezione, 24 novembre 2011, *Scarlet Extended SA Vs SABAM* e Corte di giustizia delle Comunità europee, terza sezione, 16 febbraio 2012, *SABAM Vs Netlog.*

[307] L'art. 15 della direttiva n.2000/31/CE prevede che *"1. Nella prestazione dei servizi di cui agli articoli 12, 13 e 14, gli Stati membri non impongono ai prestatori un obbligo generale di sorveglianza sulle informazioni che trasmettono o memorizzano né un obbligo generale di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite.*

2. Gli Stati membri possono stabilire che i prestatori di servizi della società dell'informazione siano tenuti ad informare senza indugio la pubblica autorità competente di presunte attività o informazioni illecite dei destinatari dei loro servizi o a comunicare alle autorità competenti, a loro richiesta, informazioni che consentano l'identificazione dei destinatari dei loro servizi con cui hanno accordi di memorizzazione dei dati."

[308] Tribunale di Roma, 16 dicembre 2009, *RTI Vs Youtube e Google.*

dell'innumerevole serie di dati che passano ogni secondo nelle maglie dei gestori o dei proprietari dei siti web"[309]. In altre pronunce, invece, è stata ricollegata la condizione di esonero di responsabilità legata al divieto previsto all'art.17, alla condizione soggettiva del prestatore di servizi. Nel caso di specie, il giudice ha fatto una differenziazione tra l'attività di *hosting* attivo e passivo, in cui il primo svolge un ruolo di immissione dei contenuti propri o di terzi, contrariamente al secondo e, similmente al *content provider*[310], risponde direttamente alle regole comuni sulla responsabilità: nel caso in questione, il giudice riteneva infatti che il *provider* fosse un *hosting* passivo e dunque non ritenuto responsabile per illeciti non ancora commessi[311]. Infine, i giudici italiani si sono occupati anche del profilo relativo all'esonero di una responsabilità soggettiva del prestatore di servizi: nello specifico, è stata considerata la condizione della conoscenza da parte del *provider* del carattere illecito o pregiudizievole nei confronti di un terzo del contenuto di un servizio al quale egli assicura l'accesso. Così nel caso dell'invio di una diffida da parte del titolare di un diritto di proprietà intellettuale che non contenga una dettagliata e specifica indicazione del video da eliminare e delle pagine *web*, non fa nascere una responsabilità nei confronti dell'*hosting provider*[312]. Al contrario qualora vi fossero tali condizioni, utili per individuare la presenza di eventuali illeciti, la giurisprudenza del caso in esame ha ritenuto che il fornitore dei servizi possa effettuare controlli rientranti nelle sue "possibilità" come ad esempio quelli posti attraverso i *software* che svolgono un'analisi automatizzata dei contenuti[313].

Dopo aver delineato quanto sia la normativa quanto la giurisprudenza siano state determinati nella definizione del ruolo e del regime di responsabilità degli ISP sul *web*, nei seguenti paragrafi saranno affrontati alcuni dei più rilevanti casi giurisprudenziali degli ultimi anni relativi al tema trattamento dei dati personali e sensibili da parte di alcuni *provider* che dominano la rete.

[309] Tribunale di Milano, sezione IV penale, 12 aprile 2010, n. 1972, *Google Vs Vivi down.* L'intera vicenda relativa al caso *Google Vs Vividown* sarà ampiamente affrontata nei paragrafi seguenti.

[310] Per la distinzione tra le due figure si rimanda a G. Cassano e F. Buffa, *Responsabilità del content provider e dell'host provider content provider*, in *www.altalex.com/documents/news/2005/07/19/responsabilita-del-content-provider-e-dell-host-provider*, 14 febbraio 2003 , in cui l'autore definisce il *content provider* come il soggetto che fornisca contenuti e risponda direttamente per eventuali illeciti perpetrati con la diffusione dei medesimi contenuti.

[311] Tribunale di Roma, IX sezione, 20 ottobre 2011, *RTI Vs Choopa.*

[312] Si rinvia alla citata ordinanza del Tribunale di Milano sul caso *RTI Vs Choopa.*

[313] P. Falletta, *op. cit.*, p.154.

2. La tutela dei dati sensibili nell'era di internet in Italia: il caso *Google VS Vividown*

Gli aspetti messi in rilevo nel paragrafo precedente relativi agli interrogativi continuamente sollevati dinanzi alla giurisprudenza sul regime di responsabilità applicabile nei confronti dei *provider*, che si pongono soprattutto nei casi di caricamento dei contenuti da parte dei loro utenti incidendo sul trattamento dei dati personali e sensibili in rete, vengono particolarmente in rilievo in un caso affrontato dalla giurisprudenza italiana, che si è concluso con la pronuncia definitiva della Corte di Cassazione nel dicembre 2013. Si tratta del noto caso giurisprudenziale *Google Vs Vividown*, in cui l'*Internet Service Provider* era stato accusato da parte di un'associazione finalizzata alla tutela delle persone affette da autismo, Vividown appunto, di avere responsabilità penale per la pubblicazione di un video contenente informazioni relative alla salute di un minore, sulla piattaforma *Google Video.* Peraltro, il processo ebbe grande impatto e risonanza anche nei confronti dell'opinione pubblica, grazie al confitto tra i diversi valori ed interessi che facevano capo alle parti in causa: oltre al suddetto ruolo dell'ISP e le responsabilità legate alla possibilità di tenere sotto controllo le informazioni in rete, riguardava anche il tema più generale della libertà di impresa, della potenziale invasività e capacità diffusiva maggiore delle nuove tecnologie rispetto ai mezzi di informazioni tradizionali, e l'amplificazione del "male" sul *web* maggiormente incidente sulla dignità della persona lesa. Nel caso di specie, alcuni hanno sottolineato che la difficoltà di venire a capo di una soluzione pacifica era dovuta proprio a tale conflitto tra valori contrastanti inteso come *"[..] il caso in cui il giurista sia chiamato, in un certo senso e in determinate situazioni, a "pesare" tanti valori in gioco e a cercare di trovare una sorta di compromesso. Già è difficile trovare un simile equilibrio in casi dove non è presente la tecnologia; si pensi a quanto può diventare complesso farlo in casi che presentino, oltre a un lato umano molto forte (e spesso tragico), anche una tecnologia capace di mutare i comportamenti delle persone e, persino, lo sfondo dove si svolgono i fatti."*[314] Dunque, tutti i giudici, dal primo grado fino alla Cassazione, che si sono pronunciati sulla questione, hanno avuto l'arduo compito di pesare tutti questi elementi in un processo caratterizzato da uno stretto legame tra le strategie commerciali, i valori dell'individuo e l' individuazione delle responsabilità oggettive, e che per tali ragione hanno subìto delle critiche, come si vedrà nei paragrafi che seguono.

[314] In questi termini, G. Ziccardi, *Caso Google Vividown. L'assoluzione non sana il conflitto, in www.ilfattoquotidiano.it/2012/12/22/caso-google-vividown-lassoluzione-non-sana-conflitto/453672/,* 22 dicembre 2012.

2.1 La ricostruzione della vicenda

La vicenda ha inizio nel maggio 2006, data in cui alcuni studenti di un Istituto tecnico di Torino giravano, all'interno dei locali della scuola, un video, di durata di circa tre minuti e mezzo[315], in cui insultavano e picchiavano un ragazzo affetto da autismo[316] e sostenevano di far parte dell'Associazione Vivi Down[317]. Tale video, dopo 4 mesi, l'8 settembre veniva caricato su Google, in particolare nel servizio Google Video: facilmente condivisibile, il video non solo rimase *online* circa due mesi, ma si collocava anche al primo posto della sezione "Video Divertenti", totalizzando circa 5500 visualizzazioni prima della sua rimozione. Due mesi dopo, il 6 novembre, un blogger italiano, Alessandro D'Amato, titolare del sito *www.giornalettismo.ilcannochiale.it*, per primo denunciò la presenza del video segnalandolo a Google.[318] Da allora la notizia fece il giro dei media, tanto quelli tradizionali come la carta stampata sia i "nuovi" media. Tale aspetto mise subito in rilievo anche le differenze tra le reazioni del suddetto mondo tradizionale dell'informazione rispetto a quello più attuale e ricco di spunti del *web*: i primi, infatti, furono più cauti ad intervenire sulla questione sia per il tema delicato oggetto del processo sia per la possibile reazione degli utenti tipo dei media tradizionali, considerati come poco interessati al problema[319]; al contrario del mondo di internet, in cui *blog*, *vblog* hanno mostrato grande interesse dal primo momento, ponendo un tema così delicato all'attenzione dell'opinione pubblica, a partire proprio dalla segnalazione da parte del blogger. Dopo la scoperta del video, inoltre, da più fronti arrivarono indignazioni: da alcuni articoli del *Giorno* e *Repubblica* che denunciavano la scoperta del video, agli interventi di sociologi, giornalisti che trattarono del tema del bullismo, fino a quello dell'allora Ministro dell'Istruzione Giuseppe Fioroni che preannunciò la volontà di costituirsi come parte civile nel processo nei confronti dei ragazzi autori del video, ancora prima della loro identificazione[320]. Dopo la segnalazione da parte del *blogger*, il 7 novembre la Polizia Postale invitava Google a

[315] Precisamente, nel video, comparivano, una decina di compagni di classe che rimanevano a guardare mentre uno di loro sferrava pugni a calcio al ragazzo disabile, un altro riprendeva la scena con la telecamera e, un altro ancora, disegnava alla lavagna il simbolo "SS" e faceva il saluto fascista. Nell'indifferenza della classe, il ragazzo aggredito rimaneva immobile.

[316] Non da sindrome di down come era stato comunicato, erroneamente, in un primo momento.

[317] L'Associazione Vivi Down Onlus è l'Associazione Italiana per la Ricerca Scientifica e la Tutela della Persona con la sindrome di Down. Fornisce alle persone con Sindrome di Down e alle loro famiglie, gli strumenti per sostenere le difficoltà che la disabilità comporta. Fu parte civile, come adesso si dirà, nel processo. Il sito dell'associazione è consultabile su *www.vividown.org/*.

[318] L'aspetto legato alla rimozione del video è stato oggetto di un aspro scontro tra l'accusa e la difesa. Per l'accusa e le parti civili, il video fu rimosso solo dopo le pressioni scaturite dall'indignazione dell'opinione pubblica e da quelle istituzionali facenti capo alla polizia postale nei confronti di Google. Al contrario, la difesa sostenne come i sistemi di controllo funzionarono dato che la rimozione del video avvenne dopo due giorni dalla denuncia del blogger italiano. Si veda sul punto G. Camera, O. Pollicino, *La legge è uguale anche sul web: Dietro le quinte del caso Google-Vividown*, Milano, 2010, p. 36.

[319] Di quest'opinione, ancora, G. Camera, O. Pollicino, *ibidem*, pp. 28-29.

[320] L'intervento dell'allora Ministro dell'Istruzione è consultabile alla pagina *www.archiviostorico.corriere.it/2006/novembre/14/Video_sul_ragazzo_Down_ministero_co_9_061114046.shtml.*

valutare il caso di rimuovere il video, mentre, nella stessa data, dagli Stati Uniti, in cui ha sede Google Inc., arrivò l'autorizzazione per la rimozione del video che effettivamente venne tempestivamente rimosso da Google. Il 9 novembre, l'Associazione Vivi Down sporse querela per il fatto ed il 13 novembre la Polizia comunicava i fatti alla Procura della Repubblica precisando che il video oggetto della questione si trovasse sul *server* allocato all'estero. Dunque, l'inchiesta partiva dalla denuncia, presentata in Procura dal legale dell'Associazione suddetta, in cui l'avvocato Guido Camera, ipotizzava un reato di diffamazione aggravata a danno della stessa, in quanto, nei video pubblicati, uno dei ragazzi protagonisti si qualificava come appartenente all'Associazione. Non solo, perché l'Associazione riteneva vi fosse stato anche un trattamento illecito dei dati personali da parte di Google. La denuncia da parte del presidente di Vivi Down, Edoardo Censi, descriveva tutti i contenuti del video in questione soffermandosi su come, fin dai primi minuti, fossero visibili i comportamenti *deplorevoli* facenti capo al gruppo di ragazzi nei confronti del coetaneo affetto dalla sindrome di down e come rientrasse nei termini del reato di diffamazione l'attribuzione del gesto effettuato nei confronti dell'Associazione. Inoltre, anche il padre del ragazzo insultato nel video sporgeva denuncia e chiedeva l'accertamento delle responsabilità per la pubblicazione del video. Fu proprio nelle parole del padre che si scorgeva quanto il video mostrasse l'incidenza perpetrata nella sfera più intima del ragazzo oggetto di scherno, ossia, nel caso di specie, quello della sua salute attraverso i comportamenti dei ragazzi autori del video. Infatti nella denuncia depositata dal padre del ragazzo si diceva che: *"[..] Da un punto di vista prima umano che giuridico è quasi superfluo raccontare lo strazio di un padre nel vedere il proprio figlio, cresciuto con tanto amore pur in mezzo alle difficoltà che la sua condizione psico-fisica comporta, trattato alla stregua di un fenomeno da barraccone, umiliato per il solo fatto di essere più debole [..]".*
Ancora, venivano anche in rilevo i profili di responsabilità imputati nei confronti dell'ISP sottolineando come *"[..] Non si comprende come un video di tale portata, [..], abbia non solo potuto circolare indisturbato tra le pagine di internet, ma sia addirittura finito all'interno di una classifica ufficiale dei video più scaricati da un sito [..]".*
Infatti, anche se nel corso del processo il genitore del ragazzo ritirò la querela sporta nei confronti di Google[321], entrambe le parti portavano all'attenzione della Procura di Milano la necessità di valutare della responsabilità penale suddetta, non solo a carico dei minori autori del video, i quali furono processati dinanzi al Tribunale dei minori[322], ma anche dei responsabili del sito internet nel quale il video occupava anche la prima posizione nella categoria dei "Video più

[321] I genitori del ragazzo ritirarono la querela a seguito delle scuse da parte di Google Italia ed alle iniziative di Google promosse in ambito sociale, ritenendo che proseguire il processo non avrebbe tutelato il ragazzo.
[322] Nel dicembre 2007, il Tribunale dei minorenni condannava gli studenti a 10 mesi di lavoro al servizio della comunità.

divertenti". Il processo quindi vedeva come parti civili del processo l'associazione Vivi Down e il Comune di Milano[323] , mentre come imputati i manager di Google: David Carl Drummond, l'allora presidente del CDA di Google Italy, George De Los Reyes, allora membro del cda di Google Italy e Peter Fleischer, responsabile delle strategie per la *privacy* per l'Europa di Google Inc.

2.2 Le motivazioni del giudice di primo grado: "tanto rumore per nulla"

In seguito alle indagini preliminari condotte dalla Procura di Milano, il giudice di primo grado, si pronunciò nel 2010 con la sentenza n. 1972 [324] prevedendo una condanna in primo grado di reclusione per i dirigenti di Google per violazione della normativa sulla *privacy* e con una assoluzione per il reato di diffamazione. Prima di analizzare i capi di imputazione del processo e le motivazioni della sentenza, pare opportuno evidenziare come il giudice estensore della sentenza di primo grado, il magistrato Oscar Magi, sembrò sottovalutare la carica innovativa del caso in questione, citando, nel dispositivo della sentenza, la famosa commedia shakespeariana "*too much ado about nothing"* ossia tanto rumore per nulla, sostenendo come in realtà non vi fossero elementi di discontinuità nel caso di specie rispetto a questioni simili giurisprudenziali di cui si era già affrontato. In realtà, è stato rilevato come la pronuncia in questione avesse una carica innovativa tanto da un punto di vista procedurale quanto da quello sostanziale e di merito, pur in presenza di aspetti di continuità con la prassi e la giurisprudenza precedente[325]: il primo aspetto riguardava l'applicabilità o meno della normativa italiana al caso oggetto del processo; il secondo, invece, il monito del giudice ai fornitori dei servizi in rete, a rispettare gli obblighi previsti dalla normativa europea e italiana finalizzati alla tutela dei dati personali.

La sentenza di primo grado iniziava con l'esposizione dei due capi di imputazione: il capo A riguardava l'ipotesi di reato per diffamazione in capo ai dirigenti di Google[326], mentre il Capo B

[323] La sede di Google Italia ha sede infatti a Milano.
[324] Tribunale di Milano, sez. IV penale, 12 aprile 2010, n.1972.
[325] G. Camera, O. Pollicino, *op. cit.*, p. 121.
[326] Il reato di diffamazione è previsto all'art. 595 c. p.:*"Chiunque, fuori dei casi indicati nell'articolo precedente, comunicando con più persone, offende l'altrui reputazione, è punito con la reclusione fino a un anno o con la multa fino a milletrentadue euro.*
Se l'offesa consiste nell'attribuzione di un fatto determinato, la pena è della reclusione fino a due anni, ovvero della multa fino a duemilasessantacinque euro.
Se l'offesa è recata col mezzo della stampa [57-58bis] o con qualsiasi altro mezzo di pubblicità, ovvero in atto pubblico [2699], la pena è della reclusione da sei mesi a tre anni o della multa non inferiore a cinquecentosedici euro.
Se l'offesa è recata a un Corpo politico, amministrativo o giudiziario, o ad una sua rappresentanza, o ad una Autorità costituita in collegio [342], le pene sono aumentate".

contestava agli imputati il concorso al trattamento illecito dei dati personali previsto all'art. 167 del *Codice della privacy.*

Tralasciando le considerazioni "in fatto" del giudice in cui si ricostruiva tutta la vicenda giudiziaria, analizziamo adesso le parti più rilevanti del ragionamento posto in essere dal giudice che portarono alla condanna in primo grado dei manager di Google[327].

Il primo elemento significativo della pronuncia stava nell'identificazione della giurisdizione italiana come quella competente della controversia, dopo che la difesa degli imputati aveva sollevato la questione di incompetenza territoriale del Tribunale di Milano. La difesa infatti, richiamando il secondo comma dell'art. 5 del *Codice della privacy* relativo all'ambito di applicazione del trattamento dii dati personali non effettuati in Italia[328], si concentrava sul presupposto che fosse rilevante soltanto il luogo in cui era localizzato il *server* che aveva raccolto ed in un primo tempo elaborato il video: ossia negli Stati Uniti, a Denver in cui sono ubicati i *server* di Google Inc. che trattano i dati provenienti da tutto il mondo. Dunque, Google Italia, per la difesa, avrebbe svolto soltanto un ruolo di *marketing* per conto della casa madre e di non avere alcun ruolo nel trattamento di tali dati[329]. Il giudice, al contrario, seguendo quanto sostenuto dai pubblici ministeri, ritenne che non doveva necessariamente esserci una corrispondenza tra i luoghi di localizzazione dei *server* e quelli nei quali aveva luogo il trattamento dei dati personali in quanto: in primo luogo, il trattamento dei dati non ha una consumazione istantanea, e come aveva sottolineato anche il padre del ragazzo vittima dell'atto di bullismo nel testo della denuncia, si articola in un processo che ha luogo in tempi ed in luoghi diversi e quindi *anche* in Italia; in secondo luogo, si fece leva sulla nozione di *trattamento* prevista dal *Codice*[330] definita come ampia da ricomprendere tutta la sequenza di atti che vanno dall'immissione del dato in rete alla sua diffusione; infine, venne dato dal giudice un significato esteso del concetto di *"strumento"* previsto dal citato art. 5 del *Codice* per

---

L'art. 110 c.p. invece riguarda il concorso al reato di più persone: *"Quando più persone concorrono nel medesimo reato, ciascuna di esse soggiace alla pena per questo stabilita, salve le disposizioni degli articoli seguenti."*

[327] Preliminarmente, il giudice evidenziava che il ritiro della querela da parte dei familiari del ragazzo offeso seppur limitava l'accertamento ai fatti che riguardano l'altra parte lesa, l'associazione ViviDown, non faceva però decadere l'imputazione del capo A, contrariamente a quanto aveva sostenuto dalla difesa.

[328] L'art. 5, comma 2 del decreto legislativo n.196/ 2003 prevede che *"Il presente codice si applica anche al trattamento di dati personali effettuato da chiunque è stabilito nel territorio di un Paese non appartenente all'Unione europea e impiega, per il trattamento, strumenti situati nel territorio dello Stato anche diversi da quelli elettronici, salvo che essi siano utilizzati solo ai fini di transito nel territorio dell'Unione europea. In caso di applicazione del presente codice, il titolare del trattamento designa un proprio rappresentante stabilito nel territorio dello Stato ai fini dell'applicazione della disciplina sul trattamento dei dati personali".*

[329] Nozione fondamentale, ai sensi del citato art. 5 del *Codice,* ai fini dell'applicabilità della normativa.

[330] L' art. 4, comma 1, lettera a) del *Codice* definisce il trattamento dei dati come *"qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati".*

identificare la normativa applicabile[331]. Dunque, il giudice rigettò l'eccezione di incompetenza territoriale sollevata dalla difesa degli imputati, che aveva sostenuto come il reato contestato fosse avvenuto a Torino dove erano stati immessi i dati sensibili e scaturito il processo. Ammise, infatti, che seppur la vicenda era iniziata a Torino nel momento del caricamento del video sul sito Google Video, una *parte* delle operazioni rientranti nella citata nozione di trattamento, fosse avvenuta proprio a Milano, sede di Google Italia con la conseguente competenza del Tribunale di Milano.

Dopo aver affrontato tali questioni preliminari, il giudice strutturò le motivazioni della sentenza verificando se fossero imputabili a Google i reati contestati dalla difesa.

Con riferimento al primo capo di imputazione sul reato di diffamazione, l'accusa aveva pertanto ritenuto responsabili del reato non soltanto gli studenti che avevano girato e caricato il video ma anche i responsabili di Google per comportamento omissivo ai sensi dell'art. 40 c.p. secondo cui *"Non impedire un evento, che si ha l'obbligo giuridico di impedire, equivale a cagionarlo":* la diffamazione non sarebbe stata impedita perché non erano stati rispettati l'art. 13 sull'informativa, l'art. 26 sui dati sensibili e l'art. 17 sul trattamento che presenta rischi specifici del *Codice della privacy.* Il magistrato sottolineò come il video non soltanto ledeva la dignità del protagonista ma offendeva anche la reputazione dell'Associazione ViviDown, organismo posto alla tutela delle persone affette da sindrome di down. Entrambi gli aspetti erano stati amplificati dalla diffusione e permanenza del video sulla piattaforma del server. Il giudice pur evidenziando la valenza diffamatoria nei confronti dei soggetti in questione, rigettò la questione sollevata dai pubblici ministeri, non rintracciando profili di responsabilità in capo alla società in base alla normativa vigente che non prevede un generale obbligo di sorveglianza da parte degli ISP[332]. Contrariamente a quanto sostenuto dall'accusa, il giudice affermò che tale impostazione non sarebbe consentita né dalla legislazione in materia di cui si è parlato né dalla logica applicabile al caso concreto sostenendo che pur ammettendo l'esistenza di tale obbligo in capo a Google, ciò non sarebbe stato sufficiente ad impedire l'evento sanzionatorio: infatti *"[…]anche se l'informativa sulla privacy fosse stata data in modo chiaro e comprensibile all'utente, non può certamente escludersi che l'utente medesimo non avrebbe caricato il file video incriminato, commettendo il reato di diffamazione".* Per tali ragione si giunse all'assoluzione per il reato di diffamazione nei confronti dei responsabili di Google. Successivamente, il giudice si concentrò sull'accertamento della violazione da parte della

[331] Il giudice infatti ritenne che i *server* non esauriscano gli "strumenti" situati nel territorio dello Stato al fine di garantire tutela al trattamento dei dati sensibili di una persona anche quando il responsabile di detto trattamento non si trovi nel territorio comunitario.

[332] Tale divieto è previsto dall'art. 17 del decreto legislativo 9 aprile 2003, n. 70, per il quale si rinvia al primo paragrafo del presente capitolo.

società sulla disciplina prevista dal *Codice ex* art.167, soffermandosi su un aspetto essenziale ai fini del tema oggetto di questo elaborato. Infatti, chiarì che nel caso di specie non si trattasse di dati soltanto personali ma anche di quelli sensibili, in grado di dare informazioni sullo stato di salute del protagonista del video. La semplice "visione", continuava il giudice, dello stato di salute del ragazzo diversamente abile seppur imprecise[333] , avevano inciso fortemente sulla sua dignità e sul suo diritto che informazioni così riservate non venissero diffuse senza aver prestato preventivamente il consenso previsto ai sensi dell'art. 23 del *Codice*. Proprio su tale punto, il giudice sostenne che non vi era dubbio che non solo non era stato prestato il consenso da parte dell'interessato, ma non gli era neanche stato richiesto: per tali ragioni ritenne sussistenti tutte le condizioni per l'identificazione di un trattamento illecito di dati personali ai sensi dell'art. 167 del *Codice della privacy*[334]. Prima di arrivare a tali conclusioni, il giudice dovette accertare se la responsabilità penale ricadesse nei confronti dei dirigenti di Google ossia accertare se il trattamento illecito fosse effettivamente imputabile a Google, oltre che agli autori del video, e se, in caso di esito positivo, fosse stato effettuato ai fini di un profitto così come prevede la disposizione. È proprio in questa parte del dispositivo che viene in luce il secondo elemento fortemente innovativo della decisione che si ritrova nelle seguenti parole del giudice: *"[..] non esiste, in materia, una zona franca (dal punto di vista oggettivo) che consenta ad un qualsiasi soggetto (persona fisica o meno che sia) di ritenersi esente dall'obbligo di legge, nel momento in cui venga, in qualsiasi modo, in possesso di dati sensibili: trattamento di dati è qualsiasi comportamento che consenta ad un soggetto di apprendere un dato e di mantenerne il possesso, fino al momento della sua distruzione."* Il fine del giudice era quello di voler ridurre al massimo questa zona franca rendendosi però conto dell'impossibilità tecnica da parte degli ISP di rispettare un obbligo così generalizzato rispetto ai dati sensibili: infatti, i *provider* dovrebbero poter controllare preventivamente i contenuti dei materiali immessi in rete, escludendo così la pubblicazione di ciò che riguardi soggetti terzi e che non abbia ricevuto il loro consenso. Ma tale previsione sarebbe in contrasto con la normativa vigente che prevede un divieto di obbligo generale di sorveglianza in capo agli ISP dei dati immessi nei loro sistemi informatici, di cui si è detto anche relativamente al primo capo di imputazione. In particolare, il giudice decise che non vi fosse tale obbligo nei confronti di Google, non abbracciando

[333] In quanto, come è stato evidenziato in precedenza, non era affetto da sindrome di down come uno dei ragazzi protagonisti del video alludeva ma autistico.

[334] L'art. 167 del *Codice* prevede che *"1. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sè o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 18, 19, 23, 123, 126 e 130, ovvero in applicazione dell'articolo 129, è punito, se dal fatto deriva nocumento, con la reclusione da sei a diciotto mesi o, se il fatto consiste nella comunicazione o diffusione, con la reclusione da sei a ventiquattro mesi.*
2. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sè o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 17, 20, 21, 22, commi 8 e 11, 25, 26, 27 e 45, è punito, se dal fatto deriva nocumento, con la reclusione da uno a tre anni."

completamente la tesi dei pubblici ministeri che avevano sostenuto come l'ISP non si fosse comportato come mero intermediario e identificando su di esso degli obblighi positivi, come si dirà nel prosieguo.[335] Tuttavia, sostenne che Google Italia non aveva adempiuto ad un altro obbligo previsto dalla normativa italiana, ossia quello di fornire una corretta e puntuale informazione sulle modalità di trattamento dei dati personali prevista all'art. 13 del Codice. Secondo, il giudice infatti le relative informazioni erano mimetizzate all'interno delle generiche condizioni generali del contratto; al contrario, l'ISP avrebbe dovuto avvertire in modo chiaro, esplicito e puntuale gli *uploaders* del video incriminato della necessità di acquisire il consenso preventivo dell'interessato, per giunta scritto perché riguardante il trattamento dei suoi dati sensibili. Motivazione che fu criticata dall'allora Garante della tutela dei dati personali, il quale in un'intervista rilasciata al *Sole 24 Ore* ritenne che la disposizione relativa all'informativa prevista dal *Codice* contenesse obblighi diversi da quelli che il giudice riteneva che Google avesse violato[336]. In realtà, altri[337] hanno sottolineato come il giudice, ponendo in rilievo la sensibilità dei dati trattati, avesse voluto considerare come la mancanza di una corretta informativa, comprendente *anche* l'obbligo di avvertire l'utente di procurarsi il consenso del soggetto al quale appartengono i dati, sia stata, nel caso di specie, determinante nell'impedire che tale consenso fosse effettivamente acquisito.

Collegato a tale aspetto vi era il secondo interrogativo sciolto dal giudice, il quale precisò che ai fini della sussistenza dell'illecito penale previsto dal *Codice,* fosse necessario il *dolo,* ossia la coscienza e la volontà di trattare dei dati in questione al fine di trarne profitto. Infatti, nella decisione veniva sottolineato come suddetta finalità era riscontrabile e ricollegabile all'interazione commerciale tra Google Italia e Google Video parlando, con riferimento a Google Video, di una *"chiara accettazione consapevole del rischio di inserimento e divulgazione di dati sensibili, che avrebbero dovuto essere oggetto di particolare tutela".*[338]Con una frase particolarmente significativa, il giudice infatti sosteneva *"[..] non è la scritta sul muro che costituisce reato per il proprietario del muro, ma il suo sfruttamento commerciale può esserlo"* poiché un profitto per Google Video c'era stato sicuramente attraverso il Sistema *AdWords,* servizio di Google che associa messaggi pubblicitari prodotti

[335] I PM, infatti, sostenevano che Google Italia avesse avuto una responsabilità per il trattamento illecito di dati personali sensibili perché nel prestare il servizio video non aveva soltanto messo semplicemente a disposizione degli utenti una piattaforma, ma era stata parte attiva nel trattamento dei dati al fine trarre un profitto attraverso la vendita di pubblicità ad *hoc*, tesi che sarà abbracciata anche dal giudice come adesso si dirà.

[336] L'intervista fu rilasciata al *Sole 24 Ore* dell'allora Garante della *privacy,* Francesco Pizzetti, il 16 aprile 2010. Il testo integrale dell'intervista è consultabile su *www.ilsole24ore.com/art/SoleOnLine4/Tecnologia%20e%20Business/2010/04/sentenza-google pizzetti.shtml?uuid=AbarP6CF.*

[337] G. Camera, O. Pollicino, *op. cit.*, pp. 137- 138.

[338] Si veda sul punto, S. Mariani, *Internet non è una "zona franca". Condannati i dirigenti di Google.*, in *www.altalex.com/documents/news/2010/04/26/internet-non-e-una-zona-franca-condannati-i-dirigenti-di-google,* 27 aprile 2010.

dagli inserzionisti alle ricerche degli utenti fatte attraverso il servizio di ricerca di Google: il guadagno di Google sta nel prezzo che l'inserzionista paga a Google ogniqualvolta un utente clicca su un messaggio pubblicitario; inoltre tali messaggi pubblicitari compaiono anche in tutte le altre piattaforme del motore di ricerca compreso Google Video. Dunque, Google Video poteva indicizzare i contenuti inseriti dagli utenti, li organizzava e li sfruttava a fini commerciali, ottenendo un profitto. In base a tali motivazioni, pur non accogliendo completamente quanto disposto dai pubblici ministeri[339], il giudice di primo grado non se ne discostava molto, in quanto sosteneva che il servizio offerto da Google Video sarebbe stato quello di un *content provider* ossia un gestore di contenuti con tutte ciò che ne derivava in termini di imputazione di responsabilità del trattamento dei dati sensibili, e non un *hosting* ossia un mero fornitore del servizio web[340]: così Google Italia si sarebbe presentato come vero e proprio centro propulsore della pubblicità, in Italia, di Google Inc., *"[..]la quale, mediante una politica molto aggressiva all'interno del mercato del video su web, avrebbe tentato di accaparrarsi una fetta sempre maggiore del mercato dei video amatoriali, permettendone il caricamento e l'utilizzo senza prestare particolare attenzione alle regole attinenti alla protezione dei dati personali."*[341]

Riassumendo quanto disposto sul Capo B da parte del Tribunale di Milano, il giudice di primo grado in generale delineava correttamente la responsabilità del provider e riconosceva l'assenza dell'obbligo generale di sorveglianza previsto dalla normativa sul commercio elettronico, ma, come scrive lo stesso magistrato *"non esiste nemmeno la 'sconfinata prateria di Internet' dove tutto è permesso e niente può essere vietato, pena la scomunica mondiale del popolo web"*: per tali ragioni, attraverso la "promozione" dell'*hosting provider* in *content provider* il giudice ravvisava un trattamento illecito dei dati sensibili ai sensi del *Codice della privacy*[342] e condannava in primo grado a 6 mesi di reclusione i responsabili di Google[343].

La sentenza di primo grado ebbe una grande ricaduta mediatica perché rappresentava uno dei

---

[339] I PM avevano sostenuto che nel caso di specie Google si fosse comportato come *host* attivo per l'attività svolta; il giudice di primo grado invece lo qualificava quale c*ontent provider*.

[340] Cfr. M. De Cata, *La responsabilità civile dell'Internet service provider*, Milano, 2010, pp. 70-71, l'autore definisce l'*host provider* quale "fornitore di ospitalità" che mette a disposizione sul suo server porzioni di disco rigido per l'apertura e la gestione di un sito web; invece il *content provider* cd. "fornitore di ospitalità" fornisce appunto contenuti ed ha un grado di coinvolgimento e dunque di responsabilità maggiore, essendo egli stesso il fornitore delle informazioni immesse in rete. Per un'analisi maggiormente dettagliata sulle diverse figure di *provider* si rinvia al primo paragrafo del presente capitolo.

[341] Cfr. ancora S. Mariani, *op. cit.*.

[342] Sulla "promozione" dell'*hosting* in *content provider* si veda M. Cammarata, *Google-Vivi Down, una sentenza da cancellare*, 19 Aprile 2010, in *www.interlex.it/675/google2.htm.*

[343] Cfr. F. G. Catullo, *Responsabilità penale dell'internet service provider: la sentenza Google ViviDown,* in G. Cassano, G. Scorza, G. Vaciago (a cura di), *op. cit.*, p. 614 in cui l'autore sottolinea come il giudice di primo grado cada in contraddizione in quanto pur convenendo che l' assenza di un obbligo di sorveglianza non possa designare un ambito di competenza per Google relativamente al reato di diffamazione, sostenga poi come tale obbligo sia idoneo a vincolare l'ISP in un ambito di responsabilità.

primi casi di un processo penale a livello internazionale per la pubblicazione di contenuti sul *web* che vedeva come imputati i responsabili di un *provider* della rete. Nella decisione adottata dal giudice venivano in rilievo le tradizionali preoccupazioni nei confronti del mondo *online* e della qualificazione agli ISP come Google quali *"sceriffi della rete"*[344]; tale aspetto era rinvenibile nella parte conclusiva della sentenza, in cui il giudice, invitava il legislatore ad intervenire *"[…] in attesa di una buona legge che costruisca una ipotesi di responsabilità penale per il mondo dei siti web (magari colposa)"*, sottolineando però *"[…]che aprire le cateratte della libertà assoluta e senza controllo non costituisce un buon esercizio del principio di responsabilità e di correttezza, che sempre dovrebbe presiedere le attività umane."* Su tali aspetti, la sentenza di primo grado subì molte critiche da parte della dottrina[345] fino a giungere alla decisione del secondo grado del giudizio che riformò la decisione.

2.3 La decisione della Corte di Appello: l'assoluzione "perché il fatto non sussiste"

Investita della questione da parte della Pubblica Accusa e degli imputati, la Corte di Appello di Milano[346], in data 21 dicembre 2012, riformò la sentenza di condanna emessa dal Tribunale di Milano che assolse i *manager* di Google per il reato di illecito trattamento dei dati ai sensi dell'art.167 del *Codice* e, riprendendo la citata formula shakespeariana adottata dal giudice di primo grado, definì come la vicenda in esame, al contrario, fosse molto complessa perché attinente al *"governo di internet"*.

Non soffermando ulteriormente l'attenzione su quanto dispose il giudice di secondo grado sulla questione della competenza di giurisdizione e su quella di diffamazione rinvenendo a considerazioni analoghe al giudice di primo grado[347], è opportuno segnalare che le argomentazioni più innovative, che poi furono quelle che riformarono la sentenza di primo grado, riguardavano proprio la condanna per il trattamento illecito dei dati personali sensibili e l'affermazione dell'insussistenza del fatto. In particolare, le motivazioni del giudice d'appello si

[344] Sul punto si rimanda a M. Cammarata, *Sentenza Google. La Rete è davvero in pericolo?,* in *www.mcreporter.info/sistema/google.htm*, 25 febbraio 2010.

[345] Per le critiche nei confronti della sentenza di primo grado cfr. L. Beduschi, *Caso Google: libertà di espressione in internet e tutela penale dell'onore e della riservatezza,* in *Il Corriere del Merito*, 2010, p.967; R. Lotierzo, *Il caso Google-Vividown quale emblema del difficile rapporto degli internet service provides con il codice della privacy,* in Cassazione Penale, 2010, p.1288 e ss.

[346] Corte d'Appello di Milano, I sezione penale,sentenza n. 8611/12, 21 dicembre 2012.

[347] Il giudice di secondo grado confermava la competenza di giurisdizione del giudice italiano e in particolare a Milano, in quanto almeno una *parte* dei fatti sarebbe accaduta in Italia, riprendendo quanto disposto dal giudice di primo grado. Anche per quanto concerneva il reato di diffamazione aggravata riprendeva *per relationem* le motivazioni del giudice di primo grado.

snodavano in tre parti:

- il superamento del reato previsto all'art. 167 del *Codice*;
- la critica dell'impostazione dell'accusa che aveva previsto un obbligo in capo al *provider* di impedimento del trattamento illecito di dati commesso dagli *uploaders*;
- la ricostruzione dei rapporti tra la disciplina sul commercio elettronico e quella della *privacy* in base al ruolo assunto dall'ISP.[348]

In primo luogo, i giudici sono intervenuti sulla questione del cd. *alert o avviso* che aveva rappresentato uno dei punti chiave della sentenza del giudice di primo grado ma che aveva anche mostrato debolezza del ragionamento effettuato dal giudice di primo istanza. In primo grado, si era infatti detto che Google avrebbe dovuto avvertire in modo chiaro, esplicito e puntuale gli studenti che caricavano il video contenente dati sensibili del soggetto terzo, della necessità di acquisire il consenso preventivo, oltre che scritto in quel caso, e delle relative responsabilità penali a carico degli stessi che sarebbero derivate dalla mancata acquisizione di detto consenso. Al contrario, la Corte di Appello sostenne come tale aspetto non avesse una copertura nel Codice, in particolare all'art. 13 relativo all'obbligo di informativa e dunque non avrebbe potuto comportare una violazione del Codice, come invece era stato precedentemente sostenuto. La Corte infatti sottolineava come la previsione di tale condotta illecita sarebbe stata possibile soltanto attraverso una mutazione del fatto tipico del reato sostenendo che *"[…] la norma di cui all'art. 167 […] richiede esplicitamente che l'autore del reato abbia agito non rispettando le disposizioni indicate. E nessuna di queste disposizioni impone all'internet service provider di rendere edotto l'utente circa l'esistenza ed i contenuti della legge della privacy".* Dunque, il reato in forza del quale erano stati condannati gli imputati ai sensi dell'art. 167 del Codice non faceva alcun riferimento all'art. 13[349] per cui, *"data questa premessa non pare possibile non cogliere l'incongruenza operata dal giudice di primo grado".*

In secondo luogo poi, il giudice escludeva qualsiasi tipo di obbligo preventivo da parte del *provider* sui contenuti immessi in rete, visto l'enorme flusso delle informazioni sul *web*: soltanto attraverso un sistema di filtraggio preventivo sarebbe potuto effettuarsi tale controllo, non applicabile per il divieto posto dalla normativa. Inoltre, continuava la Corte, che anche laddove fosse stato legislativamente previsto tale obbligo in capo all'ISP, tale filtro sarebbe stato difficilmente attivabile data la complessità tecnica di un controllo automatico e avrebbe anche *"alterato la funzionalità della rete".* Sul punto, alcuni hanno anche sottolineato come la

[348] Cfr. A. Ingrassia, *La decisione d'Appello nel caso Google vs Vivi Down: assolti i manager, ripensato il ruolo del provider in rete,* in *Il Corriere del Merito,* in *www.docplayer.it/1202670-La-decisione-d-appello-nel-caso-google-vs-vivi-down-assolti-i-manager-ripensato-il-ruolo-del-provider-in-rete.html,* 2013.

[349] Ancora A. Ingrassia, *ibidem*, sottolinea come l'omessa o inidonea informativa è sanzionata dall'art. 161 del *Codice* che prevede solo una sanzione amministrativa nel caso di violazione.

Corte aveva voluto far emergere le conseguenze da un punto di vista dei diritti garantiti in Costituzione: tale potere di verifica avrebbe infatti potuto collidere con le manifestazioni di libertà del pensiero.[350] Dunque, la sentenza del giudice di secondo grado metteva in rilievo come l'evoluzione della rete pur avendo superato la figura del "semplice" prestatore di servizio del tutto estraneo alle informazioni immesse[351] e, accordando sulla qualifica data dall'accusa a Google di *host* attivo, non poteva però applicarsi da parte dell'ISP un monitoraggio preventivo, qualunque fosse stato il suo livello di attivismo. La sentenza in esame infatti rappresentò un importante tassello nella ricostruzione della disciplina del cyberspazio e nell'individuazione del ruolo dell'ISP in rete[352].

Infine, la terza argomentazione riguardava la ricostruzione dei rapporti tra la disciplina del commercio elettronico e quella della *privacy.* In particolare, la Corte d'appello partiva dalla distinzione tra la figura dell' *host provider* e *uploader,* e tra quest'ultimo e i soggetti terzi i cui dati erano trattati nel video e, riprendeva quanto sostenuto dai difensori di Google, in particolare dall'avv. Carlo Blengino, secondo cui *"[…] trattare un video non può significare trattare il singolo dato contenuto, conferendo ad esso finalità autonome e concorrenti con quelle perseguite da chi quel video realizzava*". Dunque il giudice di secondo grado non riteneva Google come il titolare del trattamento, identificabile invece con chi aveva caricato il video, e che, in relazione alle immagini lesive della dignità del ragazzo, quest'ultima era stata *"[…] calata, per volontà dello stesso controller, in un contesto in cui emergeva, […], la sua disabilità"* e Google non poteva essere qualificabile neanche come responsabile del trattamento. Dunque, secondo il decidente, Google Video non era titolare dei dati contenuti nel video in questione e quindi il rapporto tra i soggetti di cui erano trattati i dati nei contenuti caricati dagli *uploaders* e il *provider* era disciplinato dalla normativa sul commercio elettronico: nel caso di specie, Google Video non doveva verificare il rispetto della normativa in tema di trattamento dei dati dagli *uploaders ex* art. 17 del decreto in materia di commercio elettronico né era responsabile per gli illeciti commessi da questi ultimi, salvo il caso in cui ne avesse avuto diretta conoscenza ai sensi dell'art. 16 dello stesso decreto. Quindi viene a disciplinarsi un duplice rapporto: rispettivamente tra *host* e *uploader* definito dal *Codice della privacy* in quanto il primo risulta il responsabile del trattamento dei dati del secondo e, quello tra l'*host* e soggetti terzi i cui dati sono trattati dagli *uploaders* nei contenuti condivisi, disciplinato dal decreto legislativo n. 70 del 2003[353]. Oltre alla carenza dell'elemento oggettivo del reato che era stato

[350] Cfr. O. Pollicino, *Google versus Vividown atto II: ecco le motivazioni,* in *www.diritto24.ilsole24ore.com/avvocatoAffari/mercatiImpresa/2013/02/google-versus-vividown-atto-ii-ecco-le-motivazioni.php*, febbraio 2013.
[351] Il cd. principio di *neutralità in rete* previsto dalla normativa del commercio elettronico.
[352] Ancora A. Ingrassia, *op. cit.*
[353] A. Ingrassia, *ivi.*

contestato, la Corte aveva poi ravvisato l'insussistenza anche di quello soggettivo ossia, il *dolo specifico* in quanto non vi erano prove che i responsabili di Google fossero stati a conoscenza della presenza del video e del suo contenuto. Inoltre, non convinceva neanche la ricostruzione operata dal giudice di primo grado sul profitto di Google richiesto ai sensi dell'art. 167 del *Codice.* Infatti, per la Corte non sussisteva un vantaggio conseguito dagli imputati in conseguenza della condotta tenuta, tanto più nell'ambito di un servizio gratuito quale era Google Video e in assenza di *link* pubblicitari associati allo specifico video oggetto del procedimento.[354]

Dunque, la Corte d'Appello assolse gli imputati con formula piena *"perché il fatto non sussiste",* rettificando la decisione di primo grado e sostenendo che seppure la rete fosse la *"sconfinata prateria dove tutto è permesso"*, l'ISP non poteva esserne *"lo sceriffo"*, come invece, si è detto, avevano sottolineato le critiche seguite dalla prima decisione.

2.4 Il ricorso in Cassazione: la definitiva assoluzione di Google

La Procura Generale ricorse in Cassazione, impugnando la sentenza della Corte D'Appello, ritenendo che i manager di Google fossero responsabili penalmente ai sensi dell'art. 167 del *Codice della privacy,* in base a tre presupposti:

1. il trattamento illecito dei dati sensibili da parte del *provider,* che era in linea con la nozione di *trattamento* prevista dal decreto legislativo n.196/2003 di cui si è detto, e non si era curato del divieto posto dalla stessa normativa *ex* art. 26, comma 5 che prevede che *"I dati idonei a rivelare lo stato di salute non possono essere diffusi.";*

2. l'inapplicabilità delle previsioni agli art. 16 e 17 del decreto legislativo n.70/2003 alle questioni relative al trattamento dei dati personali in base all' art.1 della normativa sul commercio elettronico;[355]

3. l'attività di indicizzazione e catalogazione del materiale da parte di Google in qualità di *host attivo* traendo un profitto dalle inserzioni pubblicitarie: dunque, non potendo qualificarsi come attività di mera memorizzazione dei contenuti, non avrebbero potuto applicarsi le disposizioni all'art. 16 e 17 della normativa sul commercio elettronico.

La Suprema Corte di Cassazione rigettò tali doglianze espresse dalla Procura Generale della

[354] E. Apa, F. De Santis, *Caso Google/Vividown: pubblicate le motivazioni della sentenza della Corte di appello di Milano,* in *www.portolano.it/pcc_newsletters/caso-googlevividown-pubblicate-le-motivazioni-della-sentenza-della-corte-di-appello-di-milano/.*

[355] L'art. 1, comma 2, lettera b) prevede che non si applicano le disposizioni del decreto a *"le questioni relative al diritto alla riservatezza, con riguardo al trattamento dei dati personali nel settore delle telecomunicazioni di cui alla legge 31 dicembre 1996, n. 675 e al decreto legislativo 13 maggio 1998, n. 171 e successive modifiche e integrazioni".*

Repubblica, confermando con sentenza n. 5107/2014[356], l'assoluzione dei dirigenti di Google in relazione al trattamento illecito dei dati personali e chiudendo definitivamente la vicenda, ridisegnando i confini di responsabilità all' ISP.

Relativamente alla prima doglianza, la Corte riteneva che non poteva esserci da parte del *provider* alcun trattamento dei dati contenuti nel video caricato poiché vi è una differenziazione tra la nozione ampia di *trattamento* e quella di *titolare* di detto trattamento che è invece più circoscritta, entrambe previste dalla normativa sui dati personali. Quest'ultimo, continuava la Corte, era colui che poteva vantare di un potere decisionale nei confronti del trattamento e sul quale ricadono una serie di obblighi[357], che se non rispettati può essere ritenuto responsabile per violazione delle norme e conseguentemente subire le sanzioni penali e amministrative previste agli articoli 161 e 167 del *Codice*. Dunque, Google e specificamente Google Video, in qualità di *host provider* e in una posizione di estraneità dei contenuti pubblicati, non poteva incorrere in tali violazioni in quanto, come prevedeva la normativa sul commercio elettronico, godeva di limitazioni di responsabilità: in particolare, quello previsto all'art. 17 che esclude obblighi generalizzati di sorveglianza sui contenuti, salvo l'obbligo di fornire informazioni a richiesta delle autorità competenti e quello all'art.16 che esclude la responsabilità degli ISP per le condotte illecite tenute dagli utenti prevedendo delle eccezioni[358]. Quindi, Nonostante vi fosse stato un trattamento illecito dei dati personali "rafforzato" dal fatto che questi fossero stati anche sensibili, non potendo essere diffusi neanche con il consenso del soggetto, tale illecito poteva essere ascrivibile solo agli *uploader* , considerando che *l'host* non appena era venuto a conoscenza del contenuto del video, aveva tempestivamente avvisato l'autorità competente *ex* art. 16 del decreto n.70 del 2003, in quel caso ascrivibile alla Polizia Postale.

Rispetto poi alla seconda doglianza, la Suprema Corte argomentò che non vi fosse incomunicabilità tra le disposizioni relative al commercio elettronico e quelle sulla riservatezza, come invece aveva sostenuto il ricorrente facendo leva sull'art. 1 del decreto legislativo n.70 del 2003. Riferendosi proprio a detta disposizione, la Corte la interpretava in modo da rimarcare come la tutela dei dati personali sia disciplinata da un *corpus* separato, quello del *Codice*, che rimane applicabile anche con l'entrata in vigore della normativa sul commercio elettronico: vi

[356] Cassazione penale, III Sezione , 17 dicembre 2013, (dep. 3 febbraio 2014), n. 5107.

[357] La Procura Generale, ritenendo al contrario Google il titolare del trattamento dei dati ai sensi dell'art.4 del *Codice*, aveva considerato violati gli obblighi relativi a tale figura: in particolare, quelli previsti agli articoli 13, 17, 23 e 26 del *Codice della privacy.*

[358] L' art. 16, comma 1 del decreto legislativo n. 70 del 2003 prevede l'irresponsabilità dell' *host* per le condotte tenute dagli utenti soltanto se *"non sia effettivamente a conoscenza del fatto che l'attività o l'informazione è illecita e, per quanto attiene ad azioni risarcitorie, non sia al corrente di fatti o di circostanze che rendono manifesta l'illiceità dell'attività o dell'informazione;*
non appena a conoscenza di tali fatti, su comunicazione delle autorità competenti, agisca immediatamente per rimuovere le informazioni o per disabilitarne l'accesso." Tale ultima circostanza è quella che si verificò nella vicenda in esame, in quanto Google Video aveva rimosso il Video dopo la segnalazione effettuata dalla Polizia Postale.

era infatti un'armonia tra le due discipline *"perfettamente riscontrabile nel caso della determinazione dell'ambito di responsabilità penale dell'Internet host provider relativamente ai dati sensibili caricati dagli utenti sulla sua piattaforma"*. Così la suddetta definizione di *titolare* del trattamento dotato di poteri decisionali in base alle finalità, alle modalità e agli strumenti del trattamento, risulta compatibile con le disposizioni limitative di responsabilità previste per gli ISP[359]. Impostazione in linea anche con alcune pronunce della Corte di Giustizia dell'Unione relative alle esenzioni di responsabilità per i prestatori di servizi[360].

L'ultima argomentazione della Corte di Cassazione riguardava il superamento della qualificazione della natura di *host attivo* di Google Video, che escluderebbe l'applicabilità delle limitazioni di responsabilità di cui agli artt. 16 e 17 del decreto legislativo n. 70/2003 di cui si è già trattato: veniva ancora una volta evidenziato come Google avesse semplicemente fornito agli utenti una piattaforma per il caricamento dei contenuti senza alcun altro contributo. La Corte infatti sostenne che l'ISP fosse un *host* seppure attivo ma non un *content provider* che, invece, fornisce contenuti e risponde per eventuali illeciti, sottolineato anche dal Codice di autoregolamentazione dell'AIIP (Associazione Italiana Internet Provider)[361]: dunque, soltanto se l'ISP fosse stato un *content provider* potevano dirsi inapplicabili le disposizioni relative agli esoneri di responsabilità di cui all'art. 16, previsione esclusa dalla Corte. La Corte poi non riteneva doversi soffermare sulle considerazioni inerenti alla sussistenza del dolo specifico nella condotta dei *manager* di Google per poter avere un profitto. Sostenendo infatti che la vocazione commerciale di Google non si potesse provare riteneva doversi escludere la possibilità che il prestatore di servizio avesse conseguito un profitto economico derivante dalla permanenza del video in rete per due mesi. Infatti, le indagini processuali avevano dimostrato come vi fosse la totale assenza di *link* pubblicitari associati al filmato oggetto del video.

Le argomentazioni della Corte di Cassazione, riassumibili nei tre punti suddetti e qualificandoli quali "principi" relativi alle responsabilità degli ISP[362], non solo misero un punto fermo al caso in esame, ma furono fondamentali per demarcare il confine tra la libertà di espressione,

---

[359] Ci si riferisce sempre a quelle previste agli articoli 16 e 17 del decreto legislativo n. 70 del 2003.

[360] Cfr. Corte di Giustizia dell'Unione Europea, sentenza del 12 luglio 2011, causa C-324/09 (L'Oreal SA / eBay), pubblicata in Gazzetta Ufficiale dell'unione Europea del 10.09.2011. In tal caso, la Corte di espresse sull'esonero di responsabilità dell'ISP *"qualora non abbia svolto un ruolo attivo che gli permetta di avere conoscenza o controllo circa i dati memorizzati".*

[361] Tale distinzione è messa in rilievo da R. Salvi, *La Corte di Cassazione sul caso Google vs Vivi Down: l'host provider non governa il mare magnum della rete*, in Diritto civile e commerciale, in *www.diritto.it/docs/36069-la-corte-di-cassazione-sul-caso-google-vs-vivi-down-l-host-provider-non-governa-il-mare-magnum-della-rete?page=2*, 18 marzo 2014.

[362] R. Salvi, *op. cit.* definisce i tre principi esposti dalla Corte quali *":(i) non è possibile attribuire all'host provider un obbligo di impedire i reati commessi dagli utenti, mancando una norma che fondi l'obbligo giuridico; (ii) le attività compiute dall'host provider sui materiali caricati dagli utenti (che non importino un intervento sul contenuto degli stessi o la loro conoscenza) non fanno venir meno le limitazioni di responsabilità previste dagli artt. 16 e 17 D.Lgs. 70/2003; (iii) solo dal momento della conoscenza dell'illiceità dei contenuti pubblicati dagli utenti può ipotizzarsi una responsabilità del provider per illecito trattamento dei dati realizzata dagli uploaders."*

governabilità della rete e tutela dei dati personali e sensibili. Come era stato evidenziato fin dai primi interventi sulla vicenda[363], infatti, vi è sempre di più la necessità che la società dell'informazione prenda sul serio la tutela dei dati considerando, come è stato mostrato, che le piattaforme presenti in rete, siano fondate su modelli di *business* in cui la conoscenza dei dati relativi alle persone sia finalizzata ad essere utilizzata a fini pubblicitari.

3. La configurazione dei dati personali in rete nella giurisprudenza della Corte di Giustizia

Il tema della tutela dei dati personali "comuni" e quelli sensibili sul *web* è oggetto delle questioni giurisdizionali non solo a livello nazionale, ma anche e soprattutto a livello europeo. Saranno adesso analizzati alcuni casi rilevanti in materia sui quali si è pronunciata negli ultimi anni la Corte di Giustizia dell'Unione europea, che pur non riguardando specificamente casi di trattamenti di dati dotati di particolare sensibilità, ma il tema più generale della tutela della riservatezza in rete, avranno un impatto anche in relazione ai primi dovendosi considerare una categoria speciale di dati "comuni". Particolarmente notevole è il primo caso che di seguito sarà trattato, in cui la Corte di Giustizia ha annullato la direttiva 2006/24/CE *sulla conservazione dei dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE* , finalizzata ad introdurre un regime derogatorio rispetto al trattamento dei dati personali[364] con conseguenze dirette negli ordinamenti degli Stati membri.

3.1 Il caso *Digital Rights Ireland*: la dichiarazione di invalidità della direttiva "Frattini"

Come è stato anticipato, la Corte di Giustizia dell'Unione europea con sentenza dell'8 aprile 2014[365], ha invalidato la direttiva 2006/24/CE sulla conservazione dei dati[366], in seguito a due

[363] G. Camera, O. Pollicino, *op.cit.*, p.156.
[364] Si fa riferimento alla sentenza *Digital Rights Ireland* di cui si dirà nel successivo paragrafo.
[365] Corte di Giustizia dell'Unione Europea, Grande Sezione, 8 aprile 2014, Cause riunite C-293/12 e C-594/12.
[366] Si fa riferimento alla Direttiva 2006/24/CE del Parlamento europeo e del Consiglio, del 15 marzo 2006, riguardante *la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE.*

rinvii pregiudiziali presentati sia dalla High Court irlandese sia dalla Verfassungsgerichtshof, la Suprema Corte Austriaca, in merito alla validità della direttiva rispetto alla protezione della vita privata e dei dati personali sanciti dalla Carta dei diritti fondamentali dell'Unione[367].

Senza soffermarsi sui singoli ricorsi pregiudiziali presentati dinanzi alla Corte[368], è sufficiente sottolineare che entrambe le Corti nazionali contestavano la direttiva nel suo complesso[369] ed in particolare le disposizioni previste agli art. 3, 4 e 6 della stessa: secondo queste infatti i fornitori dei servizi di comunicazioni elettroniche dovevano conservare i dati del traffico, di localizzazione o di identificazione dell'utente nonché poter misurare la durata delle comunicazioni[370]. Tali dati, conservati dai fornitori dei servizi per un periodo non inferiore a sei mesi e non superiori a due anni, dovevano essere disponibili alle autorità nazionali competenti per indagini, accertamenti e perseguimento di gravi reati, come definiti da ciascuno Stato membro nella rispettiva legislazione nazionale.

Innanzitutto, la Corte di Giustizia ritenne doveroso verificare se la conservazione dei dati così come previsti dalla direttiva avesse potuto rappresentare un'ingerenza nei diritti fondamentali in questione. Nonostante la direttiva non prevedesse obblighi di conservazione del contenuto delle comunicazioni utilizzate, la Corte nel dispositivo della sentenza diede risposta positiva in tal senso sostenendo anche che *"poco importa che le informazioni relative alla vita privata di cui trattasi abbiano o meno un carattere sensibile o che gli interessati abbiano o meno subito eventuali inconvenienti in seguito a tale ingerenza"*. Sottolineando come il problema della legittimità della conservazione dei dati sia precedente al trattamento degli stessi, la Corte collegava l'ambito di applicazione prima al rispetto della vita privata prevista all'art. 7 della Carta[371] e poi a quello della protezione dei dati personali all'art.8; anche la stessa previsione dell'ingerenza delle autorità nazionali competenti dei dati, rappresentava allo stesso modo una violazione dell'art. 7 citato. Dunque, le previsioni della direttiva incidevano secondo la Corte negativamente sul rispetto della vita privata in quanto *"la raccolta dei dati personali ha infatti*

[367] I parametri che si ritenevano violati nel caso di specie, erano gli art. 7 (Rispetto della vita privata e vita familiare), 8 (protezione dei dati di carattere personale) e 11 (Libertà di espressione e di informazione) della Carta.

[368] La Corte irlandese doveva risolvere una controversia tra la società *Digital Right Ireland* e alcuni enti facenti capo allo Stato (Ministero delle comunicazioni, la marina e le risorse naturali; Ministero per la giustizia, la parità e le riforme giuridiche; il Corpo di polizia irlandese; l'Avvocatura Generale) avente ad oggetto la legittimità delle disposizioni nazionali, attuative della direttiva in questione, sulla conservazione dei dati in materia di comunicazioni elettroniche. Anche la Suprema Corte Austriaca, doveva decidere su numerosi ricorsi che gli erano stati presentati al fine di ottenere l'annullamento delle relative norme nazionali sempre attuative della direttiva europea.

[369] La direttiva aveva lo scopo di armonizzare le normative interne degli Stati membri relativamente alla conservazione dei dati generati o trattati dai fornitori dei servizi di comunicazioni elettroniche.

[370] Secondo la direttiva, soltanto i contenuti delle comunicazioni elettroniche erano esclusi da detta disciplina.

[371] In tal senso la Corte di Giustizia aveva richiamato una precedente pronuncia della Corte EDU del 1987, *Lander Vs Svezia*, la quale aveva affermato come la raccolta e memorizzazione dei dati personali, senza il previo consenso del soggetto interessato, costituisce una ingerenza nel diritto al rispetto della vita privata. Tale richiamo dimostra anche il continuo contatto tra le due Corti di Lussemburgo e Strasburgo, particolarmente rilevante per il tema della protezione dei dati personali.

una portata vastissima, riguardando la totalità della popolazione degli Stati membri"[372]e, conseguentemente, anche sulla protezione dei propri dati.

Dopo tale considerazione, la Corte verificò se tale ingerenza rispettasse l'art. 52, paragrafo 1 della Carta dei diritti fondamentali dell'Unione Europea che accetta che limitazioni ai diritti fondamentali, previsti espressamente dalla legge, possano avvenire soltanto se vi sia il rispetto di tre parametri: il *contenuto essenziale* dei diritti in questione, una *finalità di interesse generale*, il *principio di proporzionalità*. Con riferimento al primo, precisava il fatto che non essendoci possibilità di conoscere il contenuto delle comunicazioni, allora il contenuto essenziale dei diritti venisse rispettato in quanto l'art. 7 della direttiva prevede il rispetto di alcuni principi generici[373]. La Corte affermava che anche il rispetto del secondo parametro, ossia quello della *finalità di interesse generale* fosse stato rispettato dalla direttiva perché coincidente con quello di garantire la sicurezza pubblica attraverso la lotta alla criminalità, anche se in contrasto con quanto disposto in una precedente sentenza[374]. Furono le argomentazioni sul rispetto o meno al terzo parametro con cui la Corte giunse al cuore della sua motivazione che segnò il punto decisivo nella dichiarazione di invalidità della direttiva in esame: l'analisi sul rispetto del *principio di proporzionalità*, ossia se l'ingerenza nei diritti suddetti fosse stata adeguata alla realizzazione degli obiettivi perseguiti e non fosse andata oltre a quanto strettamente necessario. Con riguardo al primo quesito, il giudice europeo diede risposta positiva sostenendo che la conservazione dei dati e il loro possibile utilizzo da parte delle autorità nazionali competenti fossero strumenti *idonei* a conseguire la lotta alla criminalità. Tuttavia, la Corte sostenne come la stessa lotta alla criminalità e al terrorismo, anche se obiettivi di interesse generale dovevano essere necessariamente bilanciati con altri opposti interessi, degni egualmente di tutela: nel caso di specie il rispetto della vita privata e della protezione dei propri dati. Richiamando ancora una volta la giurisprudenza della Corte EDU[375], la Corte sosteneva che potevano esservi deroghe o limitazioni a tali diritti soltanto se queste fossero strettamente necessarie, garanzie che dovevano essere ancora più forti, come nel caso in questione, quando in cui i dati fossero stati sottoposti ad un trattamento automatico e

[372] Così O. Prevosti, *Tutela della privacy come presupposto della libertà: due recenti sentenze della Corte di Giustizia dell'Unione Europea a difesa della riservatezza individuale*, in *www.osservatorioaic.it/tutela-della-privacy-come-presupposto-della-libert-due-recenti-sentenze-della-corte-di-giustizia-dell-unione-europea-a-difesa-della-riservatezza-individuale.html*, settembre 2014, p. 7.

[373] Si fa riferimento al principio di sicurezza e di protezione dei dati personali.

[374] Si tratta della sentenza CGUE, *Digital Rights Ireland Ltd Vs Irlanda*, in cui la Corte si era pronunciata in seguito ad un ricorso di annullamento *ex* art. 263 TFUE della direttiva in esame: in quel caso infatti negò che l'obiettivo principale della direttiva *data retention* potesse essere la repressione all criminalità, affermando che invece di riferisse al funzionamento del mercato interno.

[375] Corte EDU, *Liberty e altri Vs Regno Unito*, 2008: in quel caso la Corte di Strasburgo, aveva dichiarato la violazione dell'art. 8 della CEDU sostenendo che la disciplina nazionale in materia di intercettazioni via radio prevista dal Ministero britannico per legge non garantisse adeguata protezione agli individui dalle ingerenze dei pubblici poteri.

notevole e quindi vi fosse stato un rischio maggiore del loro utilizzo per scopi illegale. Dunque, la proporzionalità non era stata rispettata nel caso in questione poiché la direttiva riguardava tutte le tipologie di dati, tutti gli individui, non soltanto quelli aventi legami con la criminalità e tutti i mezzi di comunicazione elettronica (telefoni, cellulari, posta elettronica) senza alcun tipo di differenziazione[376]. Secondo la Corte, mancava anche un criterio oggettivo in base al quale le autorità nazionali avrebbero potuto, ai fini della prevenzione e accertamento di gravi reati, accedere a tali dati e utilizzarli: non vi erano le condizioni sostanziali e procedurali attraverso le quali le autorità avrebbero potuto accedere a tali dati. Ancora, con riferimento alla conservazione dei dati la direttiva aveva previsto un limite minimo di sei e massimo di 24 mesi, senza però dettare criteri oggettivi per la determinazione dell'uno o dell'altro caso per caso né ponendo una distinzione, come è stato accennato, tra i dati e gli individui coinvolti. Infine, la Corte si soffermava sul fatto che fosse in pericolo anche la sicurezza dei dati, non essendo state previste adeguate garanzie contro il pericolo di abuso[377].

Prima di giungere alle conclusioni, il giudice europeo, relativamente al rispetto della direttiva rispetto alla libertà di espressione prevista dall'art. 11 della direttiva, riprese un'affermazione dell'Avvocato Generale in cui esprimeva come il meccanismo del controllo potesse incidere *"sull'utilizzo, da parte degli abbonati o degli utenti registrati, dei mezzi di comunicazione cui fa riferimento la suddetta direttiva e, di conseguenza, sull'esercizio, da parte di questi ultimi, della loro libertà di espressione, garantita dall'articolo 11 della Carta"*[378]*:* sapere che vi sia un controllo sulle proprie informazioni, secondo la Corte, porterebbe ad una limitazione dell'uso dei mezzi di comunicazione da parte degli individui. Tale aspetto incide particolarmente sul tema oggetto del presente elaborato nel punto in cui gli individui, non sentendosi pienamente liberi di comunicare e di esprimere, limiterebbero la possibilità di costruire al meglio la propria personalità e il modo di partecipare nella società[379]. Dunque, pur non affrontando approfonditamente il tema, la Corte aveva evidenziato lo stretto legame che vi fosse tra libertà di pensiero e tutela della *privacy.*

In base a dette argomentazioni, la Corte dichiarava l'invalidità dell'intera disciplina della direttiva *data retention* per violazione dei limiti imposti dal principio di proporzionalità in

[376] Non prevedeva distinzioni neanche in base alle comunicazioni coperte dal segreto professionale o in base all'utilizzo dei dati per territori oppure, ancora, per il controllo di dati di individui legati ad ambienti criminali.

[377] Ancora O. Prevosti, *op. cit.*, p.12. L'autore sottolinea come l'art. 7 della direttiva consentiva ai fornitori dei servizi in esame di stabilire le misure tecniche ed organizzative, non consentendo la distruzione dei dati dopo il termine del periodo stabilito; inoltre non imponeva che i dati fossero conservati sul territorio europeo consentendo più facilmente la violazione dell'art. 8 della Carta di Nizza.

[378] Conclusioni dell'Avvocato Generale. In generale, l'Avvocato generale e la Corte di Giustizia pur giungendo alla stessa conclusione sull'incompatibilità della direttiva con le disposizioni della Carta di Nizza, avevano effettuato due percorsi argomentativi diversi: il primo ha ritenuto aveva ritenuto incompatibile la previsione dell'ingerenza nel godimento dei diritti fondamentali; la Corte, invece, aveva argomentato sul rispetto del parametro della proporzionalità.

[379] Tale aspetto è evidenziato da A. Baldassarre, *Globalizzazione contro democrazia*, Bari, 2002, p. 257.

riferimento agli articoli 7, 8 e 52, paragrafo 2 della Carta di Nizza, ritenendo eccessivamente sproporzionata la disciplina rispetto al diritto della riservatezza, e non l'illegittimità della raccolta in sé.

A conclusione dell'analisi della sentenza della Corte, pare opportuno soffermarsi su alcuni aspetti. In primo luogo, la dichiarazione di invalidità non giunse inattesa in quanto altre Corti costituzionali come il Tribunale costituzionale federale tedesco, la Corte Costituzionale rumena e la Corte Costituzionale della Repubblica Ceca, autonomamente, avevano censurato le normative interne attuative della direttiva a più riprese.[380] Non solo, anche la Commissione europea nel 2010 aveva espresso le sue perplessità sulla conformità della direttiva anche se ritenne come le previsioni della normativa fossero indispensabili per l'accertamento e la prevenzione di gravi reati[381]. In secondo luogo, la sentenza metteva in rilievo il citato collegamento con la giurisprudenza della Corte EDU da parte della Corte di Giustizia: tale ricorso sembrava collegabile a quella sorta di non autosufficienza della Carta dei diritti dell'Unione[382]. Infine, bisogna anche sottolineare la ricaduta della dichiarazione di invalidità a livello nazionale in particolare in Italia. La direttiva infatti era stata recepita nel nostro ordinamento con il decreto legislativo 30 maggio 2008 n.109 attraverso il quale erano state apportate modifiche al *Codice della privacy* e prevista la rispettiva disciplina all'art.132. In seguito alla dichiarazione di invalidità della direttiva, sono stati abrogati alcune disposizioni di tale articoli corrispondenti ai contenuti della direttiva[383].

3.2 Il caso *Google Spain:* la responsabilità del gestore del servizio *online* in materia di diritto all'oblio

Anche il secondo caso giurisprudenziale, pur non occupandosi specificamente di un trattamento illecito dei cd. dati sensibili, fu particolarmente rilevante perché oltre a riprendere la

[380] Si vedano sul punto A. Di Martino, *Il Bundesverfassungsgericht dichiara l'incostituzionalità della data retention e torna sul rapporto tra libertà e sicurezza*, in Giur. cost., 2010, p. 4071 ss. e v. M. Dicosola, *La data retention directive e il dialogo tra Corti costituzionali e Corte di Giustizia nel sistema multilivello europeo*, in *www.diritticomparati.it/2014/02/la-data-retention-directive-e-il-dialogo-tra-corti-costituzionali-e-corte-di-giustizia-nel-sistema-m.html*, 20 febbraio 2014.

[381] Si rinvia a Commissione europea, *Relazione della Commissione al Consiglio e al Parlamento Europeo. Valutazione dell'applicazione della direttiva sulla conservazione dei dati* , Bruxelles, 18 aprile 2011, in particolare pp. 34 ss..

[382] Si veda G. Repetto, *La Corte di giustizia dell'UE dichiara invalida la direttiva sulla Data Retention: verso la costituzionalizzazione del diritto alla privacy?*, in *www.academia.edu/8973672/La_Corte_di_giustizia_dell_UE_dichiara_invalida_la_direttiva_sulla_Data_Retention_verso_la_costituzionalizzazione_del_diritto_alla_privacy*, 24 giugno 2014.

[383] Per una disamina completa sulle conseguenze nell'ordinamento italiano si veda F. Vecchio, *L'ingloriosa fine della direttiva Data retention, la ritrovata vocazione costituzionale della Corte di Giustizia ed il destino dell'art. 132 del Codice della privacy*, in *www.diritticomparati.it/2014/06/lingloriosa-fine-della-direttiva-data-retention-la-ritrovata-vocazione-costituzionale-della-corte-di.html*, 12 giugno 2014.

problematica delle responsabilità degli *Internet service provider* in merito alle informazioni presenti sui server, diede importanti conclusioni in merito al cd. *diritto all'oblio*, che come si è visto nel primo capitolo, sarà espressamente disciplinato dal nuovo Regolamento europeo sulla *privacy*, vista la mancanza di una sua previsione nella direttiva 95/46/CE, dopo essere stato oggetto di numerose elaborazioni dottrinarie e giurisprudenziali.

Proprio tale pronuncia fu importante al fine di dettare delle regole applicabili qualora un soggetto interessato richiedesse, come nel caso di specie, un *diritto ad essere dimenticato*. Essendo considerato come una delle espressioni del diritto alla riservatezza[384], tale diritto assume una connotazione specifica con l'avvento del *web* dato che le informazioni personali, dunque anche quelle relative alla sfera più intima dell'individuo, una volta immesse e immagazzinate nel web, difficilmente possono "uscirvi" ed essere dimenticate: si parla dunque di un interesse di ogni persona a non restare indeterminatamente esposta ai danni *"[…]che arreca al suo onore e alla sua reputazione la reiterata pubblicazione di una notizia che in passato era stata legittimamente pubblicata[385]"*. Anticipando fin da subito che la carica innovativa della sentenza della Corte[386] fu quella di imporre l'obbligo di rimozione di notizie a carico dei gestori dei motori di ricerca[387], la vicenda ebbe inizio nel 2010 da una controversia nazionale spagnola che opponeva un cittadino spagnolo, il sig. Costeja Gonzalez e l'Agenzia spagnola per la protezione dei dati personali (AEPD) a Google Spain in quanto il primo aveva lamentato, in un reclamo all'Agenzia, la reperibilità di alcuni vecchi articoli che lo riguardavano tanto sulla versione *online* di un quotidiano spagnolo tanto sul motore di ricerca che rimandava a quelle stesse pagine[388]. L'interessato chiedeva all'Agenzia di ordinare al quotidiano spagnolo di cancellare le pagine in questione e a Google di occultare e non indicizzare i propri dati. Respingendo il reclamo diretto contro il quotidiano[389], l'Agenzia riteneva responsabile Google per il trattamento dei dati, il quale propose ricorso alla Corte

---

[384] Sulle nozioni di diritto all'oblio si veda P. Cendon*, Il diritto all'oblio*, in *Trattato breve dei nuovi danni*, Vol. 2, Cedam, 2011.; G. Buttarelli, *Banche dati e tutela della riservatezza*, Giuffré, 1997; L. De Grazie, *La libertà di stampa e il diritto all'oblio nei casi di diffusione di articoli attraverso internet*, in *www.rivistaaic.it/la-libert-di-stampa-e-il-diritto-all-oblio-nei-casi-di-diffusione-di-articoli-attraverso-internet-argomenti-comparativi.html*, 2013.

[385] Così R. Petti, *La protezione dei dati personali e il caso Google Spain*, 20 marzo 2015, in *www.dimt.it*.

[386] Corte di Giustizia dell'Unione europea, 13 maggio 2014, causa C-131/12 *Mario Costeja Gonzalese e AEPD Vs Google Spain e Google Inc.*

[387] La differenza con la sentenza definitiva della Cassazione del *caso Google Vs Vivi Down* è lampante dato che in quel caso la Suprema Corte aveva definito l'irresponsabilità del *provider* rispetto al video contenente informazioni sensibili.

[388] Gli articoli, pubblicati su *La Vanguardia*, riguardavano alcuni annunci di un'asta immobiliare connessa a un pignoramento subito dal soggetto interessato circa vent'anni prima ed erano stati pubblicati prima nella versione cartacea del quotidiano in questione e in seguito ricopiati nella versione *online*. Inoltre, digitando nella casella di ricerca di Google il nome e cognome del soggetto interessato, la ricerca rimandava ad una lista dei risultati alcuni *link* verso le pagine de *La Vanguardia*.

[389] Relativamente a tale aspetto, l'Agenzia per la protezione dei dati spagnola sosteneva legittima la pubblicazione degli articoli sul quotidiano essendo ordinata dal Ministero del Lavoro al fine di conferire la massima pubblicità alla vendita.

suprema spagnola che decise di promuovere rinvio pregiudiziale dinanzi alla Corte di Giustizia sulla corretta interpretazione e applicazione della direttiva 95/46/CE.

La prima questione sulla quale la Corte doveva pronunciarsi riguardava l'ambito di applicazione territoriale della direttiva e di conseguenza anche della normativa nazionale di recepimento ai sensi dell'art. 4 della direttiva[390]: la Corte si interrogava in particolare sulla nozione di *"*stabilimento" e di "ricorso a strumenti situati nel territorio di detto Stato membro" previsti dalla disposizione. Pur affermando che Google Search fosse gestito da Google Inc. che aveva sede negli Stati Uniti, l'attività promozionale avveniva direttamente da parte di Google Spain, essendo la vendita pubblicitaria il nucleo essenziale delle attività commerciale della società; per la Corte dunque era sufficiente conoscere il luogo di stabilimento di tale servizio, che avviene appunto in Spagna. Affermava poi che, essendo *"inscindibilmente connesse"* le attività del motore di ricerca e quelle di stabilimento, il trattamento dei dati personali veniva considerato nell'ambito delle attività dello stabilimento dato che Google Spain si occupava, nello Stato membro, della vendita di spazi pubblicitari che rendevano profitti grazie al servizio offerto alla casa madre. Riassumendo, la Corte dava un'interpretazione estensiva all'art. 4 della direttiva stabilendo che l'applicazione della stessa non esigeva che il trattamento della stessa fosse effettuato nel luogo di stabilimento dell'interessato ma nel contesto delle attività di quest'ultimo.

La seconda questione sollevata, invece, riguardava l'ambito di applicazione materiale della direttiva in esame, ossia se poteva ritenersi applicabile anche ai gestori dei motori di ricerca: se dunque questi potevano qualificarsi come soggetti preposti all'attività del *"trattamento dei dati personali"* previsto all'art. 2 della direttiva[391]. In particolare, il giudice di rinvio chiedeva se l'attività di indicizzazione e memorizzazione dei contenuti in rete da parte di Google potesse o

---

[390] L'art. 4 della direttiva 95/46/ce relativo al diritto nazionale applicabile prevedeva:" *1. Ciascuno Stato membro applica le disposizioni nazionali adottate per l'attuazione della presente direttiva al trattamento di dati personali:*
a) effettuato nel contesto delle attività di uno stabilimento del responsabile del trattamento nel territorio dello Stato membro; qualora uno stesso responsabile del trattamento sia stabilito nel territorio di più Stati membri, esso deve adottare le misure necessarie per assicurare l'osservanza, da parte di ciascuno di detti stabilimenti, degli obblighi stabiliti dal diritto nazionale applicabile;
b) il cui responsabile non è stabilito nel territorio dello Stato membro, ma in un luogo in cui si applica la sua legislazione nazionale, a norma del diritto internazionale pubblico;
c) il cui responsabile, non stabilito nel territorio della Comunità, ricorre, ai fini del trattamento di dati personali, a strumenti, automatizzati o non automatizzati, situati nel territorio di detto Stato membro, a meno che questi non siano utilizzati ai soli fini di transito nel territorio della Comunità europea.
2. Nella fattispecie di cui al paragrafo 1, lettera c), il responsabile del trattamento deve designare un rappresentante stabilito nel territorio di detto Stato membro, fatte salve le azioni che potrebbero essere promosse contro lo stesso responsabile del trattamento."

[391] In particolare alla lettera b), dell'art. 2 è presente la nozione di *"trattamento"* intesa quale *"qualsiasi operazione o insieme di operazioni compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali, come la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione o la modifica, l'estrazione, la consultazione, l'impiego, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, nonché il congelamento, la cancellazione o la distruzione*".

meno rientrare nella nozione di *"trattamento dei dati personali"* ai sensi della direttiva. La Corte dava risposta positiva sostenendo che l'attività di estrazione, registrazione e organizzazioni dei dati compiuta dal gestore, previste dall'art. 2 della direttiva, dovevano essere qualificate come trattamento anche qualora le informazioni fossero state pubblicate su altri media quale un quotidiano cartaceo, come nel caso di specie. Google Spain era ritenuto dal giudice europeo quale *titolare del trattamento* medesimo dato che vi era una separazione tra il trattamento compiuto dal gestore del motore di ricerca e quello del sito del quotidiano. Dunque, tale attività di indicizzazione poteva incidere sui diritti fondamentali e in particolare sulla tutela dei dati personali pertanto la Corte sosteneva come il *provider* dovesse rispettare le prescrizioni previste dalla direttiva in materia.[392] Anzi, riteneva responsabili tali soggetti anche quando i dati personali non fossero stati rimossi dalle pagine *web* pubblicate da terzi, come nel caso in questione, perché attraverso il servizio di ricerca offerto da tali soggetti si sarebbe potuto consentire l'accesso ad informazioni dettagliate sull'individuo oggetto di ricerca. Non potendo, tale servizio essere giustificato dal semplice interesse economico del gestore del trattamento, la Corte riteneva indispensabile bilanciare detto interesse con il diritto al rispetto della vita privata e della protezione dei proprio dati: quest'ultimo, comunque, non può considerarsi come sempre prevalente ma *"[…] occorre in ogni caso ricercare un giusto equilibrio che consideri la natura dell'informazione di cui trattasi e il suo carattere sensibile per la vita privata della persona suddetta, nonché l'interesse del pubblico a ricevere tale informazione, il quale può variare, in particolare, a seconda del ruolo che tale soggetto riveste nella vita pubblica."*[393]

Il giudice europeo poneva poi l'attenzione sulla questione del rispetto del diritto all'oblio. Infatti, il trascorrere del tempo può rendere non più adeguati o pertinenti o eccessivi i dati rispetto alle finalità per le quali sono stati trattati originariamente e in modo lecito: tale aspetto ha delle conseguenze dirette sul ruolo assunto dal motore di ricerca, il quale potrebbe avere l'obbligo di modificare o eliminare i dati su richiesta del soggetto interessato. La portata innovativa della sentenza stava proprio nella ricerca di un fondamento normativo del diritto all'oblio che la Corte ritenne presente negli articoli 12 e 14 della direttiva 95/46 CE: in particolare interpretando in senso ampio la previsione alla lettera b) dell'articolo 12 ricadente nella materia del diritto di accesso del soggetto interessato al trattamento, gli riconosceva anche *" […] la rettifica, la cancellazione o il congelamento dei dati il cui trattamento non è conforme alle disposizioni della presente direttiva, in particolare a causa del carattere incompleto o inesatto dei dati […]";* allo stesso modo anche il significato dell'art. 14 veniva ampliato rispetto al dettato normativo che riguardava il diritto di opposizione alla persona interessata,

[392] Sul punto R. Petti, *op. cit.*
[393] R. Petti, *ibidem.*

rinvenendo il fondamento del diritto in esame in base alla considerazione che nonostante l'esattezza di un dato, il trascorrere del tempo poteva non renderlo più corretto e dunque non più conforme alla normativa.

Attraverso tale sentenza, la Corte ha riconosciuto dunque un il diritto all'oblio e ha previsto un obbligo in capo a Google, titolare del trattamento, di evitare che certe pagine contenenti informazioni personali vengano indicizzate se non siano più giustificate da esigenze di attualità. Tuttavia, tale aspetto è stato ridotto dalla stessa Corte in quanto ha precisato che l'intervento del gestore possa avvenire soltanto dopo una preventiva disposizione da parte di un'autorità competente nazionale che nel caso in questione era rappresentata dall'AEPD: dunque, la semplice richiesta di rimozione o modifica rivolta dall'interessato all'ISP non può far sorgere nessun obbligo di attivazione senza il necessario controllo da parte dell'autorità sul bilanciamento tra l'interesse pubblico alla pubblicità della notizia e quello privato[394].

Tuttavia, l'aspetto di responsabilità delineato dalla Corte nei confronti dell'ISP lascia aperti alcuni dubbi, relativamente al fatto il trattamento dei dati in questione riguardi proprio quelli dotati di particolare sensibilità, previsti all'art. 8 della direttiva 95/46/CE concernente le *"categorie particolari di dati"*: se gli ISP fossero considerati come responsabili del trattamento di dati che rilevavano le opinioni politiche, religiose o i dati relativi allo stato di salute e alla vita sessuale, allora l'attività di questi diventerebbe automaticamente illegale ogniqualvolta le condizioni maggiormente stringenti previste per queste informazioni non verrebbero rispettate[395].

Al margine dell'analisi della sentenza in esame, bisogna mettere in rilievo come la decisione della Corte di Giustizia dell'Unione europea si discosti dall'orientamento della Corte di Cassazione italiana sicuramente dal caso *Google Vs Vividown,* in quanto anche se la vicenda in esame era diversa, che come si è avuto modo di analizzare, aveva definito un'irresponsabilità penale sui contenuti pubblicati sul suo server da utenti aventi ad oggetto dati sensibili; ma si differenzia anche da un altro intervento della Suprema Corte su un caso analogo in materia[396] in cui aveva affermato che la richiesta di modifica o cancellazione dei dati sarebbe dovuta essere rivolta al gestore del sito sorgente e non al gestore di ricerca, applicando quanto disposto dalla

[394] In tal senso si esprime M. Consonni, *Il diritto all'oblio per la Corte di Giustizia Europea nella recente decisione del caso Google Spain,* in *www.diritto24.ilsole24ore.com/art/avvocatoAffari/mercatiImpresa/2014-06-23/diritto-oblio-corte-giustizia-110906.php*, 23 giugno 2014.

[395] Di questa opinione fu l'Avvocato Generale del caso in esame nelle sue Conclusioni.

[396] Si fa riferimento alla sentenza della Corte di Cassazione del 5 aprile 2012 n. 5525.

normativa sul commercio elettronico[397]. La Corte dal canto ha ritenuto che proprio l'attività di indicizzazione da parte del motore di ricerca determinerebbe la sua responsabilità.

3.3 La sentenza *Schrems*: la ridefinizione della tutela dei dati personali in ambito transnazionale

La Corte di Giustizia è recentemente intervenuta nuovamente sul tema del rispetto del diritto alla protezione dei dati personali nell'era di internet da parte dei fornitori dei servizi con la sentenza *Schrems*[398] in cui ha invalidato una decisione del 2000 della Commissione europea che permetteva il trasferimento dei dati personali dall'Unione europea agli Stati Uniti, considerati avere quell'*adeguato* livello di tutela prevista dalla direttiva sulla *privacy* del 1995[399]. La decisione della Commissione a cui si fa riferimento è la 2000/520/CE[400] contenente il regime del cd. *Safe harbor* o approdo sicuro che era entrato in vigore 15 anni prima e aveva garantito il libero passaggio tra i *server* di Unione europea e USA ed era stato utilizzato dalle multinazionali americane del *web* quali Google, Apple, Facebook, Amazon[401]. La decisione dei giudici europei mira a tutelare maggiormente la *privacy* e in particolare i dati personali, compresi quelli sensibili, sul *web* in cui i rispettivi fornitori dei servizi sono mossi da logiche commerciali, piuttosto che al rispetto dei diritti[402]. La vicenda, che aveva luogo dopo lo scandalo PRISM[403], ha origine quando un cittadino austriaco, Maximilian Schrems, presentava una denuncia nei confronti dell'Autorità irlandese di controllo, ritenendo che alla luce del

[397] Ci si riferisce citato decreto legislativo n.70 del 2003 ed in particolare all'art. 18 che prevede un divieto di obbligo di sorveglianza per i contenuti trattati dal *provider.*

[398] Corte di giustizia dell'Unione europea (Grande Sezione), 6 ottobre 2015, causa C 362/14, *Maximillian Schrems Vs Data Protection Commissioner.*

[399] La previsione è contenuta nell'art. 25 della direttiva 95/46/CE che prevede al primo paragrafo che *" Gli Stati membri dispongono che il trasferimento verso un paese terzo di dati personali oggetto di un trattamento o destinati a essere oggetto di un trattamento dopo il trasferimento può aver luogo soltanto se il paese terzo di cui trattasi garantisce un livello di protezione adeguato, fatte salve le misure nazionali di attuazione delle altre disposizioni della presente direttiva".*

[400] *Decisione della Commissione, del 26 luglio 2000, a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio sull'adeguatezza della protezione offerta dai principi di approdo sicuro e dalle relative «Domande più frequenti» (FAQ) in materia di riservatezza pubblicate dal Dipartimento del commercio degli Stati Uniti.*

[401] Sono circa 4.500 le aziende statunitensi che avevano utilizzato tale regime, il cui scopo è quello di impedire la perdita accidentale o la rivelazione dei dati personali

[402] S. Rodotà, *Internet e privacy, c'è un giudice in Europa che frena gli Usa*, in *www.repubblica.it/tecnologia/2015/10/12/news/internet_e_privacy_c_e_un_giudice_in_europa_che_frena_gli_usa-124875972,* 12 ottobre 2015.

[403] Il PRISM è un programma gestito dall'intelligence statunitense attraverso il quale il governo USA ha chiesto ai colossi del web l'accesso alle email, numeri di telefono, foto e chat su mandato del *Foreign Intelligence Surveillance Act.* Si veda F. Pizzetti, *Datagate, Prism, caso Snowden: il mondo tra nuova grande guerra cibernetica e controllo globale*, in *www.federalismi.it/ApplOpenFilePDF.cfm?dpath=document%5Ceditoriale&dfile=EDITORIALE_26062013183526.pdf&content=Datagate,+Prism,+caso+Snowden:+il+mondo+tra+nuova+grande+guerra+cibernetica+e+controllo+globale&content_auth=Franco+Pizzetti,* 26 giugno 2013.

suddetto scandalo in merito alle attività di intelligence statunitensi, il diritto[404] e la prassi degli Stati Uniti non permettevano una tutela adeguata dei dati personali trasferiti verso tale paese: i dati forniti dall'interessato come tutti gli altri utenti di Facebook vengono trasferiti dalla filiale irlandese di Facebook sui *server* situati negli Stati Uniti. L'Autorità irlandese respingeva la denuncia ritenendosi vincolato al citato *Safe Harbor* in cui la Commissione aveva ritenuto *adeguato* il livello di protezione dei dati trasferiti nel territorio degli Stati Uniti. L'High Court irlandese rinviava la questione alla Corte di Giustizia al fine di conoscere se fosse effettivamente vincolato al meccanismo. Nell'ambito del rinvio sottolineava le preoccupazioni sull'effettivo rispetto della protezione dei dati previsto dall'accordo del 2000. In particolare, evidenziava come l'accesso eccessivo e indifferenziato dei dati da parte delle autorità statunitensi non rispettasse il principio di proporzionalità previste dalla normativa interna ed europea sulla *privacy:* l'Autorità riteneva, infatti, il meccanismo contrastante tanto ad alcuni principi costituzionali interni quali la dignità, l'autonomia personale, l'inviolabilità e la protezione della vita familiare, quanto agli articoli 7 e 8 della Carta dei diritti fondamentali. La Corte nel rispondere alle doglianze presentate dal giudice del rinvio esprime quanto sia inadeguato tutto il sistema previsto dalla decisione, non soltanto riguardo al meccanismo di trasferimento degli utenti europei negli Stati Uniti, ma anche le modalità di trattamento dei dati da parte dei colossi del *web*.

Il primo aspetto fortemente innovativo della sentenza sta nella considerazione che, nonostante l'esistenza di tale decisione della Commissione, le autorità nazionali, secondo la Corte, possano intervenire su eventuali ricorsi da parte degli interessati qualora questi considerino il Paese terzo non avere quel livello di protezione *adeguato*. Attraverso un'elencazione dei poteri di dette Autorità[405], la Corte evidenzia che in base a questi, le autorità possono esaminare in piena autonomia i ricorsi presentati nonostante l'esistenza della decisione, anche se soltanto la Corte può dichiararne la sua invalidità, come per qualsiasi atto dell'Unione europea. Nel caso di

[404] Come evidenzia G. Scorza, *Corte Ue:" Usa non proteggono privacy". Ecco cosa accade ora a Facebook, Google ed Apple,* in *www.ilfattoquotidiano.it/2015/10/06/corte-ue-usa-non-proteggono-privacy-ecco-cosa-accade-ora-facebook-google-ed-apple/2099520/*, 6 ottobre 2015, come nella decisione del 2000 la Commissione non considerò la circostanza che le leggi americane prevedevano la supervisione dei database dei giganti del web alle agenzie di intelligenze in nome della sicurezza nazionale.

[405] La Corte fa riferimento all'art. 28, paragrafo 3 della direttiva 95/46/CE secondo cui :*" Ogni autorità di controllo dispone in particolare:*

- di poteri investigativi, come il diritto di accesso ai dati oggetto di trattamento e di raccolta di qualsiasi informazione necessaria all'esercizio della sua funzione di controllo;

- di poteri effettivi d'intervento, come quello di formulare pareri prima dell'avvio di trattamenti, conformemente all'articolo 20, e di dar loro adeguata pubblicità o quello di ordinare il congelamento, la cancellazione o la distruzione dei dati, oppure di vietare a titolo provvisorio o definitivo un trattamento, ovvero quello di rivolgere un avvertimento o un monito al responsabile del trattamento o quello di adire i Parlamenti o altre istituzioni politiche nazionali;

- del potere di promuovere azioni giudiziarie in caso di violazione delle disposizioni nazionali di attuazione della presente direttiva ovvero di adire per dette violazioni le autorità giudiziarie.

È possibile un ricorso giurisdizionale avverso le decisioni dell'autorità di controllo recanti pregiudizio."

specie, quindi il *Commissioner* irlandese avrebbe dovuto sospendere il trasferimento dei dati da parte del *social network,* accertato il rischio di gravi abusi.

Successivamente la Corte interviene sul secondo punto, ossia la verifica della validità della decisione 2000/520/CE. Preliminarmente, la Corte rileva che il *Safe Harbor* è applicabile alle imprese statunitensi che lo sottoscrivono e non alle autorità pubbliche degli Stati Uniti; inoltre, le leggi USA nonché esigenze di sicurezza nazionale prevalgono sul regime dell'approdo sicuro qualora vi siano contrasti. La Corte sostiene che la Commissione, nel momento dell'adozione della decisione del 2000, non aveva verificato se vi fosse un livello di tutela dei dati personali equivalente a quello previsto nell'Unione. In realtà, le misure di tutela che la Commissione avrebbe dovuto verificare nell'ambito dell'approdo sicuro sembrano essere contemplate nell'ambito dei *Safe Harbor Privacy Principles* e soprattutto nelle FAQ allegate ad esso[406]. Inoltre, la Corte precisa che l'applicazione del *Safe Harbor* può subire delle limitazioni: in realtà, queste sono previste dalla direttiva sulla protezione dei dati personali all'art. 13 secondo cui gli Stati possono limitare i diritti previsti dalla direttiva per motivi di interesse nazionale quali la sicurezza dello Stato, la difesa e la pubblica sicurezza. Anche in questo caso, il ruolo di contemperamento tra i vari interessi deve sempre essere effettuato dalle autorità nazionali competenti.[407] Continua la Corte che, una normativa, come quella invalidata dalla sentenza, non è limitata allo stretto necessario se autorizza in modo generalizzato la conservazione di tutti i dati dei cittadini europei trasferiti verso gli Stati Uniti senza che vi siano differenziazioni, limitazioni o eccezioni in funzioni dell'obiettivo e senza circoscrivere il loro accesso da parte delle pubbliche autorità: tale tipo di normativa infatti è lesiva del contenuto essenziale del diritto al rispetto della vita privata. Ancora, riprendendosi quanto precedentemente disposto dalla sentenza sul caso *Google Spain*[408], la Corte sostiene che una normativa come quella in esame che non preveda la possibilità da parte degli utenti di usufruire di rimedi giuridici diretti ad accedere ai dati personali che lo riguardano o ad ottenere una rettifica o eliminazione, viola anche il diritto ad avere una giurisdizione effettiva, propria dello Stato di diritto. Infine, conclude, sostenendo che la Commissione, nell'adottare la decisione non aveva competenza di limitare i poteri di controllo delle Autorità nazionali qualora i cittadini dell'Unione avessero contestato la compatibilità della decisione con tutela dei diritti e libertà fondamentali. Per tali ragioni, la Corte invalida la decisione del 2000.

Occorre adesso fare alcune considerazioni conclusive sulla sentenza della Corte data

[406] Così P. Falletta, *La Corte di Giustizia, ancora una volta, contro le multinazionali del web (riflessioni su Corte di Giustizia UE (Grande sezione), 6 ottobre 2015, Schrems c. Data Protection Commissioner, C-362/14),* in *www.federalismi.it,* 23 dicembre 2015, p. 7.

[407] Così P. Falletta, *ibidem,* p.8.

[408] Si rinvia al paragrafo precedente per le posizioni della Corte di Giustizia sul caso *Google Spain*.

l'innovazione nel panorama della tutela dei dati in rete, se si considera che la previsione di una garanzia maggiore per la *privacy* ricade soprattutto su quelle informazioni che abbiamo definito come sensibili, a maggior ragione quando sia previsto il trasferimento verso Paesi posti al di fuori del territorio dell'Unione.

La prima di queste riguarda quello che è stato definito come il "tallone di Achille" della decisione della Corte di Giustizia[409] ossia quello di riconoscere alle Autorità garanti nazionali di ogni Stato membro il potere di definire singolarmente se il trasferimento dei dati dei propri cittadini sia o meno sicuro. Non solo questo potrebbe portare alla frammentazione del diritto europeo ma disincentiverebbe anche le società del *web* a stabilirsi in Europa. In tal senso, l'Autorità Garante per la protezione dei dati personali in Italia ha espresso parere positivo sulla sentenza della Corte ed in particolare sull'argomentazione di rafforzare i poteri ispettivi spettanti alle Autorità nazionali[410]. Inoltre, con una delibera del 22 ottobre 2015, il Garante ha disposto la caducazione della propria autorizzazione che consentiva l'accettazione del regime dell'approdo sicuro in Italia[411].

La seconda considerazione invece sottolinea come la sentenza invalidante della Corte di Giustizia non sia stata inattesa. Infatti, oltre ad essere stato oggetto di critiche dopo il citato scandalo PRISM e i continui attacchi alla sicurezza dati sul *web*, al *Safe Harbor* erano stati previsti dei miglioramenti da parte della stessa Commissione nel 2004[412], come quello di prevedere più controlli da parte delle autorità competenti, seguito da un intervento del Parlamento europeo del 2014 che chiedeva alla Commissione di sospendere l'accordo[413].

Il terzo aspetto, invece, vuole rimarcare la linea comune alle due sentenze analizzate nei paragrafi precedenti. Infatti, il giudice europeo in tutti e tre i casi giurisprudenziali, fa prevalere la *privacy* sulle logiche economiche proprie del *web*: alcuni parlano di una riaffermazione della *privacy*[414]. La tutela dei diritti fondamentali, come era stato anticipato, si impone all'interesse

---

[409] G. Scorza, *op. cit.*

[410] Si veda l'Intervista di Antonello Soro, Presidente del Garante della *privacy* del 21 ottobre 2015 *"Il Garante per la privacy abbia più funzioni ispettive"* consultabile su *www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/4345099.*

[411] Si fa riferimento alla delibera n. 564 del 22 ottobre 2015, pubblicata in Gazzetta Ufficiale il 20 novembre 2015. Per maggiori informazioni sulla delibera si rinvia a M. Iaselli, *Privacy: il Garante si adegua alla sentenza "Safe Harbor",* in *www.altalex.com/documents/news/2015/11/24/garante-privacy-caso-safe-harbor,* 3 dicembre 2015.

[412] Si fa riferimento al Documento di lavoro dei servizi della Commissione *sull'attuazione della decisione 520/2000/CE della Commissione sull'adeguatezza della protezione offerta dai principi di approdo sicuro e dalle relative "domande più frequenti" (FAQ) in materia di riservatezza* pubblicate dal Dipartimento del Commercio degli Stati Uniti (SEC (2004) 1323 del 20 ottobre 2004).

[413] Parlamento europeo, *Risoluzione sul programma di sorveglianza dell'Agenzia per la sicurezza nazionale degli Stati Uniti, sugli organi di sorveglianza in diversi Stati membri e sul loro impatto sui diritti fondamentali dei cittadini dell'UE, e sulla cooperazione transatlantica nel campo della giustizia e degli affari interni,* 12 marzo 2014.

[414] M. Bassini, O. Pollicino, *La Corte di giustizia demolisce il safe harbor e ridisegna i confini del diritto alla privacy in ambito transnazionale,* in *www.diritto24.ilsole24ore.com/art/avvocatoAffari/mercatiImpresa/2015-10-*

economico degli operatori del settore. Tale aspetto finalizzato al rispetto dei diritti, secondo alcuni, porta alla previsione di Carte volte alla costituzionalizzazione dei diritti sul *web*[415], come la Dichiarazione dei diritti di internet elaborata dalla Camera dei Deputati italiana.[416]

Infine, l'ultimo aspetto concerne l'intervento della Corte su tutto l'assetto previsto dalla decisione del 2000, sia per ragioni legislative sia per ragioni politiche in senso stretto[417]. Relativamente al primo aspetto, intende anticipare la sostituzione della direttiva del 1995 che come si è visto nel primo capitolo non sembra più adeguata alle sfide poste dal *web*. Infatti, ciò spiega come successivamente a tale decisione è stato sbloccato anche lo stallo tra le istituzioni europee che non permettevano un accordo sul pacchetto di nuovo regole della *privacy* delineato dal nuovo Regolamento europeo in materia di cui si è parlato. Rispetto, invece, al secondo, la Corte si è posta lo scopo di "aiutare" la Commissione in sede di nuovi accordi con gli Stati Uniti al fine di rendere più sicuri i trasferimenti dei dati dei cittadini europei dall'Europa agli Usa, visti i dubbi sollevati tanto dalla stessa Commissione quanto dal Parlamento europeo.

07/la-corte-giustizia-demolisce-safe-harbor-e-ridisegna-confini-diritto-privacy-ambito-transnazionale-153618.php, 7 ottobre 2015.

[415] S. Rodotà, *op. cit.*

[416] Il Documento è stato elaborato *dalla Commissione per i diritti e i doveri relativi ad Internet* a seguito della consultazione pubblica, delle audizioni svolte e della riunione della stessa Commissione del 14 luglio 2015. Il testo è consultabile su *www.camera.it*. Cfr. M. Pratellesi, *Ecco la Carta dei nostri diritti nell'era di internet,* in *www.espresso.repubblica.it/attualita/2015/07/28/news/ecco-la-carta-dei-nostri-diritti-nell-era-di-intenet-1.222836*, 28 luglio 2015; G. Scorza, *Carta di Internet, "l'accesso alla rete è un diritto fondamentale della persona",* in *www.ilfattoquotidiano.it/2015/07/28/carta-di-internet-il-web-non-e-far-west-ma-luogo-di-garanzia-dei-diritti-fondamentali/1912655/,* 28 luglio 2015.

[417] Si veda sul punto P. Falletta, *op. cit.*, pp. 10-11.

Conclusioni

Il riconoscimento di un diritto alla protezione dei dati personali accanto ad un tradizionale diritto alla riservatezza consente di ritenere come sia *"nata una nuova concezione integrale della persona, alla cui proiezione nel mondo corrisponde il diritto al pieno rispetto di un corpo che ormai è, al tempo stesso, "fisico" ed "elettronico"*[418]. Tuttavia, negli ultimi anni, esigenze o giustificazioni di sicurezza hanno indotto all'approvazione di normative che hanno esteso la capacità di controllo, raccolta, conservazione delle informazioni anche più intime degli individui; inoltre, sono state estese anche le capacità di indagine e di accesso delle autorità pubbliche a tali dati, in modo da non consentire più agli individui di avere un controllo sulle stesse. A difesa di una richiesta di maggiore protezione nei confronti dei propri dati, nelle pagine precedenti è stato mostrato come siano intervenute le stesse istituzioni europee, consapevoli della preoccupazione dei propri cittadini sul destino delle informazioni da loro immesse in rete. In tal senso, come si è visto, è stata fondamentale la sentenza invalidante il regime del *Safe Harbor*[419] ritenuto dalla Corte di Giustizia dell'Unione come inidoneo a garantire un livello di protezione dei dati dei cittadini europei almeno analogo a quello europeo, nonostante la Commissione europea nel 2000 avesse sostenuto il contrario. Tale decisione ha "sbloccato" anche lo stallo che da qualche anno non portava al raggiungimento di un accordo tra le istituzioni europee sulle nuove regole in materia di *privacy* che, se approvate in via definitiva nei prossimi mesi, sostituiranno la normativa vigente facente capo alla direttiva "madre" 95/46/CE e diventeranno immediatamente applicabili in tutto il territorio dell'Unione. Infatti, ancora una volta, la nuova normativa in materia di *privacy* sarà di provenienza europea. A maggior ragione, il nuovo pacchetto di regole sulla *privacy*, più attento a tutelare i dati personali dalle minacce presenti nel mondo dell'*online*, essendo contenuto principalmente in un Regolamento[420], sarà immediatamente esecutivo anche nel nostro Paese comportando una sostituzione dell'attuale *Codice.*

Dopo queste considerazioni, a conclusione del presente elaborato, occorre fare alcuni accenni alle prospettive che si aprono ai fini di una tutela più incisiva dei dati personali e in particolare di quelli sensibili che ricadono nella sfera più personale dell'individuo nel mondo *online.*

---

[418] Le parole sono tratte dal discorso di S. Rodotà, allora Presidente del Garante per la protezione dei dati personali durante la Conferenza internazionale sulla protezione dei dati che si tenne in Polonia nel settembre 2004, citata nel primo capitolo.

[419] Nella stessa direzione, le altre due pronunce della Corte di Giustizia analizzate nel terzo capitolo sono state rispettivamente sul caso *Digital Rights Ireland* e *Google Spain*, nelle quali il giudice ha fatto prevalere il diritto alla *privacy* rispetto ad altri interessi egualmente meritevoli di tutela.

[420] Il pacchetto di riforma, come si è visto nel primo capitolo, risulta composto da due strumenti legislativi: un Regolamento che si occuperà delle regole in materia di *privacy* applicabili tanto ai soggetti pubblici quanto a quelli privati; una direttiva che invece disciplinerà l'utilizzo dei dati personali nell'ambito della sicurezza e delle attività di polizia e di giustizia.

In primo luogo, come è stato anticipato in queste pagine, la prospettiva dell'adozione del nuovo Regolamento *privacy* fa ben sperare per un controllo maggiore degli utenti sulle proprie informazioni, tenendo conto, contrariamente alle discipline europee vigenti, della grande mole di dati riversata in rete e della necessità di una maggiore sicurezza dovuta all'utilizzo dei nuovi dispositivi mobili. Tale scopo è garantito, anzitutto, attraverso un ampliamento dei diritti dell'interessato mediante un accesso più facile alle proprie informazioni: dal nuovo diritto alla portabilità dei dati ad una definizione più chiara del diritto all'oblio. Ma anche attraverso il meccanismo rafforzato sia del consenso che dovrà essere sempre espresso in modo inequivocabile e dovrà essere specifico ai fini della profilazione, senza cui la stessa non potrà avvenire; sia dell'informativa all'interessato che dovrà essere più dettagliata e più efficace delle precedenti attraverso l'uso di moduli, schemi e disegni. Nella stessa ottica, anche gli obblighi posti a capo del titolare del trattamento diventano più stringenti considerando che ancor prima di procedere al trattamento dovrà progettare in un'ottica di privacy in base ai nuovi principi di *privacy by design* e *privacy by default* e prevedere all'inizio del trattamento una valutazione di impatto e verifica preliminare dello stesso. Occorrerà adesso attendere i prossimi mesi per conoscere il destino delle nuove regole in materia di *privacy* e capire che tipo di conseguenze comporterà all'interno degli Stati membri, considerando che adesso, attraverso l'utilizzo di uno strumento come quello del Regolamento, ci sarà sicuramente una maggiore uniformità di disciplina in tutto il territorio dell'Unione e dovranno necessariamente venire meno le differenze strutturali tra gli Stati.

In secondo luogo, occorre riprendere il discorso affrontato nel terzo capitolo sulla responsabilità dei fornitori della rete per i contenuti immessi dai loro utenti. Si è visto infatti, come, pur essendo prevista una normativa di riferimento in materia[421] e nonostante i ripetuti interventi della giurisprudenza europea ed italiana, non esiste tutt'ora un punto comune capace di identificare un'effettiva responsabilità del *provider,* qualora l'illecito non sia stato commesso dallo stesso. Infatti è immediatamente comprensibile come rispetto alla vita reale, sia più complicato attribuire un reato o una responsabilità ad una persona nel mondo *online* date le difficoltà di identificazione degli individui che commettono gli illeciti. In genere è possibile risalire all'autore di un illecito attraverso i cd. *file di log* del *provider,* ossia i documenti *online* nei quali vengono memorizzati il nome di accesso dell'utente, la password e le attività compiute in rete: in realtà colui che può essere rintracciato è il titolare del contratto di connessione alla rete. Proprio a causa della difficoltà di rintracciare l'autore dell'illecito, è stato valutato come il soggetto più facilmente reperibile sia proprio l'ISP che mette a disposizione il servizio

[421] Si fa riferimento tanto alla direttiva europea n. 31/2000/CE sul commercio elettronico quanto al decreto legislativo di recepimento della stessa del 9 aprile 2003 n. 70.

attraverso il quale viene commesso l'attività non autorizzata, come si è visto, ad esempio nella vicenda *Google Vs Vividown* nel caso di un trattamento illecito di dati sensibili. Dunque, in mancanza di una disciplina chiara in materia, si rende necessario di volta in volta bilanciare l'esigenza di individuare figure a cui imputare un eventuale reato, al fine di non lasciare non tutelate le pretese di risarcimento di chi ha subìto il danno, con quella di non gravare eccessivamente sui fornitori della rete e sulla loro attività per non impedire lo sviluppo e l'innovazione della rete.

L'ultima considerazione da fare riguarda lo scenario che si è aperto in seguito al *post- Safe Harbour.* Infatti, dopo la citata sentenza della Corte di Giustizia che nell'ottobre 2015 ha invalidato il regime dell'approdo sicuro, a seguito di mesi di trattative tra Unione europea e Stati Uniti, si è giunti ad un nuovo accordo sul trasferimento dei dati dei cittadini europei negli Stati Uniti, il cd. *Eu-Us Privacy Shield* ossia lo *scudo per la privacy Stati Uniti-Ue*[422], che probabilmente entrerà in vigore nei prossimi mesi. Il *Privacy Shield,* se approvato nel testo attuale, prevederà degli "impegni vincolanti" qualora le aziende vogliano trasferire i dati invece delle autocertificazioni previste dal precedente accordo. Inoltre l'accesso ai dati da parte degli apparati di sicurezza sarà soggetto a limitazioni chiare e a meccanismi di controllo al fine di evitare una sorveglianza indiscriminata e ogni anno lo *scudo* sarà ridiscusso in modo da monitorare l'andamento degli scambi di flusso dei dati. Infine, saranno previsti meccanismi di ricorso e di risoluzione delle dispute, per creare dei canali diretti con i cittadini che volessero sollevare casi di violazione della loro *privacy.* Occorrerà adesso capire se effettivamente il nuovo accordo prevederà garanzie effettive nei confronti dei dati dei cittadini europei trasferiti negli USA e dunque non soltanto destinate a rimanere sulla carta - anche perché proprio lo studente austriaco che sollevò il caso nell'ottobre 2015 dinanzi alla Corte di Giustizia, Max Schrems, ha immediatamente mostrato i suoi dubbi sulla nuova intesa, sostenendo che questa potrebbe essere dichiarata invalida dal giudice europeo, in quando per esservi un effettiva protezione dei cittadini europei, secondo lo studente, dovrebbe esservi soltanto la sua previsione da parte della legge[423].

[422] Dopo mesi di trattative la commissaria europea, Vera Jourova, insieme alla segretaria al commercio USA, Penny Pritzker, e al vicepresidente della Commissione, Andrus Ansip , sono giunti al nuovo accordo, il *Privacy Shield*. Per maggiori informazioni si rinvia a F. De Benedetti, *Addio a Safe harbor, ecco lo "Scudo per la privacy": sì all'accordo Usa-Ue sui dati personali,* in *www.repubblica.it/tecnologia/sicurezza/2016/02/02/news/safe_harbor_nuovo_accordo_usa-ue-132579711/,* 2 febbraio 2016.

[423] Si rinvia a F. Benedetti, *op. cit.*

Bibliografia

- AA. VV., *Il diritto alla riservatezza e la sua tutela penale*: *atti del terzo simposio di studi di diritto e procedura penali,* Giuffrè, Milano, 1970

- AA.VV., *L'informazione e i diritti della persona,* Jovene, Napoli, 1983

- AA. VV., *Codice della privacy. Commento al decreto legislativo 30 giugno 2003, n.196,* Giuffrè, Milano, 2004

- AA. VV., *Security Issues and Recommendations for Online Social Networks*, Giles Hogben, ENISA, in *www.enisa.europa.eu*, 14 novembre 2007

- G. Accardo, *L'Unione europea paladina della privacy*, in *www.internazionale.it*, 7 ottobre 2015

- R. Acciai (a cura di), *Il Diritto alla protezione dei dati personali. La disciplina sulla privacy alla luce del nuovo codice,* Maggioli editore, Rimini, 2004

- Agenzia dell'Unione europea per i Diritti Fondamentali, *Manuale sul diritto europeo in materia di protezione dei dati*, Belgio, 2014, in *www.fra.europa.eu/en*

- T.A. Auletta, *Riservatezza e tutela della personalità*, Giuffrè, Milano, 1978

- R. Adam, A. Tizzano, *Manuale di diritto dell' Unione europea,* Giappichelli, Torino, 2014

- E. Apa, F. De Santis, *Caso Google/Vividown: pubblicate le motivazioni della sentenza della Corte di appello di Milano*, in *www.portolano.it*

- E. Apa, O. Pollicino, *Modeling the liability of Internet Service Providres. Google VS Vividown. A Constitutional perspective,* Egea, Milano, 2013

- A. Baldassarre, *Globalizzazione contro democrazia*, Laterza, Bari, 2002

- V. Barabba, *Tra Fonti e Corti. Diritti e principi fondamentali in Europa: profili costituzionali e comparati degli sviluppi sovranazionali,* Cedam, Padova, 2008

- E. Barilà, C. Caputo, *Il trattamento dei dati sensibili da parte dei soggetti pubblici nel D.Lgs. 11 maggio* 1999, n.135, in *Tar*, 1999

- M. Bassini, O. Pollicino, *La Corte di giustizia demolisce il safe harbor e ridisegna i confini del diritto alla privacy in ambito transnazionale*,, in *www.diritto24.ilsole24ore.com*, 7 ottobre 2015

- E. Bassoli (a cura di), *Come difendersi dalla violazione dei dati su internet. Diritti e responsabilità.*, Maggioli editore, Rimini, 2012

- L. Beduschi, *Caso Google: libertà di espressione in internet e tutela penale dell'onore e della riservatezza*, in *Il Corriere del Merito*, 2010

- A. Bevere, A. Cerri, *Il diritto di informazione e i diritti della persona. Il conflitto della libertà di pensiero con l'onore, la riservatezza, l'identità personale*, Giuffrè, Milano, 2006

- P. Bilancia, M. D' Amico (a cura di), *La nuova Europa dopo il Trattato di Lisbona*, Giuffrè, Milano, 2009

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

- Frederik Z. Borgesius, *Behavioural sciences and the regulation of privacy on the internet*, A-L Sibony & A. Alemanno, University of Amsterdam, 23 ottobre 2014,

- G. Branca (a cura di), *Commentario della Costituzione*, Zanichelli, Bologna, 1975

- L. D. Brandeis, S. D. Warren, *The Right to Privacy*, in *Harvard Law Review*, 1890

- E. Brugiotti, *La privacy attraverso le "generazioni dei diritti". Dalla tutela della riservatezza alla protezione dei dati personali fino alla tutela del corpo elettronico*., in *www.dirittifondamentali.it*, 2013

- F. Buffa, G. Cassano, *Responsabilità del content provider e dell'host provider*, in *www.altalex.com*, 14 febbraio 2003 e aggiornato il 19 luglio 2005

- G. Buttarelli, *Banche dati e tutela della riservatezza*, Giuffrè, Milano, 1997

- G. Camera, O. Pollicino, *La legge è uguale anche sul web: Dietro le quinte del caso Google-Vividown*, Egea, Milano, 2010

- M. Cammarata, *Google-Vivi Down, una sentenza da cancellare*, in *www.interlex.it*, 19 aprile 2010

- M. Cammarata, *Sentenza Google. La Rete è davvero in pericolo?*, in *www.mcreporter.info*, 25 febbraio 2010

- V. Campanelli, *Infowar. La battaglia per il controllo e la libertà della rete*, Egea, Milano, 2013

- F. Cardarelli, S. Sica, V. Zeno-Zencovich (a cura di), *Il codice dei dati personali: temi e problemi*, Giuffrè, Milano, 2004

- P. Carey, *E-privacy and online data protection*, Butterworths, London, 2002

- P. Carey, *Data protection: a pratical guide to UK and EU law*, Oxford University Press, Oxford, 2004

- G. Cassano, G. Scorza, G. Vaciago (a cura di), *Diritto dell'internet. Manuale operativo. Casi, legislazione e giurisprudenza*, Cedam, Padova, 2013

- G. Cassano, *Google v. Vividown: responsabilità "assolute" e fine di Internet*, in *Il Diritto di famiglia e delle persone*, fasc. 4, 2010

- G. Cassano, *Riflessioni a margine di un convegno sul caso Google/Vivi Down*, in *Rivista penale*, fasc. 10, 2010

- G. Cellamare, *Tutela della vita privata e libera circolazione delle informazioni in una recente convenzione del Consiglio d'Europa*, in *Rivista di Diritto Internazionale*, 1982

- P. Cendon, *Trattato breve dei nuovi danni*, Volume 2, Cedam, Padova, 2011

- G.P. Cirillo, *La tutela della privacy nel sistema del nuovo codice sulla protezione dei dati personali. Tutela civile, amministrativa, penale*, Cedam, Padova, 2004

- G.P. Cirillo (a cura di), *Il Codice sulla protezione dei dati personali*, Giuffrè, Milano, 2004

- A. Cherchi, *Privacy, la Ue detta le regole per tutti*, in *www.ilsole24ore.com*, 25 gennaio 2016

- A. Clemente (a cura di), *Privacy*, Cedam, Padova, 1999

- B. Conforti, *Diritto internazionale,* VIII edizione, Editoriale scientifica, Napoli, 2010

- M. Consonni, *Il diritto all'oblio per la Corte di Giustizia Europea nella recente decisione del caso Google Spain*, in *www.diritto24.ilsole24ore.com*, 23 giugno 2014

- V. Cuffaro, V. Ricciuto (a cura di), *La disciplina del trattamento dei dati personali,* Torino, Giappichelli, 1997

- M. D'Alberti, *Autorità indipendenti (diritto amministrativo),* in *Enciclopedia Giuridica*, Roma, 1995

- F. De Benedetti, *Addio a Safe harbor, ecco lo "Scudo per la privacy": sì all'accordo Usa-Ue sui dati personali*, in *www.repubblica.it*, 2 febbraio 2016

- L. De Grazie, *La libertà di stampa e il diritto all'oblio nei casi di diffusione di articoli attraverso internet*, in *www.rivistaaic.it* , 2013

- M. Dicosola, *La data retention directive e il dialogo tra Corti costituzionali e Corte di Giustizia nel sistema multilivello europeo*, *Diritti comparati*, in *www.diritticomparati.it*, 20 febbraio 2014

- M. De Cata, *La responsabilità civile dell'Internet service provider*, Collana Univ. Milano-Bicocca-Dip. Dir. Per l'economia, Giuffrè, Milano, 2010

- A. De Cupis, *I diritti della personalità* in *Trattato di diritto civile e commerciale* già diretto da A. Cicu e F. Messineo e continuato da L.Mengoni, Giuffrè, Milano, 1956

- A. Di Martino, *Il Bundesverfassungsgericht dichiara l'incostituzionalità della data retention e torna sul rapporto tra libertà e sicurezza*, in *Giurisprudenza costituzionale,* 2010

- F. Fabris, *Il diritto alla privacy tra passato presente e futuro,* in *www.openstarts.units.it,* 15 dicembre 2009

- P. Falletta, *La Corte di Giustizia, ancora una volta, contro le multinazionali del web (riflessioni su Corte di Giustizia UE (Grande sezione), 6 ottobre 2015, Schrems c. Data Protection Commissioner, C-362/14),* in *www.federalismi.it,* 23 dicembre 2015

- P. Falletta, M. Mensi, *Il diritto del web. Casi e materiali,* Cedam, Padova, 2015

- H. Farrell, A. Newman, *This privacy activist has just won an enormous victory against U.S. surveillance. Here's how,* in *www.washingtonpost.com*, 6 ottobre 2015

- G.F. Ferrari (a cura di), *La tutela dei dati personali in Italia 15 anni dopo. Tempo di bilanci e bilanciamenti.*, Collana di Diritto dell'Economia a cura di P. Marchetti, Egea, Milano, 2013

- L. Ferrari Bravo, E. Moavero Milanesi, *Lezioni di Diritto Comunitario*, Editoriale scientifica, Napoli, 2002

- L. Ferrari Bravo, A. Rizzo, *Codice dell'Unione europea. Annotato con la giurisprudenza della Corte di Giustizia,* III edizione curata da A. Rizzo e F.M. Di Majo, Giuffrè, Milano, 2008

- G. Finocchiaro (a cura di), *Diritto all'anonimato: anonimato, norme e identità personale,* Cedam, Padova, 2008

- G. Finocchiaro, *Privacy e Protezione dei dati personali. Disciplina e strumenti operativi*, Zanichelli, Bologna, 2012

- L. Floridi, *Google, una sentenza che lascerà delusi*, in *www.lastampa.it,* 20 dicembre 2012

- M. Gambini, *Gli hosting providers tra doveri di diligenza professionale e assenza di un obbligo generale di sorveglianza sulle informazioni memorizzate*, in *www.costituzionalismo.it*, 27 dicembre 2011

- G. Gardini, *Le regole dell'informazione. Principi giuridici, strumenti, casi,* Bruno Mondadori, Milano, 2009

- C. Gattei, *Considerazioni sulla responsabilità dell'Internet provider*, in *www.interlex.it*, 23 novembre 1998

- A. Ghiribelli, *Il diritto alla privacy nella Costituzione italiana*, in *www.teutas.it*, 30 novembre 2007

- E. Giannanotonio, M.G. Losano, V. Zeno-Zencovich (a cura di), *La tutela dei dati personali. Commentario alla l.675/1996*, II edizione, Cedam, Padova, 1999

- A. Griffin, J. Merrill, *European court rules "Safe Harbour" treaty that saw Facebook hand over user data to US is invalid, after challenge by student*, in *www.independent.co.uk*, 6 ottobre 2015

- M. Iaselli, *I principi informatori del Codice della privacy fra teoria e pratica. La protezione dei dati personali alla luce del D. Lgs. 196/2003*, in *www.docplayer.it*, 2009

- M. Iaselli, *Privacy: il Garante si adegua alla sentenza "Safe Harbor"*, in *www.altalex.com*, 3 dicembre 2015

- M. Iaselli, *Accordo raggiunto sul Regolamento Europeo in materia di protezione dei dati personali*, in *www.altalex.com*, 23 dicembre 2015

- Riccardo Imperiali, Rosario Imperiali, *La tutela dei dati personali, Vademecum sulla privacy informatica*, collana Legale, pubblicato da *Il Sole 24 ore*, 1997

- A. Ingrassia, *Il ruolo dell' Isp nel ciberspazio: cittadino, controllore o tutore dell'ordine? Risposte attuali e scenari futuribili di una responsabilità penale dei provider nell'ordinamento italiano*, in *www.penalecontemporaneo.it*, 8 novembre 2012

- A. Ingrassia, *La decisione d'Appello nel caso Google vs Vivi Down: assolti i manager, ripensato il ruolo del provider in rete*, in *Il Corriere del Merito*, 2013

- A. Ingrassia, *La sentenza della Cassazione sul caso Google*, in *www.penalecontemporaneo.it*, 6 febbraio 2014

- R. Levine, *Behind the European Privacy Ruling That's Confounding Silicon Valley*, in *www.nytimes.com*, 9 ottobre 2015

- A. Loiodice, G. Santaniello, (a cura di), *La tutela della riservatezza*, Cedam, Padova, 2000

- R. Lotierzo, *Il caso Google-Vividown quale emblema del difficile rapporto degli internet service provides con il codice della privacy*, in *Cassazione Penale*, 2010

- A. Luongo, *Regole globali per disciplinare privacy ed internet*, in *www.ilsole24ore.com*, 16 aprile 2010

- A. Mantelero, *Il futuro regolamento EU sui dati personali e la valenza "politica" del caso Google: ricordare e dimenticare nella digital economy*, in *Diritto dell'Informazione e dell'informatica,* 2014

- S. Mariani, *Internet non è una "zona franca". Condannati i dirigenti di Google*, in *www.altalex.com*, 27 aprile 2010

- L. Miglietti, *Profili storico-comparativi del diritto alla privacy*, in *www.diritticomparati.it*, 4 dicembre 2014

- G. Modesti, *Commento breve al D.LGS.VO N. 196/2003. Codice in materia di protezione dei dati personali, Diritto civile e commerciale*, in *www.diritto.it*, 20 ottobre 2005

- J. Monducci, *Diritti della persona e trattamento dei dati particolari*, Giuffrè, Milano, 2003

- S. Niger, *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali*, Cedam, Padova, 2006

- U. Pagallo, *Il diritto nell'età dell'informazione. Il riposizionamento tecnologico degli ordinamenti giuridici tra complessità sociale, lotta per il potere e tutela dei diritti,* Giappichelli, Torino, 2014

- R. Pannetta (a cura di), *Libera circolazione dei dati e protezione dei dati personali*, Giuffrè, Milano, 2006

- R. Pardolesi (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, Volume I, Giuffrè, Milano, 2003

- R. Pardolesi (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, Volume II, Giuffrè, Milano, 2003

- R. Petti, *La protezione dei dati personali e il caso Google Spain*, in *www.dimt.it*, 20 marzo 2015

- A. Piersanti, V. Roidi (a cura di), *Giornalisti nella rete*, Ente dello Spettacolo, Roma, 1999

- L. Pineschi (a cura di*), La tutela internazionale dei diritti umani. Norme, garanzie e prassi*, Giuffrè, Milano, 2006

- F. Pizzetti, *Datagate, Prism, caso Snowden: il mondo tra nuova grande guerra cibernetica e controllo globale,* in *www.federalismi.it*, 26 giugno 2013

- O. Pollicino, *Google versus Vividown: gli argomenti "forti" della decisione di Appello,* in *www.diritto24.ilsole24ore.com*, 27 dicembre 2012

- O. Pollicino, *Google versus Vividown atto II: ecco le motivazioni,* in *www.diritto24.ilsole24ore.com*, 28 febbraio 2013

- O. Pollicino, *Tutela del pluralismo nell'era digitale: ruolo e responsabilità degli Internet service provider*, in *www.giurcost.org*, 2014

- M. Pratellesi, *Ecco la Carta dei nostri diritti nell'era di internet* in *www.espresso.repubblica.it*, 28 luglio 2015

- O. Prevosti, *Tutela della privacy come presupposto della libertà: due recenti sentenze della Corte di Giustizia dell'Unione Europea a difesa della riservatezza individuale,* in *www.osservatorioaic.it*, settembre 2014

- M. Prosperi, *Il diritto alla riservatezza nell'ordinamento costituzionale*, I parte, in *www.dirittosulweb.it*

- M. Prosperi, *Il diritto alla riservatezza nell'ordinamento costituzionale*, II parte, in *www.dirittosulweb.it*

- A.R. Popoli, *Social network e concreta protezione dei dati sensibili: luci ed ombre in una difficile convivenza*, in *Diritto dell'informazione e dell'informatica*, 2014

- G. Rasi*, Valutazioni del datore di lavoro sul dipendente e privacy: l'intervento del legislatore*, in *Il Sole-24Ore – Guida al lavoro*, 8 agosto 2003

- G. Repetto, *La Corte di giustizia dell'UE dichiara invalida la direttiva sulla Data Retention: verso la costituzionalizzazione del diritto alla privacy?*, in *www.academia.edu.data*, 24 giugno 2014

- F. Resta (a cura di), *La tutela dei dati personali nella società dell'informazione,* Giappichelli, Torino, 2009

- G. Resta, V. Zeno-Zencovich (a cura di), *Il diritto all'oblio su internet dopo la sentenza Google Spain*, Roma tre- press, 2015

- C. Rigotti, *Il nuovo testo unico sulla privacy*, Seac, Trento, 2003

- S. Rodotà, *Intervista su privacy e libertà*, a cura di Paolo Conti, Laterza, Roma-Bari, 2005

- S. Rodotà, *La privacy tra individuo e collettività*, Bologna, Il Mulino, in *Politica del diritto* n. 5 (settembre-ottobre) 1974

- S. Rodotà, *Tecnologie e diritti*, Il Mulino, Bologna, 1995

- S. Rodotà, *Apologia dei diritti*, La Stampa, 2 luglio 2002 in *www.ossimoro.it*

- S. Rodotà, *Tra i diritti fondamentali ed elasticità della normativa: il nuovo Codice sulla privacy*, in *Europa e Diritto Privato*, 2004

- S. Rodotà, *Internet e privacy, c'è un giudice in Europa che frena gli Usa*, in *www.repubblica.it*, 12 ottobre 2015

- S. Russo, A. Sciuto, *Habeas data e informatica*, Giuffrè, Milano, 2011

- R. Salvi, *La Corte di Cassazione sul caso Google vs Vivi Down: l'host provider non governa il mare magnum della rete*, in *Diritto civile e commerciale*, in *www.diritto.it*, 18 marzo 2014

- G. Santaniello, *La semplificazione delle regole nel codice della privacy*, in *www.interlex.it*, 3 marzo 2004

- G. Santaniello, *Le autorizzazioni per categoria relative al trattamento dei dati sensibili*, Relazione al Convegno Paradigma, Milano, 10-11 febbraio 1998.

- G. Santaniello (a cura di), *La protezione dei dati personali*, in *Trattato di diritto amministrativo* diretto da G. Santaniello, Volume trentaseiesimo, Cedam, Padova, 2005

- A. Scalisi, *Il diritto alla riservatezza*, Giuffrè, Milano, 2002

- A. Scirocco, *The Lisbon Treaty and the Protection of Personal Data in the European Union*, in *www.secure.edps.europa.eu*, 19 settembre 2008

- G. Scorza, G. Vaciago (a cura di), *Diritto dell'internet. Manuale operativo: casi, legislazione e giurisprudenza,* Cedam, Padova, 2010

- G. Scorza, *Carta di Internet, "l'accesso alla rete è un diritto fondamentale della persona",* in *www.ilfattoquotidiano.it*, 28 luglio 2015

- G. Scorza, *Corte Ue:" Usa non proteggono privacy". Ecco cosa accade ora a Facebook, Google ed Apple*, in *www.ilfattoquotidiano.it*, 6 ottobre 2015

- P. Schaar, *Data Retention: a landmark Court of Justice's ruling. (5) From now on, no more <<just in case>> retention of data*, in *www.free-group.eu*, 10 aprile 2014

- E. Stefanini, *Dati genetici e diritti fondamentali. Profili di diritto comparato ed europeo,* Cedam, Padova, 2008

- E. Varani, *Il "nuovo diritto "alla privacy. Dalla Carta di Nizza al "Codice in materia di protezione dei dati personali",* in *www.filodiritto.com*, 7 aprile 2012

- F. Vecchio, *L'ingloriosa fine della direttiva Data retention, la ritrovata vocazione costituzionale della Corte di Giustizia ed il destino dell'art. 132 del Codice della privacy*, in *www.diritticomparati.it*, 12 giugno 2014

- U. Villani, *Istituzioni di diritto dell'Unione europea*, Seconda edizione riveduta e aggiornata, Cacucci Editore, Bari, 2012

- P. Zanelli, *La Legge N. 675 del '96 : una strategia integrata di protezione per la privacy*, in *Contratto e Impresa*, 1997

- C. Zanghi, *La mancata adesione dell'Unione Europea alla CEDU nel parere negativo della Corte di giustizia,* in *www.rivistaoidu.net,* marzo 2015

- V. Zeno- Zencovich, *I diritti della personalità dopo la legge sulla tutela dei dati personali*, in *Studium Iuris*, 1997

- V. Zeno- Zencovich, *Una lettura comparatistica della l. n. 675/96 sul trattamento dei dati personali*, in *Rivista trimestrale di diritto e procedura civile*, 1998

- G. Ziccardi, *Caso Google Vividown. L'assoluzione non sana il conflitto*, in *www.ilfattoquotidiano.it*, 22 dicembre 2012

Sitografia

- www.academia.edu
- www.altalex.com
- www.archiviostorico.corriere.it
- www.camera.it
- www.coe.int/it
- www.consilium.europa.eu
- www.corriere.it
- www.corriereprivacy.it
- www.cortedicassazione.it
- www.costituzionalismo.it
- www.curia.europa.eu
- www.dimt.it
- www.diritticomparati.it
- www.dirittifondamentali.it
- www.diritto.it
- www.diritto24.ilsole24ore.com
- www.dirittosuweb.com
- www.docplayer.it
- www.ec.europa.eu/index_it.htm
- www.echr.coe.int/Pages/home.aspx?p=home&c
- www.eesc.europa.eu
- www.enisa.europa.eu
- www.espresso.repubblica.it
- www.eur-lex.europa.eu
- www.europa.eu
- www.europarl.europa.eu
- www.federalismi.it
- www.federprivacy.it/
- www.filodiritto.it
- www.fondazionecalamandrei.it
- www.fra.europa.eu/en
- www.free-group.eu
- www.garanteprivacy.it

- www.giurcost.org
- www.governo.it/la-presidenza-del-consiglio-dei-ministri
- www.helpconsumatori.it
- www.ilfattoquotidiano.it
- www.independent.co.uk
- www.infoleges.it
- www.internazionale.it
- www.iusexplorer.it
- www.lastampa.it
- www.latribuna.it
- www.normattiva.it
- www.nytimes.com
- www.openstarts.units.it/
- www.osservatorioaic.it
- www.ossimoro.it
- www.mcreporter.info
- www.papers.ssrn.com/sol3/DisplayAbstractSearch.cfm
- www.penalecontemporaneo.it
- www.portolano.it
- www.privacy.it
- www.privacyassosiation.org
- www.quirinale.it/
- www.repubblica.it
- www.rivistaaic.it
- www.rivistaoidu.net/
- www.secure.edps.europa.eu
- www.senato.it
- www.sole24ore.it
- www.teutas.it
- www.vividown.org
- www.washingtonpost.com

LUISS Guido Carli
LIBERA UNIVERSITÀ INTERNAZIONALE DEGLI STUDI SOCIALI

DIPARTIMENTO DI SCIENZE POLITICHE
Cattedra di Diritto dell'informazione e della comunicazione (C.P.)

L' EVOLUZIONE E LA DISCIPLINA DEL TRATTAMENTO DEI DATI SENSIBILI ONLINE E OFFLINE

(RIASSUNTO)

RELATORE
Chiar. mo. Prof.
Pietro Santo Leopoldo Falletta

CANDIDATA
Federica Notari
Matr. 622992

CORRELATORE
Chiar. mo. Prof.
Michele Sorice

ANNO ACCADEMICO 2014/2015

Indice

1. Il presente elaborato ha lo scopo di analizzare la disciplina dei cd. *dati sensibili*, ossia tutte quelle informazioni che ricadono nella sfera più intima dell'individuo e che dunque necessitano di una maggiore protezione rispetto alla categoria più generale dei dati personali. A tal fine, sarà presa in considerazione, sia la normativa europea sia quella italiana in materia di dati sensibili, con particolare riguardo anche al trattamento che questi dati subiscono nella realtà *online*, caratterizzata da una maggiore invasività sulle informazioni degli utenti e da una mancanza di regole specifiche da applicarsi al *web* in caso di violazioni della disciplina in esame. In quest'ottica, sarà necessario mettere in evidenza il ruolo fondamentale svolto dalla giurisprudenza, intervenuta a delineare di volta in volta i profili di responsabilità imputabili ai soggetti che forniscono i servizi in rete, i cd. *Internet service provider (ISP)*, per i contenuti immessi da soggetti terzi.

2. Prima di trattare specificamente della tutela accordata ai dati sensibili, occorre preliminarmente ripercorrere l'evoluzione storica e normativa del concetto più generale della *privacy* all'interno del quale le informazioni in questione ricadono.

Le origini della *privacy* si fanno tradizionalmente risalire alla pubblicazione di un saggio nel 1891 scritto da due avvocati di Boston, S. D. Warren e L. D. Brandeis, intitolato *The Right to Privacy*. Nato come reazione alle notizie indiscrete pubblicate su un quotidiano di Boston sulle amicizie della moglie di Warren, figlia di un noto senatore e sulle nozze della figlia di Warren, per la prima volta si poneva quella che sarebbe stata successivamente la questione della *privacy* aprendo la discussione sul tema, in quanto i due avvocati si trovarono a dover effettuare un *bilanciamento tra interessi contrapposti*: quello di rendere pubbliche le informazioni riguardanti la vita personale di un individuo e quello di tutelare tali informazioni dall'invadenza altrui. Inizialmente, dunque, il contenuto della *privacy* veniva così a coincidere con quella che sarebbe diventata poi la sua componente principale: il diritto di essere lasciati soli, *the right to be let alone*, rientrante evidentemente nelle cd. *libertà negative*[424]. È nel contesto europeo, invece, che si svilupperà un concetto di *privacy* intesa come libertà o diritto positivo, ossia la possibilità dell'individuo di scegliere senza alcun condizionamento con un'accezione più socio-relazionale del concetto e ponendo una maggiore attenzione all'aspetto della tutela dei dati personali e quindi ai connotati informazionali del diritto in oggetto.

A tal proposito, è la Convenzione europea per la salvaguardia dei diritti umani e delle libertà

[424] R. Bin, G. Pitruzzella, *Diritto costituzionale*, Torino, 2014, p. 514, in cui l'autore definisce le *libertà negative* come tutte le rivendicazioni rivolte a respingere lo Stato dalle scelte individuali oltre anche dalle ingerenze esterne di tipo "privato".

fondamentali (CEDU)[425] a qualificare per la prima volta la *privacy* come un diritto fondamentale della persona prevedendo all'art. 8 un *diritto al rispetto della vita privata e familiare*, non considerato in un'accezione assoluta ma prevedendo delle limitazioni basate su interessi pubblici egualmente degni di tutela. Il ruolo della Corte di Strasburgo è stato fondamentale ai fini della corretta interpretazione ed evoluzione della disposizione in esame, pronunciandosi in numerosi casi aventi ad oggetto anche situazioni molto eterogenee[426]. Traendo ispirazione dalla disposizione prevista all'art. 8 CEDU, lo stesso Consiglio d'Europa ha adottato nel 1981 la Convenzione n. 108 *sulla protezione delle persone rispetto al trattamento automatizzato dei dati di carattere personale*[427] che si è occupata del legame tra la protezione delle informazioni degli individui e la gestione automatizzata delle stesse dall'utilizzo fatto dalle nuove tecnologie che si sono sviluppate a partire dagli anni Settanta. Tale Convenzione ha previsto per la prima volta un riferimento specifico a *categorie speciali di dati* distinte dai tradizionali dati comuni, vietando, all'art. 6, la gestione automatica dei dati relativi alla razza, alle opinioni politiche, alle convinzioni religiose, allo stato di salute ed alla vita sessuale, a meno che il diritto interno non preveda garanzie adeguate dal punto di vista della loro tutela. Seppur con ritardo rispetto al Consiglio d'Europa, anche l'Unione europea è intervenuta prevedendo una disciplina specifica per la *privacy* nel 1995 con la direttiva n. 95/46/CE[428], non essendo state previste all'interno dei Trattati istitutivi disposizioni relative ai diritti fondamentali e dunque neanche alla tutela della riservatezza, che ha introdotto un sistema complesso di garanzie per le informazioni personali e finalizzata ad armonizzare le legislazioni degli Stati membri. L'aspetto maggiormente rilevante della direttiva comunitaria stava nel voler salvaguardare la persona umana e la sua vita privata garantendo un'effettiva tutela. Anche la direttiva, nella direzione dell'analoga disposizione contenuta nella Convenzione n.108, ha dedicato particolare attenzione alla disciplina applicabile ad alcune *categorie speciali di dati*, prevista all'art. 8 della stessa, che ha posto un divieto di trattamento da parte degli Stati membri di tutte quelle informazioni che riguardando la sfera più intima della persona ossia quelle che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale e quelle riguardanti lo stato di salute o la vita sessuale. Tuttavia, con le opportune

[425] La Convenzione, firmata dal Consiglio d'Europa nel 1950, è un trattato internazionale finalizzato alla tutela dei diritti umani e le libertà fondamentali in Europa. Tutti i 47 paesi che formano il Consiglio d'Europa, sono parte della convenzione, 28 dei quali sono membri dell'Unione europea (UE). Per maggiori informazioni sulla CEDU si rinvia a *www.eur-lex.europa.eu/summary/glossary/eu_human_rights_convention.html?locale=it.*

[426] Cfr. Corte Edu, ricorso n. 8691/79, sentenza del 2 agosto 1984, *Malone Vs Regno Unito*; Corte Edu, sentenza del 6 settembre del 1978, *Klauss Vs Repubblica Federale di Germania*; Corte Edu, sentenza del 25 febbraio 1997, *Z. Vs Finlandia*; Corte Edu, ricorso n. 10454/83, sentenza del 7 luglio 1989, *Gaskin Vs Regno Unito*; Corte Edu, ricorso n. 2872/02, sentenza del 2 marzo 2008, *K.U. Vs Finlandia.*

[427] La Convenzione è stata adottata a Strasburgo dal Consiglio d'Europa il 28 gennaio 1981 ed è stata ratificata in Italia con la legge 21 febbraio 1989, n. 98 (*Ratifica ed esecuzione della convenzione n. 108 sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale, adottata a Strasburgo il 28 gennaio 1981*).

[428] È la *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.*

garanzie, la stessa disposizione prevede alcune deroghe al suddetto divieto[429] e autorizza gli Stati a prevedere ulteriori eccezioni per motivi di interesse pubblico rilevante, lasciando margini di discrezionalità. Successivamente, l'Unione europea, tenendo conto di come lo sviluppo delle tecnologie abbia inciso fortemente sulla *privacy,* con le innovazioni apportate dal Trattato di Lisbona[430], ha previsto un *diritto alla protezione dei dati a carattere personale* sancito sia all'art. 16 del Trattato sul funzionamento dell'Unione (TFUE) sia all'art. 8 della Carta dei diritti fondamentali dell'Unione distinto tra i "tradizionali" diritti finalizzati al rispetto della vita privata o del proprio domicilio. Tuttavia, negli ultimi anni, le istituzioni europee si sono rese conto dell'inattualità della disciplina prevista dalla direttiva, in quanto al momento della sua adozione si era ben lontani da un'evoluzione del processo tecnologico e della rete come quella attuale capace di minare fortemente la sicurezza delle informazioni personali. Così, in seguito ad un'iniziativa del 2012 della Commissione europea[431], sono state elaborate nuove regole in materia di *privacy* tenendo conto della maggiore richiesta di un controllo sui propri dati degli individui nel mondo della rete e, al contempo, favorendo maggiori opportunità all'interno dell'economia digitale. Infatti, dopo quasi quattro anni, lo scorso 15 dicembre 2015 è stato raggiunto un accordo sul pacchetto delle nuove regole, dopo i negoziati finali tra il Parlamento, la Commissione ed il Consiglio dell'Unione europea, i cd. *triloghi,* in seguito ai quali occorrerà attendere, nei prossimi mesi, la conferma del Consiglio e del Parlamento europeo. Il pacchetto di riforma si compone di due strumenti legislativi: un regolamento, che interesserà tutti i soggetti privati e parte di quelli pubblici e che sarà immediatamente applicabile e sostituirà la direttiva del 1995 sulla protezione dei dati personali; una direttiva, che riguarda l'uso dei dati personali nell'ambito della sicurezza e delle attività di polizia e di giustizia e che necessiterà del recepimento per diventare operativa nei vari Stati, finalizzata

[429] L' art. 8, paragrafo 2 della direttiva n.95/46/CE prevede deroghe qualora: *"a) la persona interessata abbia dato il proprio consenso esplicito a tale trattamento, salvo nei casi in cui la legislazione dello Stato membro preveda che il consenso della persona interessata non sia sufficiente per derogare al divieto di cui al paragrafo 1, oppure*
b) il trattamento sia necessario, per assolvere gli obblighi e i diritti specifici del responsabile del trattamento in materia di diritto del lavoro, nella misura in cui il trattamento stesso sia autorizzato da norme nazionali che prevedono adeguate garanzie, oppure
c) il trattamento sia necessario per salvaguardare un interesse vitale della persona interessata o di un terzo nel caso in cui la persona interessata è nell'incapacità fisica o giuridica di dare il proprio consenso; o
d) il trattamento sia effettuato, con garanzie adeguate, da una fondazione, un'associazione o qualsiasi altro organismo che non persegua scopi di lucro e rivesta carattere politico, filosofico, religioso o sindacale, nell'ambito del suo scopo lecito e a condizione che riguardi unicamente i suoi membri o le persone che abbiano contatti regolari con la fondazione, l'associazione o l'organismo a motivo del suo oggetto e che i dati non vengano comunicati a terzi senza il consenso delle persone interessate; o
e) il trattamento riguardi dati resi manifestamente pubblici dalla persona interessata o sia necessario per costituire, esercitare o difendere un diritto per via giudiziaria."

[430] Il Trattato di Lisbona, firmato a Lisbona il 13 dicembre 2007, è composto dal Trattato dell'Unione europea (TUE) e dal Trattato sul funzionamento dell'Unione europea (TFUE).

[431] Commissione europea, *Proposta di regolamento del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (regolamento generale sulla protezione dei dati),* Bruxelles, 25 gennaio 2012. Tutte le informazioni relative all'iniziativa della Commissione sono consultabili su *www.ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm.*

invece a sostituire una decisione quadro del 2008 in materia[432]. Tuttavia, l'aspetto più innovativo riguarda il regolamento, che, se entrerà in vigore, sarà immediatamente esecutivo all'interno degli Stati membri comportando una sostituzione delle legislazioni in materia. Prevedendo una disciplina più attuale e coerente in materia di protezione dei dati personali in tutto il territorio dell'Unione, il testo del Regolamento ha ampliato i diritti facenti capo all'interessato: dal nuovo diritto alla *portabilità dei dati* ad una definizione più chiara del *diritto all'oblio*. Ma ha anche rafforzato alcuni meccanismi, come quello del consenso - che dovrà essere sempre espresso in modo inequivocabile e dovrà essere specifico ai fini della profilazione, senza del quale la stessa non potrà avvenire - e quello dell'informativa all'interessato; in entrambi i casi, le informazioni dovranno essere più dettagliate e più efficaci delle precedenti attraverso l'uso di moduli, schemi e disegni. Nella stessa ottica, anche gli obblighi posti a capo del titolare del trattamento diventano più stringenti nel nuovo regolamento, considerando che, ancor prima di procedere al trattamento, dovrà progettare in un'ottica di *privacy* in base ai nuovi principi di *privacy by design* e *privacy by default* e prevedere all'inizio del trattamento una valutazione di impatto e verifica preliminare dello stesso. Inoltre, anche la nuova normativa conferma la previsione di una disciplina specifica applicabile per quei dati che sono, per loro natura, particolarmente sensibili e idonei ad incidere in materia di diritti fondamentali e che dunque meritano di una protezione specifica. Nulla è innovato rispetto alla normativa attuale, visto che tali dati non possono essere trattati senza il consenso esplicito da parte dell'interessato; tuttavia deroghe specifiche possono essere previste nei confronti di esigenze specifiche e a quella "tradizionale" del trattamento rientrante tra le attività (legittime) poste in essere da associazioni o fondazioni il cui scopo è quello di consentire l'esercizio delle libertà fondamentali. Deroghe al divieto di trattamento di tali categorie di dati possono essere consentite se previste dalla legge e fatte salve adeguate garanzie in modo di tutelare i dati personali e altri diritti fondamentali come la salute pubblica, la protezione sociale e la gestione dei servizi sanitari, finalizzata quest'ultima a garantire la qualità e costo-efficacia delle procedure per rispondere alle richieste di prestazioni e servizi nel sistema di assicurazione sanitaria, o per scopi storici, statistici e di ricerca scientifica. Occorrerà adesso attendere i prossimi mesi per conoscere il destino delle nuove regole in materia di *privacy* e capire che tipo di conseguenze comporterà all'interno degli Stati membri.

3. Non soltanto la normativa europea, ma anche quella italiana è intervenuta nel prevedere una disciplina finalizzata alla tutela della riservatezza e di conseguenza, sulla scia degli interventi europei, anche per quelle informazioni personali più *sensibili* rispetto alle altre. Preliminarmente, occorre evidenziare come non molto diversamente dagli altri Paesi europei, nella Costituzione

[432] È la decisione Quadro n. 2008/977/GAI *sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale* del 27 novembre 2008.

italiana mancano riferimenti alla *privacy*, perché al momento dell'entrata in vigore della Carta, costituiva un tema poco dibattuto. Tuttavia, a partire dagli anni Cinquanta, la giurisprudenza ha iniziato ad affrontare sempre più frequentemente le questioni attinenti alla riservatezza, pronunciandosi su casi di opere cinematografiche e pubblicazioni relative a vicende personali di personaggi famosi che chiedevano ai giudici una tutela della propria riservatezza[433]. Dunque, nonostante il vuoto normativo, la giurisprudenza e la dottrina hanno ricavato un fondamento costituzionale del diritto da una lettura sistematica sia di disposizioni "generali" come quella previste dagli artt. 2 e 3 della Cost. sia di quelle finalizzate a tutele singole e specifiche come quelle agli artt. 13, 14, 15 e 21 Cost. L'Italia ha previsto l'adozione di una disciplina specifica in materia di *privacy* con ritardo rispetto agli altri Paesi europei come la Francia e la Germania che, invece, si erano dotati di una normativa apposita già a partire dagli anni Settanta spinti dalla diffusione dei nuovi mezzi tecnologici. Infatti fu soltanto nel 1996 che si realizzò il primo intervento normativo in tal senso, con la legge n. 675[434], attraverso il recepimento della direttiva *privacy* 95/46/CE. Introducendo per la prima volta in Italia il principio secondo cui, la riservatezza delle persone fisiche e giuridiche rappresenti un diritto assoluto e inviolabile meritevole di tutela attraverso la comminazione di sanzioni penali, civili e amministrative e, perseguita attraverso l'uso congiunto degli strumenti del controllo e del consenso cd. *informato* con quello più limitato dell'autorizzazione, la legge si è posta l'obiettivo di fornire al cittadino tutti gli strumenti per consentire al cittadino una tutela piena ed effettiva. Nello specifico, la legge n. 675/1996 si è preoccupata di prevedere specifiche tutele per i cd. *dati sensibili* disciplinati all'art. 22 della legge rubricati al Capo IV sul *"trattamento dei dati particolari".* Infatti, sin dal primo intervento normativo in materia, il legislatore ha considerato che alcuni tipi di dati, per il loro contenuto, dovevano essere assoggettati a norme specifiche per la loro incisività nella sfera privata in modo da delimitare all'interno della generale categoria dei dati personali, una più ristretta coincidente con il cd. *nucleo duro della privacy*[435], che comprendono tutte quelle informazioni che necessitano di un bisogno di segretezza. L'art. 22 ha previsto la disciplina in materia di dati sensibili che poi sarà ripresa anche dalla successiva e attuale normativa prevista dal *Codice della privacy.* Nel primo comma dell'articolo, i dati sensibili vengono definiti come *"I dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso,*

[433] Si fa riferimento alle prime pronunce della Corte di Cassazione sul tema. La prima è la sentenza del 22 dicembre 1956, n. 4487 sul caso Caruso; la seconda è la n.990 del 20 aprile 1963 sulla pubblicazione del libro "Il grande amore"; e, la terza sul caso Soraya Esfandiari la n. 2129 del 27 maggio 1975.

[434] La legge del 31 dicembre 1996, n. 675 in materia di Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali, pubblicata in Gazzetta Ufficiale dell'8 Novembre 1997 - Suppl. Ordinario n. 3. La legge è stata abrogata ai sensi dell'articolo 183, comma 1, lettera a), del Codice in materia dei dati personali.

[435] Per una definizione del concetto di *nucleo duro della privacy* si rinvia a S. Rodotà, *Tecnologie e diritti,* Bologna, 1995, p.105.

filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale" e che "*[…]possono essere oggetto di trattamento solo con il consenso scritto dell'interessato e previa autorizzazione del Garante."* Dunque la "super protezione" attribuita al trattamento di tali dati deriva dalla doppia garanzia dell'autorizzazione al Garante e del consenso manifestato in forma scritta da parte dell'interessato. Nel secondo comma, l'art. 22 specifica i tempi e le modalità della decisione adottata dal Garante in base alla richiesta di autorizzazione. Il legislatore è intervenuto a più riprese[436] a modificare la disposizione, prevedendo delle deroghe al regime del consenso scritto dell'interessato e della previa autorizzazione del Garante applicabili nel caso di dati appartenenti a confessioni religiose, ad associazioni od organizzazioni a carattere sindacale o di categoria ad altre associazioni, organizzazioni o confederazioni a carattere sindacale o di categoria.

Dopo circa sette anni di vigenza, la legge del 1996, non avendo considerato il mutamento del contesto tecnologico, è stata considerata obsoleta e abrogata dal decreto legislativo n. 196 del 2003 contenente il *Codice per la protezione dei dati personali*[437], attualmente in vigore. Il *Codice* ha rappresentato la prima esperienza di codificazione e coordinamento normativo di tutte le disposizioni, definendo organicità alla disciplina della riservatezza. Articolato in tre parti e 24 titoli per un totale di 186 articoli, si estende in realtà ben oltre attraverso alcuni allegati che ne costituiscono parte integrante[438]. Nella Prima Parte, il Codice contiene le disposizioni generali ossia le finalità, i principi alla base della legge, le definizioni degli istituti e la disciplina generale; nella Seconda, sono invece previste disposizioni particolari per specifici settori ad integrazione o in deroga a quelle della Prima Parte; infine, la Terza disciplina il meccanismo della tutela dell'interessato da attivarsi per i trattamenti illeciti dei dati personali e l'assetto sanzionatorio penale e amministrativo. Per ciò che riguarda nello specifico la disciplina applicabile ai dati sensibili, il *Codice della privacy* riprende il sistema previsto dalla legge n. 675 del 1996 ma prevede regimi diversi a seconda se il titolare del trattamento sia un soggetto pubblico o privato. La definizione di dato sensibile si ritrova all'art. 4 del *Codice*[439] ed è sostanzialmente analoga a quella precedente, dandone un'accezione particolarmente ampia in quanto non è finalizzata a tutelare soltanto il trattamento dei dati *"che rivelano"* le informazioni sensibili ma anche quelli *"idonei a rilevare"*

[436] Le modifiche furono apportate dai decreti legislativi dell'11 maggio 1999 n.135 e del 28 dicembre 2001 n. 467.

[437] Il decreto legislativo del 30 giugno 2003, n. 196 fu emanato in base alla legge delega del 24 marzo 2001 n.127. Pubblicato in G.U. il 29 luglio 2003 ed entrato in vigore il 1 gennaio 2004, ha introdotto nell'ordinamento italiano il Testo Unico in materia di privacy.

[438] Si fa riferimento ai codici di deontologia; il cd. "Disciplinare tecnico" sulle misure minime di sicurezza ad integrazione degli art. 33-36 del Codice e, anche se non allegate, le autorizzazioni generali per vari settori di attività che si riferiscono ai trattamenti dei dati sensibili e giudiziari.

[439] All' art. 1, comma 4, lettera d), i dati sensibili sono definiti come *"i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale."*

ossia quelli che anche indirettamente o attraverso processi induttivi o presuntivi sono in grado di rivelare il bene protetto, come il nome o il cognome ma anche lo stato di famiglia. Per quanto riguarda i soggetti pubblici, questi possono effettuare un trattamento di dati sensibili sulla base delle disposizioni specifiche previste dagli articoli 20 e 22 del *Codice in materia di protezione dei dati personali*, mentre i soggetti privati e gli enti pubblici economici possono effettuare, come nello schema precedente, un trattamento di dati sensibili con il consenso scritto dell'interessato e la previa autorizzazione del Garante per la protezione dei dati personali ai sensi dell'articolo 26 del Codice salvo alcune eccezioni specificamente previste[440]. Inoltre, all'interno dei dati sensibili, il *Codice* ha accordato una tutela particolare ad alcuni di questi: i cd. *dati supersensibili* ossia quelli relativi alla salute e alla sfera sessuale per i quali sono previste disposizioni specifiche. Ai sensi della lettera d), comma 1 dell'art. 154 del Codice, il Garante per la protezione dei dati ha poi adottato le cd. *autorizzazioni generali* per il trattamento dei dati sensibili (oltre che per quelli giudiziari): infatti, il Garante, sotto espressa previsione del legislatore, ha ritenuto troppo gravoso e pericoloso l'obbligo di richiedere autorizzazioni specifiche al trattamento di dati sensibili e aveva previsto la necessità di prevedere autorizzazioni generali per interi settori o categorie di dati e dei trattamenti autorizzati. Recentemente, il Garante ha rinnovato le autorizzazioni al trattamento dei dati sensibili e giudiziari che saranno efficaci dal 1° gennaio 2015 fino al 31 dicembre 2016, in sostituzione di quelle in scadenza al 31 dicembre 2014. Le nuove autorizzazioni rispecchiano per molti aspetti quelle già adottate e apportano le necessarie integrazioni derivanti da modifiche normative intervenute nei settori considerati. In ciascuna autorizzazione sono individuate le finalità dei trattamenti, le categorie dei dati trattati, degli interessati, dei destinatari della comunicazione e diffusione e sulla limitazione del periodo di conservazione degli stessi. Esse sono l' autorizzazione generale: n. 1/2014 al trattamento dei dati sensibili nei rapporti di lavoro, n. 2/2014 al trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale, n. 3/2014 al trattamento dei dati sensibili da parte degli organismi di tipo associativo e delle fondazioni, n. 4/2014 al trattamento dei dati sensibili da parte dei liberi professionisti, n. 5/2014 al trattamento dei dati sensibili da parte di diverse categorie di titolari, n. 6/2014 al trattamento dei dati sensibili da parte degli investigatori privati, n. 7/2014 al trattamento dei dati a carattere giudiziario da parte di privati, di enti pubblici economici e di soggetti pubblici, n. 8/2014 al trattamento dei dati genetici, n. 9/2014 al trattamento dei dati personali effettuato per scopi di ricerca scientifica.

4. Nonostante la normativa contenga previsioni altamente garantistiche per i dati sensibili, tale protezione non sembra sempre essere rispettata nella sua applicazione pratica. Infatti, la necessità di una tutela più intensa per i dati personali e soprattutto per quelli sensibili è richiesta ancora di più

[440] Il comma 3 e 4 dell'art. 26 prevedono rispettivamente i casi di trattamenti ai quali non si applica la disposizione in esame e i casi di trattamenti effettuabili senza il consenso dell'interessato ma con la previa autorizzazione del garante.

nell'era di Internet: seppur siano immediatamente visibili i vantaggi offerti della rete[441], altrettanto evidente è la moltiplicazione dei rischi legati alla tutela della riservatezza in rete in tutti i suoi aspetti dovuti soprattutto alla previsione di nuovi profili di responsabilità, nei confronti dei dati degli utenti del *web*, in capo ad alcuni soggetti non previsti nell'*offline* ma che assumono un ruolo centrale nell' *online*: i cd. *Internet service provider* (denominati con l'acronimo ISP) ossia i soggetti che forniscono i servizi di connessione, trasmissione, memorizzazione dati anche mettendo a disposizione spazi di memoria per ospitare i siti. Il ruolo assunto da tali figure non è soltanto legato agli aspetti più prettamente economici delle nuove tecnologie, nelle quali i prestatori di servizi *online* forniscono la connessione alla rete, ma coinvolge anche valori più strettamente connessi alle libertà e ai diritti fondamentali della persona. Tale aspetto ha determinato, prima a livello europeo e poi a quello interno, la necessità di prevedere norme specifiche relative al tema della responsabilità degli ISP nel caso di violazioni commesse attraverso i servizi che essi forniscono agli utenti; in particolare attraverso la direttiva europea n. 2000/31/CE conosciuta come direttiva *e-commerce* finalizzata ad assicurare la libera prestazione dei servizi *online* nell'Unione europea, creando una base comune di regole per il commercio elettronico in tutto il territorio dell'Unione e recepita in Italia con il decreto legislativo n.70 del 2003. Prevedendo differenti figure di *provider* in base all'attività svolta[442], il principio generale che accompagna il regime di responsabilità dei prestatori dei servizi della normativa in materia è quello di *neutralità* secondo cui il prestatore dei servizi non è ritenuto responsabile per il contenuto delle informazioni immesse dagli utenti né di eventuali illeciti commessi da terzi, purché sussistano determinate condizioni. Tale aspetto è previsto all'art. 17 del decreto legislativo n. 70 del 2003 che prevede una clausola generale sia di esclusione dall'obbligo di sorveglianza degli ISP sui contenuti e le informazioni che circolano sulla rete da lui gestita sia di ricerca attiva dei fatti che indichino la presenza di illiceità[443].

Per ciò che concerne nello specifico il trattamento illecito di dati sensibili nel mondo *online*, è opportuno segnalare un caso affrontato dalla giurisprudenza che ha aperto in Italia una discussione proprio sulla responsabilità del *provider*. Si tratta del noto caso giurisprudenziale *Google Vs*

[441] Sul punto, si veda, G. Napoli, *Responsabilità dell'Internet Service Provider nella giurisprudenza civile*, in G. Cassano, G. Scorza, G. Vaciago (a cura di), *Diritto dell'internet. Manuale operativo. Casi, legislazione e giurisprudenza*, Padova, 2013, p.463 in cui l'autrice evidenzia come Internet sia capace di condividere e consultare un numero inestimabile di informazioni e di risorse, ovunque queste siano allocate *"facendo sì che gli individui stabiliti ai capi opposti del globo possano facilmente contattarsi e scambiarsi opinioni con banali gesti, ormai istintivi e quotidiani nonché imprescindibili per chiunque".*

[442] I *provider* si distinguono in base alle attività di *mere conduit* (mero trasporto), *caching* (memorizzazione temporanea) e *hosting* (memorizzazione permanente). Le figure sono sostanzialmente analoghe nella normativa comunitaria e in quella interna.

[443] Il quadro normativo previsto è stato integrato dal ruolo apportato dalla giurisprudenza europea ed italiana intervenuta di volta in volta a definire quale fosse il regime di responsabilità applicabile agli ISP. Sul punto si rinvia a Corte di Giustizia delle Comunità europee, terza sezione, 24 novembre 2011, *Scarlet Extended SA Vs SABAM*; Corte di giustizia delle Comunità europee, terza sezione, 16 febbraio 2012, *SABAM Vs Netlog*; Tribunale di Roma, 16 dicembre 2009, *RTI Vs Youtube e Google;* Tribunale di Milano, sezione IV penale, 12 aprile 2010, n.1972, *Google Vs Vivi down*; Tribunale di Roma, IX sezione, 20 ottobre 2011, *RTI Vs Choopa*.

Vividown, in cui l'*Internet Service Provider* era stato accusato da parte di un'associazione finalizzata alla tutela delle persone affette da autismo, *Vividown* appunto, di avere responsabilità penale per la pubblicazione di un video contenente informazioni relativa alla salute di un minore, sulla piattaforma Google Video. La vicenda iniziata dinanzi al Tribunale di Milano in primo grado, che aveva deciso per la condanna di Google, in quanto aveva ritenuto che vi fosse stata una violazione per il trattamento dei dati personali ai sensi dell'art. 167 del *Codice della privacy*, si è conclusa definitivamente con la pronuncia della Corte di Cassazione nel dicembre 2013 che ha assolto il *provider* riformando la decisione del primo grado[444].

Anche la Corte di Giustizia dell'Unione europea è intervenuta in casi analoghi recentemente, decidendo di tutelare effettivamente sul *web* i dati personali "comuni" e sensibili. In particolare, nel caso *Digital Rights Ireland*[445], la Corte di Giustizia, in seguito a due rinvii pregiudiziali presentati dalla High Court irlandese e dalla Suprema Corte austriaca (Verfassungsgerichtshof), ha annullato la direttiva 2006/24/CE *sulla conservazione dei dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica*, sostenendo che, permettendo la conservazione di tali dati e l'accesso delle autorità nazionali a tali dati, la direttiva aveva interferito in modo eccessivo con i diritti fondamentali del rispetto della vita privata e della protezione dei dati personali. Ancora, in un'altra questione, il caso *Google Spain*[446], la Corte, oltre a riprendere la problematica delle responsabilità degli *Internet service provider* in merito alle informazioni presenti sui server, ha fornito importanti considerazioni sul cd. *diritto all'oblio*, di derivazione giurisprudenziale, che sarà espressamente disciplinato dal nuovo Regolamento europeo sulla *privacy*. La portata innovativa della sentenza sta, oltre, nel riconoscimento di un *diritto ad essere lasciato solo*, anche nella previsione di un obbligo in capo al Google, titolare del trattamento, di evitare che certe pagine contenenti informazioni personali vengano indicizzate qualora non siano più giustificate da esigenze di attualità. Infine, la Corte di Giustizia è di recente intervenuta sul tema del rispetto del diritto alla protezione dei dati personali nell'era di internet da parte dei fornitori dei servizi, nel caso *Schrems*[447] in cui ha invalidato una decisione del 2000 della Commissione europea[448], che conteneva il cd. *Safe Harbor* e che permetteva il trasferimento dei dati personali dall'Unione europea agli Stati Uniti, considerati avere quell'adeguato livello di tutela prevista dalla direttiva sulla privacy del 1995.

[444] Cassazione penale, III Sezione , 17 dicembre 2013, (dep. 3 febbraio 2014), n. 5107.
[445] Corte di Giustizia dell'Unione Europea, Grande Sezione, 8 aprile 2014, Cause riunite C-293/12 e C-594/12.
[446] Corte di Giustizia dell'Unione europea, 13 maggio 2014, causa C-131/12, *Mario Costeja Gonzalese e AEPD Vs Google Spain e Google Inc.*
[447] Corte di giustizia dell'Unione europea (Grande Sezione), 6 ottobre 2015, causa C 362/14, *Maximillian Schrems Vs Data Protection Commissioner*.
[448] Si fa riferimento alla decisione della Commissione n. 2000/520/CE.

5. Negli ultimi anni, esigenze o giustificazioni di sicurezza hanno indotto sempre di più all'approvazione di norme che hanno esteso la capacità di controllo, raccolta, conservazione delle informazioni anche più intime degli individui; inoltre, sono state sempre più estese anche le capacità di indagine delle autorità pubbliche a tali dati, tali da non consentire più agli individui di avere un controllo sulle stesse. A difesa di una richiesta di maggiore protezione nei confronti dei propri dati, sono intervenute in prima linea le stesse istituzioni europee, consapevoli della preoccupazione dei propri cittadini delle informazioni da loro immesse in rete. Non solo i casi giurisprudenziali di cui si è detto dimostrano come i giudici europei si sono posti sempre di più l'obiettivo di tutelare la *privacy* e in particolare i dati personali, compresi quelli sensibili, soprattutto nella realtà *online,* ma anche la prospettiva dell'adozione del nuovo Regolamento *privacy* fa ben sperare per un controllo più incisivo degli utenti sulle proprie informazioni, tenendo conto, contrariamente alle discipline europee vigenti, della grande mole dei dati riversata in rete e della necessità di una maggiore sicurezza dovuta all'utilizzo dei nuovi dispositivi mobili. Inoltre, dopo la citata sentenza della Corte di Giustizia che nell'ottobre 2015 ha invalidato il regime dell'approdo sicuro, in seguito alle recenti trattative tra Unione europea e Stati Uniti, si è giunti ad un nuovo accordo sul trasferimento dei dati dei cittadini europei negli Stati Uniti, il cd. *Eu-Us Privacy Shield* ossia lo scudo per la privacy Stati Uniti-Ue, che probabilmente entrerà in vigore nei prossimi mesi. Dalle informazioni sul nuovo accordo è stato previsto che l'accesso ai dati da parte degli apparati di sicurezza sarà soggetto a limitazioni chiare e a meccanismi di controllo al fine di evitare una sorveglianza indiscriminata e ogni anno lo scudo sarà ridiscusso in modo da monitorare l'andamento degli scambi di flusso dei dati. Occorrerà adesso capire se il nuovo accordo prevederà garanzie effettive nei confronti dei dati dei cittadini europei trasferiti negli USA, anche perché proprio lo studente austriaco che sollevò il caso nell'ottobre 2015 dinanzi alla Corte di Giustizia, Max Schrems, ha immediatamente mostrato i suoi dubbi sulla nuova intesa, sostenendo che anche questa potrebbe essere dichiarata invalida dal giudice europeo, in quanto per esservi un effettiva protezione dei cittadini europei, secondo lo studente, dovrebbe esservi soltanto la sua previsione da parte della legge.

Bibliografia

- AA. VV., *Il diritto alla riservatezza e la sua tutela penale*: *atti del terzo simposio di studi di diritto e procedura penali*, Giuffrè, Milano, 1970

- AA.VV., *L'informazione e i diritti della persona*, Jovene, Napoli, 1983

- AA. VV., *Codice della privacy. Commento al decreto legislativo 30 giugno 2003, n.196,* Giuffrè, Milano, 2004

- AA. VV., *Security Issues and Recommendations for Online Social Networks*, Giles Hogben, ENISA, in *www.enisa.europa.eu*, 14 novembre 2007

- G. Accardo, *L'Unione europea paladina della privacy*, in *www.internazionale.it*, 7 ottobre 2015

- R. Acciai (a cura di), *Il Diritto alla protezione dei dati personali. La disciplina sulla privacy alla luce del nuovo codice*, Maggioli editore, Rimini, 2004

- Agenzia dell'Unione europea per i Diritti Fondamentali, *Manuale sul diritto europeo in materia di protezione dei dati*, Belgio, 2014, in *www.fra.europa.eu/en*

- T.A. Auletta, *Riservatezza e tutela della personalità*, Giuffrè, Milano, 1978

- R. Adam, A. Tizzano, *Manuale di diritto dell' Unione europea,* Giappichelli, Torino, 2014

- E. Apa, F. De Santis, *Caso Google/Vividown: pubblicate le motivazioni della sentenza della Corte di appello di Milano*, in *www.portolano.it*

- E. Apa, O. Pollicino, *Modeling the liability of Internet Service Providres. Google VS Vividown. A Constitutional perspective*, Egea, Milano, 2013

- A. Baldassarre, *Globalizzazione contro democrazia*, Laterza, Bari, 2002

- V. Barabba, *Tra Fonti e Corti. Diritti e principi fondamentali in Europa: profili costituzionali e comparati degli sviluppi sovranazionali*, Cedam, Padova, 2008

- E. Barilà, C. Caputo, *Il trattamento dei dati sensibili da parte dei soggetti pubblici nel D.Lgs. 11 maggio* 1999, n.135, in *Tar*, 1999

- M. Bassini, O. Pollicino, *La Corte di giustizia demolisce il safe harbor e ridisegna i confini del diritto alla privacy in ambito transnazionale*,, in *www.diritto24.ilsole24ore.com*, 7 ottobre 2015

- E. Bassoli (a cura di), *Come difendersi dalla violazione dei dati su internet. Diritti e responsabilità.*, Maggioli editore, Rimini, 2012

- L. Beduschi, *Caso Google: libertà di espressione in internet e tutela penale dell'onore e della riservatezza*, in *Il Corriere del Merito*, 2010

- A. Bevere, A. Cerri, *Il diritto di informazione e i diritti della persona. Il conflitto della libertà di pensiero con l'onore, la riservatezza, l'identità personale*, Giuffrè, Milano, 2006

- P. Bilancia, M. D' Amico (a cura di), *La nuova Europa dopo il Trattato di Lisbona*, Giuffrè, Milano, 2009

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

- Frederik Z. Borgesius, *Behavioural sciences and the regulation of privacy on the internet*, A-L Sibony & A. Alemanno, University of Amsterdam, 23 ottobre 2014,

- G. Branca (a cura di), *Commentario della Costituzione*, Zanichelli, Bologna, 1975

- L. D. Brandeis, S. D. Warren, *The Right to Privacy*, in *Harvard Law Review*, 1890

- E. Brugiotti, *La privacy attraverso le "generazioni dei diritti". Dalla tutela della riservatezza alla protezione dei dati personali fino alla tutela del corpo elettronico*., in *www.dirittifondamentali.it*, 2013

- F. Buffa, G. Cassano, *Responsabilità del content provider e dell'host provider*, in *www.altalex.com*, 14 febbraio 2003 e aggiornato il 19 luglio 2005

- G. Buttarelli, *Banche dati e tutela della riservatezza*, Giuffrè, Milano, 1997

- G. Camera, O. Pollicino, *La legge è uguale anche sul web: Dietro le quinte del caso Google-Vividown*, Egea, Milano, 2010

- M. Cammarata, *Google-Vivi Down, una sentenza da cancellare*, in *www.interlex.it*, 19 aprile 2010

- M. Cammarata, *Sentenza Google. La Rete è davvero in pericolo?,* in *www.mcreporter.info*, 25 febbraio 2010

- V. Campanelli, *Infowar. La battaglia per il controllo e la libertà della rete*, Egea, Milano, 2013

- F. Cardarelli, S. Sica, V. Zeno-Zencovich (a cura di), *Il codice dei dati personali: temi e problemi*, Giuffrè, Milano, 2004

- P. Carey, *E-privacy and online data protection*, Butterworths, London, 2002

- P. Carey, *Data protection: a pratical guide to UK and EU law*, Oxford University Press, Oxford, 2004

- G. Cassano, G. Scorza, G. Vaciago (a cura di), *Diritto dell'internet. Manuale operativo. Casi, legislazione e giurisprudenza*, Cedam, Padova, 2013

- G. Cassano, *Google v. Vividown: responsabilità "assolute" e fine di Internet*, in *Il Diritto di famiglia e delle persone*, fasc. 4, 2010

- G. Cassano, *Riflessioni a margine di un convegno sul caso Google/Vivi Down*, in *Rivista penale*, fasc. 10, 2010

- G. Cellamare, *Tutela della vita privata e libera circolazione delle informazioni in una recente convenzione del Consiglio d'Europa*, in *Rivista di Diritto Internazionale*, 1982

- P. Cendon, *Trattato breve dei nuovi danni*, Volume 2, Cedam, Padova, 2011

- G.P. Cirillo, *La tutela della privacy nel sistema del nuovo codice sulla protezione dei dati personali. Tutela civile, amministrativa, penale*, Cedam, Padova, 2004

- G.P. Cirillo (a cura di), *Il Codice sulla protezione dei dati personali*, Giuffrè, Milano, 2004

- A. Cherchi, *Privacy, la Ue detta le regole per tutti*, in *www.ilsole24ore.com*, 25 gennaio 2016

- A. Clemente (a cura di), *Privacy*, Cedam, Padova, 1999

- B. Conforti, *Diritto internazionale*, VIII edizione, Editoriale scientifica, Napoli, 2010

- M. Consonni, *Il diritto all'oblio per la Corte di Giustizia Europea nella recente decisione del caso Google Spain*, in *www.diritto24.ilsole24ore.com*, 23 giugno 2014

- V. Cuffaro, V. Ricciuto (a cura di), *La disciplina del trattamento dei dati personali,* Torino, Giappichelli, 1997

- M. D'Alberti, *Autorità indipendenti (diritto amministrativo),* in *Enciclopedia Giuridica,* Roma, 1995

- F. De Benedetti, *Addio a Safe harbor, ecco lo "Scudo per la privacy": sì all'accordo Usa-Ue sui dati personali,* in *www.repubblica.it,* 2 febbraio 2016

- L. De Grazie, *La libertà di stampa e il diritto all'oblio nei casi di diffusione di articoli attraverso internet,* in *www.rivistaaic.it* , 2013

- M. Dicosola, *La data retention directive e il dialogo tra Corti costituzionali e Corte di Giustizia nel sistema multilivello europeo, Diritti comparati,* in *www.diritticomparati.it,* 20 febbraio 2014

- M. De Cata, *La responsabilità civile dell'Internet service provider,* Collana Univ. Milano-Bicocca-Dip. Dir. Per l'economia, Giuffrè, Milano, 2010

- A. De Cupis, *I diritti della personalità* in *Trattato di diritto civile e commerciale* già diretto da A. Cicu e F. Messineo e continuato da L.Mengoni, Giuffrè, Milano, 1956

- A. Di Martino, *Il Bundesverfassungsgericht dichiara l'incostituzionalità della data retention e torna sul rapporto tra libertà e sicurezza,* in *Giurisprudenza costituzionale,* 2010

- F. Fabris, *Il diritto alla privacy tra passato presente e futuro,* in *www.openstarts.units.it,* 15 dicembre 2009

- P. Falletta, *La Corte di Giustizia, ancora una volta, contro le multinazionali del web (riflessioni su Corte di Giustizia UE (Grande sezione), 6 ottobre 2015, Schrems c. Data Protection Commissioner, C-362/14),* in *www.federalismi.it,* 23 dicembre 2015

- P. Falletta, M. Mensi, *Il diritto del web. Casi e materiali,* Cedam, Padova, 2015

- H. Farrell, A. Newman, *This privacy activist has just won an enormous victory against U.S. surveillance. Here's how,* in *www.washingtonpost.com,* 6 ottobre 2015

- G.F. Ferrari (a cura di), *La tutela dei dati personali in Italia 15 anni dopo. Tempo di bilanci e bilanciamenti.,* Collana di Diritto dell'Economia a cura di P. Marchetti, Egea, Milano, 2013

- L. Ferrari Bravo, E. Moavero Milanesi, *Lezioni di Diritto Comunitario,* Editoriale scientifica, Napoli, 2002

- L. Ferrari Bravo, A. Rizzo, *Codice dell'Unione europea. Annotato con la giurisprudenza della Corte di Giustizia*, III edizione curata da A. Rizzo e F.M. Di Majo, Giuffrè, Milano, 2008

- G. Finocchiaro (a cura di), *Diritto all'anonimato: anonimato, norme e identità personale,* Cedam, Padova, 2008

- G. Finocchiaro, *Privacy e Protezione dei dati personali. Disciplina e strumenti operativi*, Zanichelli, Bologna, 2012

- L. Floridi, *Google, una sentenza che lascerà delusi*, in *www.lastampa.it*, 20 dicembre 2012

- M. Gambini, *Gli hosting providers tra doveri di diligenza professionale e assenza di un obbligo generale di sorveglianza sulle informazioni memorizzate*, in *www.costituzionalismo.it*, 27 dicembre 2011

- G. Gardini, *Le regole dell'informazione. Principi giuridici, strumenti, casi,* Bruno Mondadori, Milano, 2009

- C. Gattei, *Considerazioni sulla responsabilità dell'Internet provider*, in *www.interlex.it*, 23 novembre 1998

- A. Ghiribelli, *Il diritto alla privacy nella Costituzione italiana*, in *www.teutas.it*, 30 novembre 2007

- E. Giannanotonio, M.G. Losano, V. Zeno-Zencovich (a cura di), *La tutela dei dati personali. Commentario alla l.675/1996*, II edizione, Cedam, Padova, 1999

- A. Griffin, J. Merrill, *European court rules "Safe Harbour" treaty that saw Facebook hand over user data to US is invalid, after challenge by student*, in *www.independent.co.uk*, 6 ottobre 2015

- M. Iaselli, *I principi informatori del Codice della privacy fra teoria e pratica. La protezione dei dati personali alla luce del D. Lgs. 196/2003*, in *www.docplayer.it*, 2009

- M. Iaselli, *Privacy: il Garante si adegua alla sentenza "Safe Harbor"*, in *www.altalex.com*, 3 dicembre 2015

- M. Iaselli, *Accordo raggiunto sul Regolamento Europeo in materia di protezione dei dati personali*, in *www.altalex.com*, 23 dicembre 2015

- Riccardo Imperiali, Rosario Imperiali, *La tutela dei dati personali, Vademecum sulla privacy informatica*, collana Legale, pubblicato da *Il Sole 24 ore*, 1997

- A. Ingrassia, *Il ruolo dell' Isp nel ciberspazio: cittadino, controllore o tutore dell'ordine? Risposte attuali e scenari futuribili di una responsabilità penale dei provider nell'ordinamento italiano,* in *www.penalecontemporaneo.it,* 8 novembre 2012

- A. Ingrassia, *La decisione d'Appello nel caso Google vs Vivi Down: assolti i manager, ripensato il ruolo del provider in rete,* in *Il Corriere del Merito,* 2013

- A. Ingrassia, *La sentenza della Cassazione sul caso Google,* in *www.penalecontemporaneo.it,* 6 febbraio 2014

- R. Levine, *Behind the European Privacy Ruling That's Confounding Silicon Valley*, in *www.nytimes.com*, 9 ottobre 2015

- A. Loiodice, G. Santaniello, (a cura di), *La tutela della riservatezza,* Cedam, Padova, 2000

- R. Lotierzo, *Il caso Google-Vividown quale emblema del difficile rapporto degli internet service provides con il codice della privacy,* in *Cassazione Penale*, 2010

- A. Luongo, *Regole globali per disciplinare privacy ed internet*, in *www.ilsole24ore.com,* 16 aprile 2010

- A. Mantelero, *Il futuro regolamento EU sui dati personali e la valenza "politica" del caso Google: ricordare e dimenticare nella digital economy*, in *Diritto dell'Informazione e dell'informatica,* 2014

- S. Mariani, *Internet non è una "zona franca". Condannati i dirigenti di Google*, in *www.altalex.com,* 27 aprile 2010

- L. Miglietti, *Profili storico-comparativi del diritto alla privacy*, in *www.diritticomparati.it,* 4 dicembre 2014

- G. Modesti, *Commento breve al D.LGS.VO N. 196/2003. Codice in materia di protezione dei dati personali, Diritto civile e commerciale,* in *www.diritto.it,* 20 ottobre 2005

- J. Monducci, *Diritti della persona e trattamento dei dati particolari,* Giuffrè, Milano, 2003

- S. Niger, *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali,* Cedam, Padova, 2006

- U. Pagallo, *Il diritto nell'età dell'informazione. Il riposizionamento tecnologico degli ordinamenti giuridici tra complessità sociale, lotta per il potere e tutela dei diritti,* Giappichelli, Torino, 2014

- R. Pannetta (a cura di), *Libera circolazione dei dati e protezione dei dati personali,* Giuffrè, Milano, 2006

- R. Pardolesi (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, Volume I, Giuffrè, Milano, 2003

- R. Pardolesi (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, Volume II, Giuffrè, Milano, 2003

- R. Petti, *La protezione dei dati personali e il caso Google Spain*, in *www.dimt.it*, 20 marzo 2015

- A. Piersanti, V. Roidi (a cura di), *Giornalisti nella rete*, Ente dello Spettacolo, Roma, 1999

- L. Pineschi (a cura di*), La tutela internazionale dei diritti umani. Norme, garanzie e prassi*, Giuffrè, Milano, 2006

- F. Pizzetti, *Datagate, Prism, caso Snowden: il mondo tra nuova grande guerra cibernetica e controllo globale*, in *www.federalismi.it*, 26 giugno 2013

- O. Pollicino, *Google versus Vividown: gli argomenti "forti" della decisione di Appello*, in *www.diritto24.ilsole24ore.com*, 27 dicembre 2012

- O. Pollicino, *Google versus Vividown atto II: ecco le motivazioni*, in *www.diritto24.ilsole24ore.com*, 28 febbraio 2013

- O. Pollicino, *Tutela del pluralismo nell'era digitale: ruolo e responsabilità degli Internet service provider*, in *www.giurcost.org*, 2014

- M. Pratellesi, *Ecco la Carta dei nostri diritti nell'era di internet* in *www.espresso.repubblica.it*, 28 luglio 2015

- O. Prevosti, *Tutela della privacy come presupposto della libertà: due recenti sentenze della Corte di Giustizia dell'Unione Europea a difesa della riservatezza individuale,* in *www.osservatorioaic.it*, settembre 2014

- M. Prosperi, *Il diritto alla riservatezza nell'ordinamento costituzionale*, I parte, in *www.dirittosulweb.it*

- M. Prosperi, *Il diritto alla riservatezza nell'ordinamento costituzionale*, II parte, in *www.dirittosulweb.it*

- A.R. Popoli, *Social network e concreta protezione dei dati sensibili: luci ed ombre in una difficile convivenza,* in *Diritto dell'informazione e dell'informatica*, 2014

- G. Rasi, *Valutazioni del datore di lavoro sul dipendente e privacy: l'intervento del legislatore,* in *Il Sole-24Ore – Guida al lavoro*, 8 agosto 2003

- G. Repetto, *La Corte di giustizia dell'UE dichiara invalida la direttiva sulla Data Retention: verso la costituzionalizzazione del diritto alla privacy?,* in *www.academia.edu.data*, 24 giugno 2014

- F. Resta (a cura di), *La tutela dei dati personali nella società dell'informazione,* Giappichelli, Torino, 2009

- G. Resta, V. Zeno-Zencovich (a cura di), *Il diritto all'oblio su internet dopo la sentenza Google Spain*, Roma tre- press, 2015

- C. Rigotti, *Il nuovo testo unico sulla privacy*, Seac, Trento, 2003

- S. Rodotà, *Intervista su privacy e libertà*, a cura di Paolo Conti, Laterza, Roma-Bari, 2005

- S. Rodotà, *La privacy tra individuo e collettività*, Bologna, Il Mulino, in *Politica del diritto* n. 5 (settembre-ottobre) 1974

- S. Rodotà, *Tecnologie e diritti*, Il Mulino, Bologna, 1995

- S. Rodotà, *Apologia dei diritti*, La Stampa, 2 luglio 2002 in *www.ossimoro.it*

- S. Rodotà, *Tra i diritti fondamentali ed elasticità della normativa: il nuovo Codice sulla privacy*, in *Europa e Diritto Privato*, 2004

- S. Rodotà, *Internet e privacy, c'è un giudice in Europa che frena gli Usa*, in *www.repubblica.it*, 12 ottobre 2015

- S. Russo, A. Sciuto, *Habeas data e informatica*, Giuffrè, Milano, 2011

- R. Salvi, *La Corte di Cassazione sul caso Google vs Vivi Down: l'host provider non governa il mare magnum della rete*, in *Diritto civile e commerciale*, in *www.diritto.it*, 18 marzo 2014

- G. Santaniello, *La semplificazione delle regole nel codice della privacy*, in *www.interlex.it*, 3 marzo 2004

- G. Santaniello, *Le autorizzazioni per categoria relative al trattamento dei dati sensibili*, Relazione al Convegno Paradigma, Milano, 10-11 febbraio 1998.

- G. Santaniello (a cura di), *La protezione dei dati personali*, in *Trattato di diritto amministrativo* diretto da G. Santaniello, Volume trentaseiesimo, Cedam, Padova, 2005

- A. Scalisi, *Il diritto alla riservatezza*, Giuffrè, Milano, 2002

- A. Scirocco, *The Lisbon Treaty and the Protection of Personal Data in the European Union*, in *www.secure.edps.europa.eu*, 19 settembre 2008

- G. Scorza, G. Vaciago (a cura di), *Diritto dell'internet. Manuale operativo: casi, legislazione e giurisprudenza*, Cedam, Padova, 2010

- G. Scorza, *Carta di Internet, "l'accesso alla rete è un diritto fondamentale della persona",* in *www.ilfattoquotidiano.it*, 28 luglio 2015

- G. Scorza, *Corte Ue:" Usa non proteggono privacy". Ecco cosa accade ora a Facebook, Google ed Apple*, in *www.ilfattoquotidiano.it*, 6 ottobre 2015

- P. Schaar, *Data Retention: a landmark Court of Justice's ruling. (5) From now on, no more <<just in case>> retention of data*, in *www.free-group.eu*, 10 aprile 2014

- E. Stefanini, *Dati genetici e diritti fondamentali. Profili di diritto comparato ed europeo*, Cedam, Padova, 2008

- E. Varani, *Il "nuovo diritto "alla privacy. Dalla Carta di Nizza al "Codice in materia di protezione dei dati personali"*, in *www.filodiritto.com*, 7 aprile 2012

- F. Vecchio, *L'ingloriosa fine della direttiva Data retention, la ritrovata vocazione costituzionale della Corte di Giustizia ed il destino dell'art. 132 del Codice della privacy*, in *www.diritticomparati.it*, 12 giugno 2014

- U. Villani, *Istituzioni di diritto dell'Unione europea*, Seconda edizione riveduta e aggiornata, Cacucci Editore, Bari, 2012

- P. Zanelli, *La Legge N. 675 del '96 : una strategia integrata di protezione per la privacy*, in *Contratto e Impresa*, 1997

- C. Zanghi, *La mancata adesione dell'Unione Europea alla CEDU nel parere negativo della Corte di giustizia*, in *www.rivistaoidu.net*, marzo 2015

- V. Zeno- Zencovich, *I diritti della personalità dopo la legge sulla tutela dei dati personali*, in *Studium Iuris*, 1997

- V. Zeno- Zencovich, *Una lettura comparatistica della l. n. 675/96 sul trattamento dei dati personali*, in *Rivista trimestrale di diritto e procedura civile*, 1998

- G. Ziccardi, *Caso Google Vividown. L'assoluzione non sana il conflitto*, in *www.ilfattoquotidiano.it*, 22 dicembre 2012

Sitografia

- www.academia.edu
- www.altalex.com
- www.archiviostorico.corriere.it
- www.camera.it
- www.coe.int/it
- www.consilium.europa.eu
- www.corriere.it
- www.corriereprivacy.it
- www.cortedicassazione.it
- www.costituzionalismo.it
- www.curia.europa.eu
- www.dimt.it
- www.diritticomparati.it
- www.dirittifondamentali.it
- www.diritto.it
- www.diritto24.ilsole24ore.com
- www.dirittosuweb.com
- www.docplayer.it
- www.ec.europa.eu/index_it.htm
- www.echr.coe.int/Pages/home.aspx?p=home&c
- www.eesc.europa.eu
- www.enisa.europa.eu
- www.espresso.repubblica.it
- www.eur-lex.europa.eu
- www.europa.eu
- www.europarl.europa.eu
- www.federalismi.it
- www.federprivacy.it/
- www.filodiritto.it
- www.fondazionecalamandrei.it
- www.fra.europa.eu/en
- www.free-group.eu
- www.garanteprivacy.it

- www.giurcost.org
- www.governo.it/la-presidenza-del-consiglio-dei-ministri
- www.helpconsumatori.it
- www.ilfattoquotidiano.it
- www.independent.co.uk
- www.infoleges.it
- www.internazionale.it
- www.iusexplorer.it
- www.lastampa.it
- www.latribuna.it
- www.normattiva.it
- www.nytimes.com
- www.openstarts.units.it/
- www.osservatorioaic.it
- www.ossimoro.it
- www.mcreporter.info
- www.papers.ssrn.com/sol3/DisplayAbstractSearch.cfm
- www.penalecontemporaneo.it
- www.portolano.it
- www.privacy.it
- www.privacyassosiation.org
- www.quirinale.it/
- www.repubblica.it
- www.rivistaaic.it
- www.rivistaoidu.net/
- www.secure.edps.europa.eu
- www.senato.it
- www.sole24ore.it
- www.teutas.it
- www.vividown.org
- www.washingtonpost.com