Università
Ca'Foscari
Venezia

Corso di Laurea

in Economia Aziendale

(vecchio ordinamento, ante D.M. 509/1999)

Tesi di Laurea

IL BILANCIAMENTO TRA DIRITTO ALLA *PRIVACY* E DIRITTO ALLE INFORMAZIONI NELL'ESERCIZIO DELL' ATTIVITA' D'IMPRESA: IL CASO "MANNI" (CGE C-398/15)

Relatore:
Ch. Prof. Giuliana Martina

Correlatore:
Ch. Prof. Camardi Carmela

Laureando:
Ermenegildo Stragliotto
Matricola 723574

Anno Accademico
2017/2018

INDICE

INTRODUZIONE

Obiettivo di questo elaborato è quello di compiere una disamina sulla tematica del trattamento e della protezione dei dati personali alla luce delle limitazioni che tale diritto fondamentale può subire: se, da un lato, il trattamento dei dati personali rappresenta una prerogativa del singolo individuo, l'attenuazione dello stesso può talvolta giustificarsi con esigenze di tipo economico o sociale tanto nell'ambito dell'operatività di soggetti privati quanto nell'ordinaria attività degli enti pubblici.

L'attenzione sarà posta in particolare su quelli che possono essere i contrasti tra diritti personali e diritti dei principali soggetti economici che rappresentano il motore di ogni sistema economico, cioè le imprese (siano esse pubbliche o private)

Principale fine di questo lavoro sarà quello di illustrare e analizzare quali possono essere gli strumenti, i modelli e i criteri presenti all'interno dell'ordinamento giuridico nazionale ed europeo, in grado di mantenere una coesistenza armonica, un equilibrio tra più interessi contrapposti.

Si tratterà innanzitutto di comprendere a cosa ci si riferisce quando si parla di "dati personali", in particolare soffermandosi sulla natura, sulle caratteristiche e sulla tipologia di questi dati. Com'è noto, la data del 25 maggio 2018 ha segnato l'entrata in vigore per tutti gli Stati appartenenti all'Unione Europea del regolamento 2016/679, relativo alla protezione delle persone fisiche con riguardo al trattamento e alla libera circolazione dei dati personali. Tralasciando per il momento le criticità della normativa rilevate da operatori e parte della dottrina, il menzionato regolamento riveste un'importanza fondamentale in quanto intende rafforzare e armonizzare le norme concernenti la protezione dei dati personali dei cittadini e dei residenti dell'Unione Europea, sia all'interno dell'area comunitaria sia al di fuori di essa. Tale esigenza di ampliare la sfera di tutela dei dati personali è via via cresciuta nel tempo fino a rendersi assolutamente necessaria negli anni più recenti, a causa della rapida espansione negli ultimi anni di nuove tecnologie e piattaforme che hanno permesso alle imprese operanti nel mercato, o agli enti della pubblica amministrazione, di utilizzare, o peggio sfruttare, il valore economico (e non) dei dati degli utenti.

Considerata l'irrinunciabilità dell'evoluzione tecnologica quale motore imprescindibile dello sviluppo socio-economico di una società moderna, la tutela del valore che hanno assunto le informazioni personali, fino ad oggi imperniato sul diritto alla protezione dei dati personali sancito dall'art 1 del c. d. Codice della Privacy, con l'introduzione del GDPR (General Data Protection Regulation) ha acquisito una prospettiva di efficacia duratura: in quest'ottica si è posto l'obiettivo di uno sviluppo sostenibile delle dinamiche tecnologiche, che all'interno del mondo economico e sociale deve basarsi su un bilanciamento virtuoso tra l'interesse economico e le garanzie di controllo dei dati delle persone fisiche.

Nell'ambito della tutela dei dati personali, il GDPR ha avuto anche il merito anche di introdurre e positivizzare il c.d. diritto all'oblio, chiamato nel gergo giuridico anglosassone *the right to be forgotten*: all'articolo 17 si sancisce infatti che *"l'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali"*, qualora sussista uno dei motivi elencati dalle lettere a), b), c).. f) dello stesso articolo 17.

Accantonando per un attimo le varie impostazioni dottrinali esistenti e prescindendo da un'analisi comparata delle applicazioni normative sul tema (di cui si discuterà più approfonditamente nei prossimi capitoli), se per diritto all'oblio si fa riferimento a un generico "diritto dell'individuo ad essere dimenticato", va da sé che uno dei fini principali di questo lavoro sarà quello di evidenziare le possibili sfere di contrasto di cui tale diritto può rendersi protagonista in particolari contesti: si pensi ai possibili conflitti che possono sfociare qualora a fare da contraltare ci sia la libertà d'impresa, il diritto di cronaca, la libertà di manifestazione di pensiero o più in generale qualunque situazione in cui si manifesti un interesse pubblico a voler "ricordare" un determinato fatto o notizia relativo a una persona.

Lungi da poter affrontare una tematica così complessa in maniera esauriente, l'attenzione di questo progetto sarà posta principalmente su due casi particolari che, a parere di chi scrive, rappresentano per alcuni versi due soluzioni divergenti rispetto al problema sopracitato del bilanciamento tra diritti della sfera individuale e diritti della collettività.

Per questa ragione, dapprima l'analisi ricadrà sulla causa C-131/12 della Corte di Giustizia Europea, più comunemente conosciuta come *Caso Google Spain,* ove la Corte ha dovuto confrontarsi con il diritto da parte del singolo di richiedere al gestore del motore di ricerca la cancellazione di link che riportavano a pagine contenenti dati personali.

Successivamente invece si procederà ad esaminare la causa C-398/15 della CGE (2017), denominata *Caso Manni*, in cui i giudici si sono espressi sulla possibilità da parte di un singolo di richiedere la cancellazione di dati personali contenuti all'interno del registro delle imprese.

Com'è evidente, nel primo caso il diritto all'oblio dell'individuo urta sia con gli interessi economici dell'impresa privata sia più in generale e concretamente con l'interesse generale alla libertà di informazione; nel secondo caso, i diritti della sfera privata trovano un ostacolo nell'interesse al corretto funzionamento del mercato, costituito nella fattispecie in esame dal sistema della pubblicità legale.

Alla luce di quanto detto in merito all'introduzione del GDPR, e attraverso l'analisi di casi concreti, la sfida consisterà nel capire quali significativi interventi siano stati messi in atto per la tutela dei dati personali e quali siano ancora le criticità e le debolezze da risolvere: l'ultimo capitolo sarà infatti dedicato ad illustrare le prospettive evolutive e le soluzioni più adeguate per garantire ai dati personali un livello di tutela adeguata, che non comprima o limiti eccessivamente gli interessi contrapposti.

CAPITOLO I: Dal diritto alla riservatezza alla protezione dei dati personali: aspetti storici della necessità di tutela della sfera privata nei confronti dell'evoluzione tecnologica

Sommario: • 1.1. Il concetto di Privacy: origine ed evoluzione nell'esperienza statunitense • 1.2 Le esigenze per l'affermazione di un diritto alla riservatezza nel contesto europeo • 1.3 Il diritto alla riservatezza nell'esperienza italiana • 1.4 Il riconoscimento del diritto alla riservatezza e del diritto alla privacy nel contesto europeo • 1.5 Differenza concettuale tra riservatezza, privacy e protezione dei dati personali • 1.6 Considerazioni preliminari sulla protezione dei dati personali alla luce del Regolamento 2016/679

1.1. Il concetto di Privacy: origine ed evoluzione nell'esperienza statunitense

Sebbene già nell'Antica Grecia, Aristotele offrisse una distinzione tra la sfera pubblica della *polis* e quella privata dell'*oikos*, non si può dire che nel mondo della Grecia classica vi fosse una concezione rivendicativa del concetto di privacy, inteso come autonomo diritto meritevole di tutela: anzi, nella Repubblica di Platone, il mito dell'Anello di Gige[1] testimonia una certa riluttanza da parte del mondo classico verso l'idea della riservatezza, vista negativamente come possibilità da parte dell'uomo di sottrarsi agli obblighi etici e sociali[2].

1 Nel secondo libro della Repubblica di Platone viene narrato il mito dell'Anello di Gige, bovaro al soldo del re Candaule di Lidia, che grazie a un anello ritrovato in una voragine apertasi nel terreno, acquisì il dono dell'invisibilità. Sfruttando questa abilità, riuscì a intrufolarsi nel palazzo del Re, a sedurre la moglie di Candaule e con il suo aiuto ad uccidere il Re, divenendo così il nuovo regnante. Il racconto viene utilizzato come metafora per dimostrare che nessun uomo, qualora vi sia l'opportunità di non essere scoperto, desiste dal compiere azioni illegittime a proprio vantaggio. Nel mondo digitale, oggi si fa riferimento al mito di Gige per indicare quel particolare fenomeno per cui l'anonimato su Internet induce "comportamenti giuridicamente vietati, socialmente dannosi, moralmente deprecabili". Sartor, G., Di Cocco, C., *Temi di diritto dell'informatica (terza Edizione),* Giappichelli Editore, Torino, 2017, pag. 19.

2 Colomba, G. , Zanetti G., *Aspetti problematici della nozione di privacy da un punto di vista filosofico-giuridico* in "Teoria e critica della regolazione sociale", n.1, 2017, pag 27. Allo stesso modo Fabris, F.

Secondo il grande costituzionalista Stefano Rodotà, recentemente scomparso, le condizioni per l'affermazione di un moderno diritto alla privacy si originarono contestualmente alla disgregazione della società feudale[3]. La privacy emerse quindi come un'esigenza della nuova classe borghese di porre un freno e un limite all'ingerenza dello stato, un modo per l'individuo di opporsi alla forza della Corona[4].

Premesso questo, tradizionalmente le origini dell'attuale concetto di privacy si fanno però risalire a un saggio dal titolo *"The right to privacy. The implicit made explicit",* pubblicato nel 1890 da Samuel Warren[5] e Louis Brandeis. Si tratta di uno scritto di matrice ideologica profondamente liberale: i due giuristi avanzarono un primo tentativo di sostenere che l'affermazione di una tutela del cittadino dall'illegittima ingerenza del potere pubblico nella vita privata costituisse un diritto meritevole di protezione a livello costituzionale[6]. Accanto alla tradizionale inviolabilità del domicilio, i due studiosi suggerirono che la tutela dovesse essere ampliata ad altri beni attinenti alla sfera individuale, quali *thoughts, sentiments and emotions[7].*

, *Il diritto alla privacy tra passato, presente e futuro* in Rivista di Scienze della Comunicazione, n.2, 2009, pag. 94

3 S. Rodotà, *La privacy tra individuo e collettività,* in «Politica del Diritto», 1974, p. 545 e ss.

4 Tale considerazione trova un suo fondamento ad esempio nel celebre discorso pronunciato alla Camera dei Lord, da William Pitt: "*Il più povero degli uomini può, nella sua casetta, lanciare una sfida opponendosi a tutte le forze della corona. La casetta può essere fragile, il suo tetto può essere traballante, il vento può soffiare da tutte le parti, la tempesta può entrare e la pioggia può entrare, ma il re d'Inghilterra non può entrare; tutte le sue forze non osano attraversare la soglia di tale casetta in rovina"*. Tratto da W. Pitt, The Elder, Lord Chatham, discorso del marzo 1763, citato in Colomba, G. , Zanetti G., *Aspetti problematici della nozione di privacy da un punto di vista filosofico-giuridico,* cit., pag. 28

5 Il saggio prese le mosse dalle vicende legate alla vita privata dello stesso Warren:l'avvocato aveva intentato una causa contro il giornale Evening Gazete di Boston, reo di aver pubblicato indiscrezioni relative ala vita matrimoniale della moglie dello stesso Warren.

6 Mancini, A. , *La protezione dei dati personali* in Megale, M. (a cura di), *ICT e diritto nella società dell'informazione,* Giappichelli Editore, Torino, 2017, pag. 107

7 Fabris, F. , *Il diritto alla privacy tra passato, presente e futuro* in Rivista di Scienze della Comunicazione, n.2, 2009, pag. 95

La privacy viene ad assumere un significato sintetizzabile nell'espressione *the right to be alone*[8]*,* vale a dire il diritto ad essere lasciati soli per godere in pace della propria vita. Si passa così dalla *privacy-property* alla *privacy-dignity: il right to privacy* diviene espressione dell'emersione di una nuova società fondata sulla libertà individuale[9].

Cambiamento sociale ed evoluzione tecnologica dei mezzi di comunicazione (nel 1875 venne introdotta la stampa rotativa che segnò l'avvento dell'era della società dell'informazione) rappresentano gli aspetti dai quali il concetto di privacy non poté e non potrà neppure in futuro prescindere: d'altronde già Warren e Brandeis denunciavano che *"Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that "what is whispered in the closet shall be proclaimed from the house-tops.*[10]*"*

Vi è da dire tuttavia che, nelle intenzioni dei due giuristi di Boston, l'obiettivo era quello di costruire il right to privacy allo scopo di limitare il diritto fondamentale alla libertà di manifestazione del pensiero e non di ergerlo a diritto costituzionalmente riconosciuto[11]. L'importanza dell'opera in esame non risiede tanto nell'influenza che essa ebbe negli anni immediatamente successivi, che anzi risultò assai scarsa[12], ma

8 La fortunata espressione fu in realtà coniata dal giudice Thomas Cooley, che in un trattato del 1988 in tema di illeciti extracontrattuali, dove propose una concezione di privacy intesa come mezzo di tutela della proprietà privata dalle ingerenze altrui. Colomba, G. , Zanetti G., *Aspetti problematici della nozione di privacy da un punto di vista filosofico-giuridico,* cit., pag. 30

9 Mantelero, A. , *Il costo della privacy tra valore della persona e ragione d'impresa*, Giuffré Editore, Torino, 2007, pag. 3.

10 Warren S., Brandeis, L. , *The right to privacy* in Harvard Law Reviews, vol. IV, n.5, 1980, pag.193

11 Pizzetti, F. , *Privacy e il diritto europeo alla protezione dei dati personali: dalla Direttiva 95/46 al nuovo Regolamento Europeo,* Giappichelli editore, Torino, 2016, pag. 48.

12 L'atteggiamento della giurisprudenza americana nei confronti del tema della privacy risultava infatti oscillare tra una visione che difendeva la dimensione privata e nello specifico la privacy e una visione più ostile al riconoscimento di un autonomo diritto. Questa antiteticità ha ostacolato per molto tempo l'affermarsi di una teoria positiva in materia e allo stesso tempo non ha permesso di chiarire la natura del concetto. Si rimanda all'analisi di Miglietti, L., *Profili storico-comparativi del diritto alla privacy* in Diritti Comparati, 2014, disponibile al sito http://www.diritticomparati.it/profili-storico-comparativi-del-diritto-alla-privacy

piuttosto nell'ennesima dimostrazione dell' "eterna giovinezza"[13] del *common law* quale sistema giuridico in grado di adattarsi, aprirsi ed evolversi in ragione dei mutamenti economici, sociali e politici implicanti il riconoscimento di nuovi diritti.

Sul fronte normativo, i giudici statunitensi della prima metà del 1900 cercarono di tutelare la dimensione della riservatezza facendo leva su un'interpretazione sempre più estensiva del 4° emendamento della Costituzione americana[14]. Il cambio di passo si ebbe nel 1965 nel caso *Charles Katz vs. United States*. La vicenda si incentrava sulla legittimità o meno di alcune intercettazioni telefoniche effettuate dal FBI nei confronti del signor Katz. Sospettato di essere coinvolto in attività criminali inerenti il gioco d'azzardo, l'FBI decise di apporre una cimice all'esterno del telefono pubblico.
I giudici infatti reputarono che fosse necessario fornire una diversa lettura del IV Emendamento, che tenesse conto della circostanza per cui la privacy di un privato debba ritenersi costituzionalmente tutelata, anche qualora egli si trovi in un luogo pubblico[15], vale a dire: la tutela offerta dal IV Emendamento deve essere afferibile alle persone, e non ai luoghi[16].

In virtù della sentenza appena citata, il cambio di paradigma apportato, consente di affermare che il diritto alla privacy viene violato quando, attraverso mezzi di controllo esterno, è leso lo spazio nel quale si esplica la personalità dell'individuo[17].

Nel corso degli anni, il concetto di privacy è andato via via dilatandosi, tanto che è possibile rinvenire all'interno del contesto giuridico statunitense una classificazione più o meno condivisa: si parla di *accessibility privacy* quando ci si confronta con situazioni di tutela dinanzi a tentativi di intrusione nella sfera fisica dell'individuo; con il termine *decisional privacy* ci si riferisce invece a situazioni in cui la libertà

13 In tal senso, Pagallo, U. *La tutela della privacy negli Stati Uniti D'America e in Europa*, Giuffré Editore, Torino, pag. 64

14 Testo del IV Emendamento della Costituzione Americana (1787) *"Il diritto dei cittadini di godere della sicurezza personale, della loro casa, delle loro carte e dei loro beni, nei confronti di perquisizioni e sequestri ingiustificati non potrà essere violato; e non si emetteranno mandati giudiziari se non su fondati motivi sostenuti da giuramento o da dichiarazione solenne e con descrizione precisa del luogo da perquisire e delle persone da arrestare o delle cose da sequestrare. "*

15 Surace, M. *Analisi socio-giuridica, cit.*

16 Cassano, G. , *Stalking, atti persecutori, cyberbullismo e tutela dell'oblio,* Wolters Kluver, Assago, 2017, pag. 50

17 In tal senso, Parisi, A. G. , *E-contract e privacy* cit.

individuale è lesa da interferenze che limitano o annichiliscono le scelte e le decisioni del soggetto; infine, si ha a che fare con l'*informational privacy* quando in gioco vi sono il controllo della gestione e del trasferimento di informazioni personali[18].

Per utilizzare le parole di Mantelero, il right to privacy statunintense è divenuto *"la misura di un equilibrio relativo esistente fra individuo e società… e nel contempo un concetto che pervade il diritto di quella nazione, riaffiorando in molteplici forme".* Vale a dire: la privacy rappresenta un contenitore concettuale di difficile definizione, dove sono ravvisabili tutte quelle forme di protezione della libertà personale riservate dall'ordinamento giuridico al singolo[19].

1.2 Le esigenze per l'affermazione di un diritto alla riservatezza nel contesto europeo

Se come si è visto nell'esperienza americana, il right to privacy sorse in prima istanza come mezzo per segnare i confini tra sfera personale e diritto all'informazione, per interessare solo in un secondo momento il controllo dell'ingerenza delle attività dell'amministrazione pubblica, secondo parte della dottrina in Europa si affermò primariamente come *diritto alla protezione dei dati personali, "inteso come diritto di libertà, legato al diritto dell'individuo a non essere sottoposto a controlli e raccolta di informazioni sulla propria vita senza il suo consenso o senza che sussistano ragioni di prevenzione o repressione di reati esplicitamente previste dalle leggi"*[20].

L'esperienza del totalitarismo del '900 in Europa costituì la causa principale dell'emersione di un diritto alla riservatezza, stante il diffuso e invasivo controllo dello Stato sulla vita dei cittadini. Una lesione della dignità e della riservatezza delle persone che non trovò semplice sfogo nell'intromissione nelle conversazioni telefoniche o postali, bensì anche nell'archiviazione, nella conservazione e nel

18 Tavani, T. H. , *Ethics and Tecnology: Controversies, Questions, and Strategies for Ethical Computing,* John Wiley & Sons. Inc.,, Nashua, 2012, pag 135-136

19 Mantelero, A. , *Il costo della privacy tra valore della persona e ragione d'impresa* cit., pag. 13-14

20 Citazione tratta da Pizzetti, F. , *Privacy e il diritto europeo alla protezione dei dati personali cit.,* pag. 55

trattamento dei dati degli individui: ad esempio, noti furono i contributi in termini tecnologici che l'azienda americana IBM fornì al regime nazista per l'individuazione e la catalogazione di dati relativi alle persone di origine ebraica[21].

Nonostante questo, l'affermazione di un diritto alla riservatezza non trovò spazio nelle costituzioni europee: sebbene le carte fondamentali fossero state redatte da classi politiche di prima qualità, mancò una percezione adeguata della portata e delle conseguenze dell'incessante evoluzione dei mezzi tecnologici in relazione all'operatività dei diritti e delle libertà individuali[22].

1.3 Il diritto alla riservatezza nell'esperienza italiana

Giunti a tal punto, prima di addentrarsi nell'analisi sulla nascita e sull'evoluzione dello specifico diritto alla protezione dei dati personali, appare interessante, se non quasi necessario, compiere una panoramica sul diritto alla riservatezza all'interno dell'esperienza italiana e individuare un eventuale legame con l'esperienza statunitense descritta anteriormente.

Il diritto alla riservatezza trovò la sua prima affermazione all'interno dell'ordinamento giuridico italiano con la sentenza della Corte di Cassazione del 20 aprile 1963[23]. Controvertendo a una sentenza di qualche anno precedente,[24] la Corte affermò: *"Sebbene non sia ammissibile il diritto tipico alla riservatezza, viola il diritto*

21 *Ibidem*, pag. 54

22 Mantelero, A. , *Il costo della privacy tra valore della persona e ragione d'impresa* cit., pag. 56; M. , Gorla S., *Storia della privacy,* pag.

23 Cassaz. Civ. , sentenza n.990 del 20 aprile 1963

24 Nella controversia sorta tra gli eredi del noto tenore napoletano Caruso e Tirrenia Film, produttore del film "Leggenda di una voce", i primi si rivolsero al giudice per richiedere l'inibitoria della rappresentazione del film in questione. I giudici, negando la loro richiesta, si pronunciarono in questo modo: "*Nessuna disposizione di legge autorizza a ritenere che sia sancito, come principio generale, il rispetto assoluto dell'intimità della vita privata, tanto meno come limite della libertà dell'arte, salvo che l'operato dell'agente, offendendo l'onore o il decoro o la reputazione della persona, ricada nello schema generale del fatto illecito. Il semplice desiderio di riserbo non è stato ritenuto dal legislatore quale interesse tutelabile fuori dai casi in cui è riconosciuto espressamente un diritto della personalità"*. Vedasi il testo integrale: Cassaz. Civ., sentenza n. 4487 del 22 dicembre 1956.

assoluto di personalità, inteso quale diritto erga omnes alla libertà di autodeterminazione nello svolgimento della personalità dell'uomo come singolo, la divulgazione di notizie relative alla vita privata, in assenza di un consenso almeno implicito, ed ove non sussista, per la natura dell'attività svolta dalla persona e del fatto divulgato, un preminente interesse pubblico di conoscenza. [25]"

Come si può evincere chiaramente dalla massima sopra riportata, la Cassazione non riconobbe la tipicità del diritto alla riservatezza, ma accolse una configurazione unitaria del diritto alla personalità[26].

Nei primi anni '70 si ebbero le prime avvisaglie circa la consacrazione di un diritto alla riservatezza all'interno del panorama giuridico italiano. Con la L. 8 aprile 1974, n. 98, vennero introdotti l'art. 615-bis, il quale puniva le interferenze illecite nella vita privata, e l'art. 617-bis[27], il quale vietava l'installazione di apparecchiature atte ad intercettare o impedire comunicazioni o conversazioni. Altra normativa in un certo senso antesignana al riconoscimento del diritto alla riservatezza, fu quella introdotta nell'ambito del rapporto di lavoro subordinato dal cosiddetto Statuto dei lavoratori (Legge n. 300 del 20 Maggio 1970). Diversi sono gli articoli che sottendono a un primo tentativo da parte del legislatore di proteggere la sfera personale del lavoratore, tutelandone il diritto alla dignità e alla riservatezza: l'articolo 2 sulla regolamentazione dell'utilizzo delle guardie giurate nei locali ove si svolge l'attività

25 Il caso in questione verteva su alcune pubblicazioni effettuate dal settimanale "Il Tempo" in merito ad alcune indiscrezioni intime legate alla vita privata dell'amante del Duce, Clara Petacci.

26 Surace, M. *Analisi socio-giuridica,* cit.

27 Articolo 615-bis c.p.:

"1: Chiunque, mediante l'uso di strumenti di ripresa visiva o sonora, si procura indebitamente notizie o immagini attinenti alla vita privata svolgentesi nei luoghi indicati nell'articolo 614, è punito con la reclusione da sei mesi a quattro anni.

2.: Alla stessa pena soggiace, salvo che il fatto costituisca più grave reato, chi rivela o diffonde, mediante qualsiasi mezzo di informazione al pubblico, le notizie o le immagini ottenute nei modi indicati nella prima parte di questo articolo."

3 (...)

Articolo 617bis c.p:

1. Chiunque, fuori dei casi consentiti dalla legge [c.p.p. 266-271] , installa strumenti, parti di apparati o di strumenti al fine di intercettare od impedire comunicazioni o conversazioni telegrafiche o telefoniche tra altre persone è punito con la reclusione da uno a quattro anni.

2. (...)

produttiva, l'articolo 4 sulla proibizione all'utilizzo di impianti audiovisivi per il controllo dei dipendenti, l'articolo 5 sul divieto di accertamenti o controlli diretti da parte del datore di lavoro sulle idoneità o sulle infermità per malattia o infortuni, l'articolo 6 sullo svolgimento di visite personali di controllo. Come si può ricavare dalla lettura di questi articoli (a cui si rimanda), la tutela della dignità e della riservatezza del lavoratore costituisce lo scopo del titolo I dello Statuto dei Lavoratori. Le disposizioni della legge mirano a tutelare due aspetti diversi del diritto alla riservatezza: il primo consiste nel diritto alla non intrusione in spazi privati sia materiali sia immateriali, quali le vicende personali; il secondo mira invece a favorire un maggior controllo sulle informazioni personali del lavoratore. Tuttavia vi è da rammentare che nelle disposizioni sopra menzionate, il diritto alla riservatezza del prestatore di lavoro va bilanciato con il contrapposto interesse dell'imprenditore di essere a conoscenza di comportamenti e aspetti anche privati della vita del lavoratore, qualora essi possano in qualche modo condizionare la funzionalità della relazione contrattuale[28].

Di particolare rilievo in relazione al tema relativo al trattamento dei dati personali, appare la norma sancita dall'articolo 8, che impedisce la raccolta di materiale informativo su cui basare possibili discriminazioni[29]: l'articolo infatti afferma che *"È fatto divieto al datore di lavoro, ai fini dell'assunzione, come nel corso dello svolgimento del rapporto di lavoro, di effettuare indagini, anche a mezzo di terzi, sulle opinioni politiche, religiose o sindacali del lavoratore, nonché su fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore."* La norma in questione vieta cioè al datore di lavoro di ottenere informazioni sulla sfera privata e personale del lavoratore o aspirante tale, ove non sia giustificato dall'oggetto del contratto. Lo Statuto dei lavoratori attribuisce alla riservatezza *"natura di vero e proprio diritto indisponibile in tutti i casi in cui si supera la soglia di ciò che è legittimamente verificabile e/o conoscibile"*[30].

---

28 In tal senso, si invita alla lettura del saggio di Bellavista, A. , *Dignità e riservatezza del lavoratore* in Lambertucci, P. (a cura di), Dizionari del diritto privato. Diritto del lavoro, Giuffrè, Milano, 2010, pag. 145-153.

29 *Ibidem*, pag. 150-151

30 Citazione tratta da Chieco, P. , *Privacy e lavoro: la disciplina del trattamento dei dati personali del lavoratore*, Cacucci, Bari, 2000, pag. 12. Per un approfondimento sul tema, si rimanda a

Nonostante questi interessanti spunti normativi, indice dell'interesse da parte del legislatore di tutelare alcuni aspetti della riservatezza dei singoli. Si dovette attendere una sentenza della Corte di Cassazione del 1975 per riconoscere definitivamente l'esistenza di un autonomo diritto alla riservatezza. In una controversia relativa alla pubblicazione da parte di alcuni quotidiani di alcune fotografie ritraenti alcuni atteggiamenti intimi dell'ex imperatrice iraniana Soraya Esfandiari con un uomo all'interno della sua abitazione, i giudici sancirono che *"deve ritenersi esistente nel nostro ordinamento un generale diritto della persona alla riservatezza, inteso alla tutela di quelle situazioni e vicende strettamente personali e familiari le quali, anche se verificatesi fuori dal domicilio domestico, non hanno per i terzi un interesse socialmente apprezzabile, contro le esigenze che, sia pure compiute con mezzi leciti, per scopi non esclusivamente speculativi e senza offesa per l'onore, la reputazione o il decoro, non siano giustificate da interessi pubblici preminenti"*[31].

Uniformandosi a una pronuncia della Corte Costituzionale del 1973[32], la sentenza cita gli artt. 2, 3, 27, 29 e 41 Cost., quali norme da cui discendere i principi di "*tutela della sfera privata del soggetto con conseguenti limitazioni ad altre garanzie costituzionali quali, per esempio, il diritto all'informazione*"[33]. La Corte esaminò i tre possibili contenuti del diritto alla riservatezza: escludendo il significato troppo ristretto di diritto a essere lasciato solo legato alla tutela del domicilio, e quello al contrario troppo generico e dilatato di diritto alla privacy di matrice statunitense, i giudici finirono per adottare una concezione intermedia per la quale il diritto alla riservatezza si considera esteso anche a *"tutte quelle vicende...il cui carattere intimo è*

31 Cass. Civ. Sentenza n. 2129 del 27 Maggio 1975, GI, 1976, I, 1 970 (Massima)

32 Nella sentenza i giudici, che erano stati chiamati a pronunciarsi sulla legittimità costituzionale di alcuni articoli inerenti l'utilizzo dell'immagine altrui, affermarono che tali norme *"Non contrastano con le norme costituzionali ed anzi mirano a realizzare i fini dell'art.2 affermati anche negli art.3, comma 2, e 13, comma 1, che riconoscono e garantiscono i diritti inviolabili dell'uomo, fra i quali rientra quello del proprio decoro, del proprio onore, della propria rispettabilità,* ***riservatezza,*** *intimità e reputazione, sanciti espressamente negli art. 8 e 10 della Convenzione Europea sui diritti dell'uomo"* Corte Costituzionale, Sent. n. 38 del 12 Aprile 1973.

33 Surace, M. *Analisi socio-giuridica,* cit.

dato dal fatto che si svolgono in un domicilio ideale, non materialmente legato ai tradizionali rifugi della persona umana"[34].

Come anticipato, prima di spingersi a esaminare l'evoluzione del diritto alla riservatezza e del correlato diritto alla protezione dei dati personali nel contesto europeo degli ultimi anni, è interessante compiere un confronto tra right to privacy statunitense e diritto alla riservatezza.

Il concetto di privacy sviluppatosi negli Stati Uniti presenta innegabilmente una natura poliedrica, dal momento che si esplica in situazioni e contesti profondamente differenti: dal diritto del singolo ad impedire intrusioni dei mass media nella propria vita privata al diritto di aborto, passando per la libertà sessuale[35].

Il diritto alla riservatezza in Italia invece, essendo stato riconosciuto come valore essenziale della persona, rientra tra i diritti inviolabili della persona e quindi viene tutelato dall'articolo 2 della Costituzione: esso si manifesta in una libertà dal contenuto prettamente negativo, inteso come diritto a pretendere che nessuno violi la sfera personale di un soggetto in assenza del suo consenso[36].

1.4 Il riconoscimento del diritto alla riservatezza e del diritto alla privacy nel contesto europeo

Dal punto di vista sovranazionale europeo, si dovette aspettare la stipula della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (d'ora in avanti CEDU) per aver un primo riconoscimento, seppur parziale, del diritto alla riservatezza[37]. Nel testo dell'articolo 8 manca però un

34 Bevere, A. , Cerri, A. , *Il diritto di informazione e i diritti della persona: il conflitto della libertà di pensiero con l'onore, la riservatezza, l'identità personale,* Giuffrè Editore, Milano, 2006, pag. 130

35 Mantelero, A. , *Il costo della privacy tra valore della persona e ragione d'impresa* cit., pag 1 e ss.

36 Di Rago, G., *La privacy e le imprese,* Halley Editrice, Matelica, 2005, pag. 13 e ss.

37 L'art. 8 della CEDU recita infatti: "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*

esplicito riferimento alla protezione dei dati personali. Ciò non riduce l'importanza di queste norme, dal momento che il richiamo alla centralità della società democratica quale parametro su cui misurare la compressione del diritto individuale ha rappresentato la premessa per la futura individuazione del diritto alla protezione dei dati personali[38].

Infatti nel 1981 la Convenzione n. 108, detta Convenzione di Strasburgo, enunciò per la prima volta tutta una serie di principi ai quali gli stati firmatari dovevano adeguarsi al fine di assicurare un legittimo trattamento dei dati degli individui nei confronti di ogni elaborazione automatizzata di dati concernenti soggetti identificati o identificabili[39]. All'interno della convenzione particolare interesse assume anche l'articolo 2 che definisce i concetti di "dati personali" e "elaborazione automatizzata", su cui ci si soffermerà in seguito.

Proprio negli anni '80, in virtù del nuovo contesto sociale, economico, culturale e tecnologico dettato dall'avvento della società dell'informazione digitale, le istanze e le esigenze di tutela della sfera personale si moltiplicarono.

Malgrado l'approvazione da parte del Consiglio D'Europa della Convenzione n. 108, all'interno della Comunità Europea fino al 1995 non si provvedette alla formulazione di alcuna disciplina sul tema della protezione dei dati personali. Tale ritardo fu strettamente imputabile agli avvenimenti che stavano caratterizzando gli anni '90 e che stavano portando progressivamente alla costruzione dell'attuale impianto dell'Unione Europea. Nello specifico, due essenzialmente furono le problematiche connesse alla mancata adozione di una regolamentazione sul tema in oggetto: in primo luogo, con l'entrata in vigore del Trattato di Maastricht nel 1993 vi fu l'abbattimento di ogni controllo doganale tra le frontiere degli stati aderenti; in secondo luogo, con la Convenzione di Schengen allo stesso modo si ebbe la caduta di ogni controllo relativo alle persone fisiche. Con la cancellazione di queste frontiere, si

reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui."

38 Pizzetti, F. , *Privacy e il diritto europeo alla protezione dei dati personali* cit., pag. 58

39 L'articolo 1 della Convenzione di Strasburgo recita: *"Scopo della presente Convenzione è quello di garantire, sul territorio di ciascuna Parte, ad ogni persona fisica, quali che siano la sua nazionalità o la sua residenza, il rispetto dei suoi diritti e delle sue libertà fondamentali, e in particolare del suo diritto alla vita privata, in relazione all'elaborazione automatica dei dati a carattere personale che la riguardano".*

ponevano numerose incognite in termini di applicazione di normative relative ai dati personali, in virtù del fatto che ogni Paese possedeva (o non possedeva) una normativa al riguardo. A seguito delle trattative che durarono circa 5 anni, nel 1995 gli sforzi profusi dagli Stati sfociarono nella direttiva 95/46, che venne a costituire il primo tentativo di regolamentazione comune europea[40]. Al fine di provvedere al corretto funzionamento del mercato interno e quindi alla libera circolazione di merci, persone, servizi e capitali, la direttiva intendette assicurare la libera circolazione[41] dei dati personali da uno Stato all'altro, senza che ne venissero lesi i diritti fondamentali della persona[42].

L'effetto principale di questa Direttiva fu sicuramente l'affermazione del principio del mutuo riconoscimento fra i diversi Paesi membri: in ogni Paese dell'Unione si applicava la legge di protezione dei dati del Paese in cui aveva sede lo stabilimento principale del titolare del trattamento. In questo modo le frontiere immateriali esistenti tra i vari paesi vennero eliminate, o meglio vennero spostate sulla base dei confini dell'Unione Europea: i vincoli e le condizioni della Direttiva resero difficili i rapporti con i Paesi Extra-UE che non assicuravano le medesime garanzie in tema di protezione dei dati personali[43].

Da queste considerazioni, è facile comprendere la funzione "ancillare" che rivestì la direttiva 95/46 nei confronti del corretto funzionamento del mercato interno, o meglio del principio di liberazione circolazione di merci, servizi, persone e capitali: era necessario che ogni paese convergesse verso l'adozione interna della nuova disciplina affinché divenisse pienamente efficace la Convenzione di Schengen. La direttiva fu a lungo considerata un'imposizione di Bruxelles, più che una significativa

40 Pizzetti, F. , *Privacy e il diritto europeo alla protezione dei dati personali* cit., pag. 64 e ss.

41 I flussi di dati oggetto dell'attenzione della Direttiva erano principalmente dovuti a tre situazioni. In primis, l'implementazione di un mercato interno aveva fatto aumentare i flussi transfrontalieri di dati personali tra tutti i soggetti della vita economica e sociale degli Stati; in secondo luogo, l'intercambio di dati tra le imprese private era anch'esso accresciuto sensibilmente; in terzo luogo, le amministrazioni pubbliche dei vari paesi avevano l'obbligo di collaborare e scambiarsi dati personali in applicazione del diritto comunitario. Ziccardi, G. , *Informatica giuridica: privacy, sicurezza informatica, computer forensics e investigazioni digitali (Seconda edizione),* Giuffrè Editore, Milano, 2012, pag. 118.

42 Si rinvia al Considerando n.3 della direttiva 95/46.

43 Pizzetti, F. , *Privacy e il diritto europeo alla protezione dei dati personali* cit., pag. 66

presa di posizione sulla scia di quanto affermato con la Convenzione n. 108. Lo testimonia la divergenza di vedute circa l'effettivo inquadramento del diritto alla protezione dei dati : se da un lato i Garanti della privacy nazionali (autorità indipendenti introdotte dalla direttiva) affermavano con convinzione che la protezione dei dati personali costituisse un diritto fondamentale, dall'altro lato le imprese, destinatari principali della normativa, negarono con forza che la sola Direttiva fosse sufficiente per elevare la protezione dei dati a un livello giuridico sovrastante[44].

La disputa sulla qualificazione giuridica da fornire al diritto alla protezione dei dati personali fu risolta con la sottoscrizione della Carta di Nizza (si ricorda che con il Trattato di Lisbona le è stato attribuito lo stesso valore dei Trattati), che all'articolo 8 comma 1 sancisce che *"Ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano[45]".* Tale disposizione fu poi ripresa all'articolo 1 dal "Codice della Privacy" (D. lgs. 30 Giugno 2003). Con tale atto, il Legislatore intese coordinare in forma sistematica le norme previgenti, abrogando la legge del 1996 e inglobando tutte le disposizioni normative in materia. Scopo della legislazione della privacy non fu quello di impedire o limitare la circolazione delle informazioni all'interno della società, bensì assicurare che tali informazioni corrispondessero alla realtà e che venissero diffuse negli ambiti pertinenti[46]: si affermava il principio per cui i dati personali andavano tutelati in ragione del valore sociale dell'individuo.

Al fine di comprendere la portata del Codice e in generale tutto l'impianto della privacy che analizzeremo, è importante chiarire alcune nozioni basilari, quali dati personali, trattamento di dati personali, dati sensibili, comunicazione e diffusione.

Alla stregua dell'articolo 4, comma 1, lett. b), per dato personale si intende *"qualunque informazione relativa a persona fisica, persona giuridica, ente od*

---

44 *Ibidem*, pag. 68; sul punto si osservi anche il caso Olcese Cassazione Civ.. Sez. I, 30 giugno 2001, n. 8889, testo rintracciabile al sito http://www.privacy.it/archivio/cassaz20010630.html

45 Per completezza, è utile riportare anche il 2° e 3° comma dell'articolo in questione: *"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 Ł soggetto al controllo di un'autorità indipendente. "*

46 Di Rago, G., *La privacy e le imprese* cit., pag. 14

associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale". Di particolare importanza sono: i dati che permettono l'identificazione, come per esempio i dati anagrafici (nome e cognome) e i dati che permettono un'identificazione indiretta, come ad esempio il codice fiscale o il numero di targa; i dati cosiddetti sensibili, vale a dire quelli che rilevano l'origine etnica o razziale, le convinzioni religiose, filosofiche, le opinioni politiche, l'appartenenza sindacale; i dati giudiziari, riguardanti condanne penali e reati.

Con il termine "trattamento", ci si riferisce a *"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" (art 4, comma 1 lett. a).*

I termini *"comunicazione"* e *"diffusione"* concernono il dare conoscenza dei dati personali, anche mediante messa disposizione o consultazione, a uno o più soggetti determinati diversi dall'interessato, o a soggetti indeterminati nel secondo caso.

Dal punto di vista soggettivo, il Codice riporta anche altre tre nozioni che vanno spiegate: il "titolare del trattamento" è *la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordina alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza" (art. 4, comma 1, lett. f); "*l'interessato" *è "la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali" (art. 4, comma 1, lett. i);* il responsabile è invece *"la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali (art. 4, comma 1, lett. i).*

Per quanto concerne i principi introdotti dal decreto legislativo, indubbiamente vi fu il principio di necessità[47], in base al quale le informazioni personali dovevano

47 Il principio in esame viene integrato da quanto disposto dall'art. 11, per il quale: "1. I dati personali oggetto di trattamento sono:

a) trattati in modo lecito e secondo correttezza;

essere consentite soltanto per il raggiungimento di finalità esplicite e rese note all'interessato, ed utilizzate soltanto per il tempo strettamente necessario (art.3): l'identificazione dell'interessato poteva avvenire solo quando non esistevano altre modalità meno invasive per perseguire le medesime finalità[48].

In relazione all'ambito oggettivo di applicazione, l'articolo 5 richiamava "il criterio dello stabilimento territoriale" del soggetto che effettuava il trattamento. Quindi, nel caso in cui un istituto di credito con filiali estere avesse effettuato operazioni di trattamento sui dati personali di un soggetto, aveva l'onere di assicurarsi che le filiali in questione rispettassero la normativa italiana.

Altro principio da sottolineare all'interno del Codice fu quello relativo al trasferimento dei dati all'estero, ove bisognava distinguere tra Paesi appartenenti all'Unione europea e paesi extra-UE. Nel primo caso come già anticipato dalla direttiva 95/46, l'articolo 42 ribadiva che il trattamento dei dati personali era soggetto al principio di libera circolazione, motivo per cui non era possibile porre in essere ostacoli atti a limitare o impedire il trasferimento di dati. Nel secondo caso invece, da un lato l'articolo 45 vietava il trasferimento di dati nei casi in cui l'ordinamento dello stato di destinazione non assicurasse un livello adeguato di tutela delle persone, mentre dall'altro lato l'articolo 43 poneva tutta una serie di condizioni senza le quali non era possibile procedere al trasferimento di dati personali[49].

b) raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi;

c) esatti e, se necessario, aggiornati;

d) pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;

e) conservati in una forma che consenta l'identificazione del5 Codice in materia di protezione dei dati personali l'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

2. I dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati.

48 Iaselli, M. , *Il Codice della Privacy: una lettura ragionata*, lulu.com, 2011, pag. 4-5

49 Si riportano sinteticamente le condizioni indicate dall'articolo 43 del Codice della Privacy per le quali è consentito trasferire dati personali in un Paese non appartenente all'UE:
a) se esiste un consenso espresso dell'interessato (scritto se si tratta di dati sensibili)

b) se è necessario per l'esecuzione di obblighi derivanti da un contratto del quale è parte l''interessato

Per quanto riguarda l'introduzione dei diritti in capo all'interessato, l'articolo 7 del Codice prevede in prima istanza che l'interessato abbia diritto alla conferma dell'esistenza o meno di dati personali in possesso di un determinato soggetto privato o pubblico: in particolare, ha diritto a ottenere l'indicazione dell'origine dei dati personali, delle finalità e modalità del trattamento, della logica applicata in caso di trattamento elaborato con strumenti elettronici, degli estremi identificativi del titolare dei responsabili e del rappresentato disegnato al trattamento, dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati (Art 7, c.2). Inoltre, ex art.7 c.3 l'interessato ha diritto di ottenere: l'aggiornamento, la rettificazione o integrazione dei dati; la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge; il diritto di opporsi per motivi legittimi al trattamento dei dati personali che lo riguardano e al trattamento di dati personali che lo riguardano a fini di invio di materiale pubblicitario, vendita diretta o ricerche di mercato.

1.5 Differenza concettuale tra riservatezza, privacy e protezione dei dati personali

Prima di addentrarsi nell'analisi del Regolamento UE 2016/679, è utile cercare di far chiarezza, per quanto possibile, sull'uso e sul significato dei termini riservatezza, privacy e protezione dei dati personali (*o data protection*).

Nel tentativo di delimitare i confini delle tre nozioni, si può in primo luogo affermare che la riservatezza può essere definita come un *"modo di essere negativo della persona rispetto agli altri soggetti"* che "*soddisfa quel bisogno di ordine spirituale che consiste nell'esigenza di isolamento morale, di non comunicazione esterna di quanto*

c) se è necessario per la salvaguardia di un interesse pubblico rilevante individuato da legge o regolamento

d) se è necessario per la salvaguardia della vita o dell'incolumità fisica di un terzo

f) se è effettuato in accoglimento di una richiesta di accesso ai documenti amministrativi

g) se è necessario, in conformità ai rispettivi codici deontologici, per esclusivi scopo scientifici o statistici o in alcuni casi per scopi storici.

attiene all'individua persona; costituisce quindi una qualità morale della persona stessa[50]". Premesso questo, esiste un orientamento che mira a far coincidere il concetto di privacy con quello di riservatezza e a declinarlo come *"diritto di mantenere il controllo sulle proprie informazioni*[51]*", "che si concretizza nella libertà di mantenere il controllo sul flusso dei dati e delle informazioni che riguardano e identificano l'individuo, in modo che l'informazione oggetto di trattamento rispecchi fedelmente l'attuale, integrale ed effettiva identità personale dell'interessato*[52]*".* In sintesi, tale orientamento si manifesta in una tendenza volta a configurare privacy e riservatezza in una relazione di fungibilità, giacché l'elemento comune a entrambe risiede nell'intenzione di escludere uno o più soggetti dal venir a conoscenza di determinate informazioni personali[53].

Negli ultimi anni, è andata prendendo piede un'ulteriore prospettiva di tipo funzionale, che tende a distanziare la nozione di privacy dalla sfera della riservatezza e a identificarla sostanzialmente con il diritto alla protezione dei dati personali[54]. La prova di questa affermazione risiede nel comma 1, art 2 del D. Lgs. n. 196/2003 che dispone che ogni trattamento di dati personali deve effettuarsi nel rispetto dei diritti e delle libertà fondamentali della persona, nonché della sua dignità, *"..con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali".* In questo modo, il legislatore ha riportato il diritto alla riservatezza al suo significato originario, ossia a quello di libertà dal contenuto principalmente negativo, mentre il diritto alla protezione dei dati personali, o privacy, assume una

50 Seguendo tale orientamento, il diritto alla riservatezza è stato collocato all'interno dei diritti della personalità e qualificato come diritto a una vita intima. Sul punto citato, vedasi l'illuminante opera di De Cupis, A., *I diritti della personalità*, Giuffré Editore, Milano, 1973, pag. 256-257

51 Rodotà, S., T*ecnologie e diritti*, Il Mulino, Bologna, 1995, pag. 122

52 L. Ferola, *Dal diritto all'oblio al diritto alla memoria sul web. L'esperienza applicativa italiana*, in Diritto dell'Informazione e dell'Informatica, Vol. 28, n°6, 2012, pag. 1001

53 Gardini, G., *Le regole dell'informazione: l'era della post-verità,* Giappichelli Editore, Torino, 2017, pag. 292

54 Tra i vari, si menzionano Di Rago, G., *Le privacy e le imprese* cit., pag. 13; Finocchiaro G, *La protezione dei dati personali e la tutela dell'identità*, In Delfini F., Finocchiaro G., *Diritto dell'informatica*, Utet Giuridica, Milano, 2014, pag. 151 e ss.; Falletti E., *L'evoluzione del concetto di privacy e della sua tutela giuridica* in Cassano, G., Scorza, G., Vaciago, G., *Diritto dell'internet. Manuale Operativo., Casi Legislazione, Giurisprudenza,* CEDAM, Milano, 2012, pag. 22 e ss.

connotazione positiva, consistente nel potere di controllare e intervenire sul flusso di informazioni che riguardano la propria persona[55].

Un terzo filone di pensiero[56] ha avanzato l'idea per cui la data protection, sebbene riguardi indubbiamente la privacy, non può consumarsi nel diritto al controllo delle "informazioni private", ma si estende *"alla tutela di ogni informazione riferita o riferibile a una persona identificata o identificabile, quale che ne sia il contenuto o l'oggetto"*[57]. A sostegno di questa tesi, sembra essere la giurisprudenza della Corte di Giustizia dell'Unione Europea, la quale nella sentenza *Maximilian Schrems c. Data Protection Commissioner* propende per differenziare privacy e data protection,, riconoscendo nel primo un diritto ad aver uno spazio privato libero da altrui ingerenze, mentre nel secondo un diritto al corretto trattamento dei propri dati personali, indipendentemente dal fatto che essi siano privati. L'elemento dirimente tra le nozioni di diritto alla riservatezza e il diritto alla privacy, coincidenti secondo questo orientamento, e il diritto alla protezione dei dati personali, si rivela essere la portata esclusivamente individualistica dei primi rispetto alla duplice natura del secondo [58]. In tal senso, si osserva che la disciplina della raccolta e del trattamento dei dati personali non può ridursi "*a una cifra individualistica*[59]", dal momento che coinvolge o addirittura finisce per scontrarsi con garanzie di trasparenza e legalità preposte al funzionamento di altri sistemi, quali ad esempio il corretto funzionamento del mercato che per l'appunto verrà preso in esame in questa tesi.

Si può dedurre quindi che tra riservatezza o privacy e protezione dei dati personali sussista un rapporto di specialità bilaterale o reciproca, in quanto la prima protegge la vita privata anche al di fuori del contesto del trattamento dei dati, mentre la seconda tutela la correttezza del trattamento dei dati personali[60], a prescindere che questo influisca sulla sfera privata dell'individuo.

55 Di Rago, G., *La privacy e le imprese,* pag. 14 e ss.

56 In particolare, si rimanda a Lamanuzzi, M., *Diritto penale e trattamento dei dati personali. Codice della privacy, novità introdotte dal regolamento UE 2016/679 e nuove responsabilità per gli enti* in JusOnline, 2017, n.1, pag. 218 e ss.

57 Pizzetti. F., *Privacy e il diritto europeo alla protezione dei dati personali* cit., pag. 45

58 Lamanuzzi, M., *Diritto penale e trattamento dei dati personali* cit., pag. 222-223.

59 Rodotà, S., T*ecnologie e diritti* cit., pag. 19 e ss., 101 e ss.; il diritto alla proteione dei dati personali protegge l'informazione riferita e il suo uso, ma non la personalità dell'individuo nel suo complesso. Pisapia, A., *La tutela per il trattamento e la protezione dei dati personali,*

A parere di chi scrive, la tesi appena riportata appare la più condivisibile in ragione del valore dinamico e funzionale che viene attribuito alla disciplina della *data protection.* Questo non significa asserire che i due istituti non abbiano punti di contatto o talvolta di sovrapposizione: affermare ciò, significherebbe sminuire il dettato legislativo dell'articolo 2, comma 1 del decreto legislativo e la relativa tendenza a identificarlo con l'espressione "Codice della Privacy".

La privacy è il diritto di scegliere quali aspetti, fatti o caratteristiche del nostro spazio personale rendere conoscibili agli altri. Per chiarire il concetto è utile esemplificare: se una persona volontariamente esibisce una spilla di appartenenza a un determinato partito politico, è conscio del fatto che egli rinuncia alla segretezza dell'informazione sul suo credo politico; viceversa, se l'azienda presso quale lavora tale individuo, redige un archivio per classificare i dipendenti per la loro appartenenza politica basandosi sul fatto di aver esibito volontariamente una spilla, non si configura nessuna violazione della privacy, bensì entra in gioco la protezione dei dati personali e quindi sarà necessario analizzare le finalità dell'azione dell'azienda e l'esistenza o meno del consenso in capo al lavoratore. D'altro canto infatti, la normativa sulla protezione dei dati personali si applica qualora vengano utilizzati sistemi di archiviazione: il considerando n. 15 del GDPR afferma che *"La protezione delle persone fisiche dovrebbe applicarsi sia al trattamento automatizzato che al trattamento manuale dei dati personali, se i dati personali sono contenuti o destinati a essere contenuti in un archivio".*

1.6 Considerazioni preliminari sulla protezione dei dati personali alla luce del Regolamento 2016/679

Il 25 Maggio 2018, dopo due anni dall'approvazione del Parlamento Europeo, è entrato in vigore il Regolamento UE 2016/679, più noto come General Data Protection Regulation (GDPR). Il GDPR è stato pensato in un'ottica completamente differente rispetto a quelle adottate in passato, poiché l'accento è stato posto sul ruolo fondamentale che i dati personali rivestono nel nostro sistema, qualificati dalla nuova

60 Tale teoria è supportata nell'articolo di Lamanuzzi, M., *Diritto penale e trattamento dei dati personali* cit., pag. 223.

normativa quali diritti fondamentali dell'uomo. Per utilizzare un'efficace espressione di Rosario Cerra, Presidente del Centro Economia Digitale, l'introduzione del GDPR rappresenta "una vera rivoluzione copernicana"[61]. Negli ultimi anni infatti il problema emerso è quello della trasformazione delle persone da consumatori a produttori di dati, i quali hanno acquisito valore economico e sociale meritevole di tutela. Per questa ragione, il Regolamento ha cercato da un lato di responsabilizzare maggiormente chi gestisce i dati, e dall'altro di render maggiormente consapevoli i cittadini.

Come anticipato nell'introduzione di questo progetto, lo scopo principale dei redattori del GDPR è stato quello di architettare una disciplina in grado di rimanere al passo con i tempi, o meglio al passo con l'incessante emersione di nuovi strumenti tecnologici. Per questa ragione, il GDPR non offre modelli standard, generici e predefiniti, ma lascia al singolo il compito di determinare quali siano le misure, tecniche e le strategie organizzative che riescano a garantire la protezione del dato personale[62].

Il Regolamento si presenta come un sistema di norme globali e uniformi che valorizzano le varie rappresentazioni concettuali del dato personale, quale: oggetto di trattamento, componente del patrimonio informativo circolante, portatore di valore economico, portatore di valore morale. L'esigenza dell'interessato in relazione a queste sfaccettature del dato personale è quello di detenerne il potere di gestione, oltre a esigerne la protezione da eventuali abusi. Per garantire l'efficacia duratura di questo sistema, è stato predisposto un meccanismo flessibile di interazione tra diritti fondamentali: se da un lato, il GDPR afferma il diritto alla protezione dei dati personali quale diritto fondamentale "*considerato alla luce della sua funzione sociale*" (considerando 1), dall'altro lato questo interagisce con tutti gli altri diritti e libertà fondamentali riconosciuti dalle norme europee (diritto di cronaca, diritto di informazione, libertà d'impresa…) in ossequio al principio di proporzionalità (considerando 4).

61 Si rimanda a https://www.privacyitalia.eu/gdpr-rivoluzione-copernicana/7825/

62 Per ulteriori considerazioni si rinvia genericamente a De Stefani, F., *Le regole della privacy: guida pratica al nuovo GDPR,* Hoepli Editore, Milano, 2018.

Quest'opera di bilanciamento e armonizzazione tra diritti differenti, non significa tuttavia scoraggiare la circolazione dei dati nell'economia digitale. La protezione dei dati va collocata in un contesto collettivo, ove "sale alla ribalta" la funzione sociale della tutela in esame[63]. Per conciliare quindi lo sviluppo dell'economia digitale con il tema dei dati personali, è stato necessario predisporre una "tutela anticipata", che trova nel concetto di *privacy by design*[64] la sua traduzione operativa. Essa consiste nel fatto che la tutela dei dati personali deve essere tenuta in conto fin dalla progettazione dell'attività o del progetto predisposto da un'impresa privata o da un ente pubblico: si tratta di un sistema basato sul principio di prevenzione (e non di correzione) dei rischi per cui il titolare del trattamento deve adottare misure tecniche e organizzative atte a garantire il rispetto del Regolamento, individuando i mezzi da utilizzare e le modalità di trattamento idonei[65].

Accanto a tale tutela, è necessario menzionare anche la c.d. *privacy by default:* con tale espressione il legislatore europeo ha voluto stabilire che la protezione dei dati personali sia garantita come "impostazione predefinita" (art 25, c. 2). Ne discende che tutte le valutazioni che il titolare del trattamento deve effettuare in tema di protezione dei dati personali devono essere compiute a monte, adottando un approccio pratico realizzabile in una serie di tecniche specifiche e diversificate, quali possono essere la pseudonimizzazione, la minimizzazione dei dati trattati, la trasparenza effettiva su finalità e modalità di raccolta dei dati.

---

63 Pizzetti, F., (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Giappichelli Editore, Torino, 2018, pag. 52

64 Si riporta il testo del comma 1 dell'articolo 25 del Regolamento UE 2016/679: "*Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati. "*

65 Per approfondimenti si rimanda a Naldi, M., D'Acquisto G., *Big data e Privacy by design,* Giappicheli Editore, Torino, 2017.

Rimandando le considerazioni in merito alle future prospettive applicative del GDPR e il relativo approfondimento sul bilanciamento tra la tutela dei dati personali e altri diritti fondamentali, alla luce dell'oggetto di questa tesi preme sottolineare l'importanza della disciplina del diritto alla cancellazione dei dati personali (più comunemente, e per taluni erroneamente, chiamato diritto all'oblio) istituita dal Regolamento. L'articolo 17 stabilisce che *"L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali",* salvo la sussistenza di ragioni specifiche che limitano tale diritto.

L'esercizio di tale potere appare oramai indispensabile nell'era digitale, ove il largo utilizzo di strumenti tecnologici e la perenne e quasi inconsapevole condivisione di informazioni personali mettono a rischio gli ambiti privati della vita personale o agevolano pratiche commerciali illecite tese alla massimizzazione del profitto. Per comprendere la natura relativa di questo diritto, nei prossimi capitoli si ripercorrerà la storia della sua evoluzione attraverso alcune sentenze della Corte di Giustizia Europea.

CAPITOLO II: Il caso Google Spain: una "costellazione complessa" di diritti fondamentali contrastanti

Sommario: • 2.1 Natura e accezioni del diritto all'oblio • 2.2 Il caso Google Spain • 2.3 Luci ed ombre della Sentenza Google Spain • 2.4 Sviluppi recenti in tema di diritto all'oblio e ambito di applicazione: Google vs. CNIL

2.1 Natura e accezioni del diritto all'oblio

Come è stato anticipato nel primo capitolo, il diritto all'oblio viene connesso e oramai ancorato al novero dei diritti relativi alla protezione dei dati personali. Per utilizzare le parole di un autore *"esso è generalmente considerato come un diritto che, fin dal suo sorgere, si configura come un aspetto puntuale del diritto all'autodeterminazione informativa e al controllo sull'uso che viene fatto dei dati personali compreso il diritto a chiederne la cancellazione quando ne ricorrano le condizioni"*[66].

Tuttavia, compiendo una riflessione più ampia e approfondita sulla natura di tale diritto, in relazione alle categorie concettuali analizzate precedentemente, bisogna constatare che nelle originarie formulazioni, esso si manifesta come diritto legato al rispetto della dignità e alla riservatezza personale in aperto e permanente contrasto con il diritto alla libertà d'informazione e libera manifestazione di pensiero. Tradizionalmente il suddetto diritto si riferisce alla prerogativa di un soggetto di non vedere pubblicate notizie relative a vicende personali già pubblicate in precedenza e riproposte trascorso un notevole lasso di tempo. In tale accezione, il problema risiede nel comprendere quando e se vicende legittimamente pubblicate possano essere riproposte o se lo scorrere del tempo, in un certo senso, renda illecita tale pratica[67]. Secondo un'illuminante definizione di Ferri, il diritto all'oblio appartiene "alle ragioni e alle regioni del diritto alla riservatezza"[68].

66 Pizzetti, F., *Il caso del diritto all'oblio*, Giappichelli Editore, Torino, 2013, pag. 30

67 Resta, G. , Zencovich, V. Z., *Il diritto all'oblio su internet dopo la sentenza Google Spain,* RomaTre-Press, Roma, 2015, pag. 30

68 Ferri, G.B., *Diritto all'informazione e diritto all'oblio* in Riv. Dir. Civ., n. I, 1990, pag. 808 e ss.

A tal punto è interessante riportare le considerazioni elaborate da Roberto Pardolesi[69]. Secondo l'autore, il diritto all'oblio presenterebbe due anime, una di matrice domestica e una di matrice eurounitaria, le quali pur essendo entrambe di natura giurisprudenziale, non possono risolversi in unico concetto.

La prima versione si interseca con il diritto alla riservatezza. In aperto contrasto con il diritto di cronaca, l'aspirazione all'oblio si origina attorno a vicende che precedentemente avevano catturato l'attenzione del pubblico e si basa sul principio per cui l'interesse pubblico alla conoscenza di un fatto debba affievolirsi fino a dissolversi con il trascorrere del tempo: in poche parole, il fatto divenuto pubblico riacquista con il tempo la sua natura di fatto privato[70]. Tale impostazione ha trovato la sua legittimazione soprattutto con la sentenza n. 3679 del 1998 della Cassazione, con cui si è stabilito che ai tradizionali criteri di verità, pertinenza e continenza che devono sussistere al momento della pubblicazione di una notizia, vada aggiunto anche quello dell'attualità della notizia, quale manifestazione del diritto alla riservatezza, *inteso come l'interesse di ogni persona a non restare indeterminatamente esposta ai danni ulteriori che arreca al suo onore e alla sua reputazione la reiterata pubblicazione di una notizia in passato legittimamente divulgata*[71].

Seppur tale versione domestica del diritto all'oblio appaia più "semplice" nella sua interpretazione e nel suo bilanciamento tra interesse pubblico e interesse privato, tuttavia non sono mancate negli ultimi anni pronunce giurisprudenziali che hanno minato tale percezione.

Per quanto concerne invece la versione eurounitaria del diritto all'oblio, essa prende origine dall'attività dell'autorità spagnola per la protezione dei dati in relazione alle richieste di rimozione di links di articoli di stampa pervenutele a partire dal 2010.

E' evidente che l'attività giornalistica è stata profondamente segnata dallo sviluppo di Internet, considerata la possibilità di circolare e diffondere opinioni, fatti e dati in maniera trasversale e costante. La conseguenza è che è divenuto estremamente

69 R. Pardolesi, *L'ombra del tempo e (il diritto al)l'oblio*, in "Questione giustizia", Riv. Trim., n.1, 2017, pp. 76-85

70 I*bidem.*

71 Massima della sentenza della III Sezione della Cass. Civ., n. 3679 del 9 Aprile 1998.

complicato l'esercizio del diritto all'oblio in quanto le legittime richieste di cancellazione o aggiornamento devono prender in considerazione tutti i luoghi virtuali in cui tale informazione è stata veicolata (sito, copia cache della pagina web, sull'indicizzazione dei risultati dei motori di ricerca).

Tale orientamento di più ampio respiro europeo si concentra quindi sul coniugare le esigenze individuali del diritto all'oblio con la disciplina relativa alla protezione dei dati personali. Il caso Google Spain rappresenta indubbiamente il punto più significativo, ma anche controverso dell'affermazione di tale diritto, giacché nel contesto digitale la definitiva eliminazione di contenuti relativi a dati personali risulta impresa ardua: la rete non dimentica mai. Il diritto al controllo dei propri dati personali sembra al momento infrangersi contro il muro invalicabile della tecnica[72]. Del resto, già nel 1955 il filosofo tedesco Martin Heidegger ammoniva sui pericoli della tecnica (tecnologia): *"Il mondo si trasforma in un completo dominio della tecnica. Di gran lunga più inquietante è che l'uomo non è affatto preparato a questo radicale mutamento del mondo[73]".*

2.2 Il caso Google Spain

Il 5 Marzo 2010, il sig. Costeja Gonzalez presentò un reclamo all' *Agencia Española de Protección de Datos (AEPD)* contro il quotidiano catalano La Vanguardia e contro Google Spain e Google Inc. L'attore lamentava il fatto che, qualora un utente di Internet introducesse il suo nome completo nel motore di ricerca di Google, i risultati evidenziavano link verso due pagine del quotidiano contenenti due articoli rispettivamente del 19 Gennaio e del 9 Marzo 1998. In tali articoli, figurava un annuncio per una vendita all'asta di immobili connessa ad un pignoramento effettuato per la riscossione coattiva di crediti previdenziali ai danni del sig. Costeja Gonzalez.

72 Finocchiaro, G., Delfini, G. (a cura di), *Diritto dell'informatica*, Utet Giuridica, Milano, 2014,pag. 151 e ss.

73 Per una riflessione più approfondita sul rapporto tra tecnica e uomo, si veda Heidegger, M, *La questione della tecnica,* GoWare, Firenze, 2017. La critica dell'autore non può essere banalizzata come una semplice avversione allo sviluppo tecnologico, bensì come un avvertimento nel considerare l'essenza della tecnica come una questione eminentemente metafisica.

Quest'ultimo chiedeva in primo luogo che fosse ordinato al quotidiano La Vanguardia di sopprimere o modificare le pagine in questione di modo che i suoi dati personali non apparissero più; in secondo luogo, chiedeva che fosse ordinato a Google Spain e Google Inc. di eliminare od occultare i suoi dati personali, affinché non comparissero più tra i risultati della ricerca. Dal momento che il pignoramento effettuato nei confronti del sig. Gonzalez, era stato interamente risolto, egli argomentava che non sussisteva più alcuna ragione per cui, a distanza di dodici anni, continuasse a rimanerne traccia in Internet.

Con la decisione del 30 Luglio 2010, l'Agenzia spagnola ha respinto il reclamo presentato nei confronti del quotidiano, dal momento che la pubblicazione delle informazioni relative al pignoramento era stato fatto in ottemperanza a un ordine del Ministero del Lavoro e degli Affari sociali, e quindi in conformità alla legge, allo scopo di conferire massima pubblicità alla vendita pubblica e quindi garantire la più ampia partecipazione possibile all'asta. L'AEPD accoglieva invece il reclamo diretto a Google, ritenendo i gestori di motori di ricerca assoggettati alla normativa in materia di protezione dei dati personali, stante la loro funzione di intermediari. Inoltre, l'autorità spagnola si arrogò il potere di rimuovere e di vietare l'accesso a taluni dati dati gestiti dai motori di ricerca, qualora si possa ritenere che la localizzazione e la diffusione degli stessi possano violare il diritto fondamentale alla protezione dei dati e la dignità delle persone.

Di rimando, Google Spain e Google Inc. depositarono due ricorsi separati, poi riuniti, dinanzi all' Audiencia Nacional[74]. Stante la necessità di interpretare la direttiva 95/46 alla luce delle nuove tecnologie emerse successivamente alla sua adozione, il giudice decise di rinviare la decisione alla Corte di Giustizia Europea, chiedendo quali obblighi sussistessero in capo ai gestori di motori di ricerca per la tutela dei dati personali delle persone interessate[75].

L' Audiencia Nacional sospese il procedimento e sottopose alla CGE tre questioni pregiudiziali.

74 L' *Audiencia Nacional* è un tribunale spagnolo con sede a Madrid che ha giurisdizione in tutto il territorio nazionale. E' un tribunale che funge sia come corte d'appello sia come giudice di prima istanza nelle materie che la Ley Organica del Poder Judicial elenca.

75 Vedasi la Causa C-131/12. della Corte di Giustizia Europea del 13 Maggio 2014, par. 15-19.

La prima verteva sull'ambito territoriale di applicazione della direttiva 95/46, vale a dire se fosse possibile ritenere che la succursale spagnola di Google fosse responsabile del trattamento dei dati personali alla luce di uno dei tre criteri di collegamento indicati alle lettere a), b) e c) dell'articolo 4 della direttiva[76].

La seconda questione pregiudiziale consisteva nel comprendere se l'attività di Google (localizzazione delle informazioni, indicizzazione, memorizzazione temporanea e messa a disposizione a terzi secondo un determinato ordine di preferenza) fosse da ricomprendersi nella nozione di "trattamento di dati" ai sensi dell'articolo 2, lett. b) della direttiva.

La terza questione invece faceva riferimento al diritto alla cancellazione e/o opposizione al trattamento di dati in relazione al diritto all'oblio. Il giudice spagnolo chiedeva se i diritti di cancellazione e congelamento dei dati (art. 12, lett b) e il diritto di opposizione al trattamento (art. 14, 1° co., lett. a) della direttiva 95/46, implicassero che l'interessato potesse rivolgersi ai motori di ricerca per bloccare l'indicizzazione delle informazioni personali sul web qualora ritenesse che esse recassero pregiudizio alla sua persona o che fossero semplicemente dimenticate.

I giudici della CGE attribuirono a Google una responsabilità in merito a tutte le tre questioni sollevate.

---

76 Si riporta il testo dell'articolo 4 della direttiva 95/46.

Diritto nazionale applicabile

"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."

Relativamente all'aspetto della territorialità, i giudici disposero che per estendere la giurisdizione europea in un determinato paese membro, è sufficiente che il trattamento delle informazioni personali sia effettuato *"nel contesto delle attività*[77] *di tale stabilimento qualora quest'ultimo sia destinato a garantire in tale Stato membro, la promozione e la vendita degli spazi pubblicitari proposti dal suddetto motore di ricerca..."*. La conseguenza pratica di tale decisione è l'applicabilità del diritto comunitario, sebbene Google Spain risulti una filiale di un'organizzazione con sede legale in California. Sulla nozione di stabilimento, la stessa Corte confermò tale orientamento nella sentenza Weltimmo, decretando l'impossibilità di interpretare restrittivamente l'espressione *"nel contesto delle attività di uno stabilimento"*[78].

Sulla seconda questione, la Corte nutrì ancora meno dubbi: le attività svolte da Google sono contemplate in modo esplicito all'interno dell'articolo 2, lett b). Tra le altre cose, la sentenza richiama un analogo caso, in cui l'apparizione su una pagina internet di dati personali era stata già oggetto di una precedente pronuncia[79]. Sul terzo punto, quello di maggiore interesse in virtù del tema di questo lavoro, la decisione dei giudici è stata piuttosto sorprendente, dato lo scostamento dalle argomentazioni e delle conclusioni dell'Avvocato Generale Jääskinen. Quest'ultimo si pronunciava così: *"La costellazione particolarmente complessa e difficile di diritti fondamentali che questo caso presenta, osta alla possibilità di rafforzare la posizione giuridica della persona interessata ai sensi della direttiva riconoscendole un diritto all'oblio. Ciò vorrebbe dire sacrificare diritti primari come la libertà di espressione e di*

77 Causa C-131/12 della Corte di Giustizia Europea del 13 Maggio 2014, par. 52-55.

78 Causa C-230/14 della Corte di Giustizia Europea del 1 Ottobre 2015, par. 25 e 66.

79 Si tratta della denominata sentenza Lindqvist, C.101/01 della Corte di Giustizia Europea del 6 Novembre 2003. Il caso riguardava un procedimento penale svolto dinanzi al giudice svedese contro la si.ra Lindqvist, rea di aver violato la normativa svedese relativa alla protezione dei dati personali, pubblicando sul sito della parrocchia della Chiesa protestante di Svezia dati personali riguardanti un determinato numero di persone che vi lavorano in qualità di volontari, senza aver ottenuto preventivamente il loro consenso. Nell'interpretazione della direttiva, i giudici cosi si espressero: *"...l'operazione consistente nel fare riferimento, in una pagina Internet, a diverse persone e nell'identificarle vuoi con il loro nome, vuoi con altri mezzi, ad esempio indicando il loro numero di telefono o informazioni relative alla loro situazione lavorativa e ai loro passatempo, costituisce un «trattamento di dati personali interamente o parzialmente automatizzato» ai sensi dell'art. 3, n. 1, della direttiva 95/46."*

informazione. Inoltre, inviterei la Corte a non concludere che questi interessi concorrenti possono essere ponderati in modo soddisfacente in situazioni individuali sulla base di una valutazione caso per caso, lasciando la decisione ai fornitori di servizi di motore di ricerca su Internet"[80].

La Corte negò appieno le affermazioni dell'Avvocato Generale, facendo partire il suo ragionamento da quanto enunciato dall'articolo 6 della direttiva. L'articolo in questione infatti dispone come i dati debbano essere trattati: a) lealmente e lecitamente, b) rilevati per finalità determinate, esplicite e legittime e successivamente trattati in modo non incompatibile con tali finalità, c) adeguati, pertinenti e non eccedenti rispetto alle finalità, d) esatti e aggiornati, e) conservati in modo da consentire l'identificazione delle persone interessate per un arco di tempo non superiore a quello necessario al conseguimento delle finalità.

Alla luce di quanto riportato, i giudici reputarono che l'articolo 12 lett b) che regola la cancellazione, la rettifica o il congelamento dei dati, possa applicarsi qualora il trattamento dei dati sia incompatibile con la direttiva stessa, anche quando l'incompatibilità derivi dal fatto che tali dati siano inadeguati, non pertinenti o eccessivi in rapporto alle finalità del trattamento o che per l'appunto siano conservati per un tempo superiore a quello strettamente necessario[81]. Ne discende che un trattamento di dati personali inizialmente lecito può con il passare del tempo divenire incompatibile con la suddetta direttiva.

Secondo la Corte, l'interessato, forte della tutela dei suoi diritti fondamentali sanciti dagli articoli 7 e 8 della Carta dei diritti fondamentali[82], può richiedere che le sue informazioni personali non vengano più messe a disposizione degli utenti del web

80 Resta, G. , Zencovich, V. Z., *Il diritto all'oblio su internet dopo la sentenza Google Spain,* cit. pag. 7-8

81 Causa C-131/12 della Corte di Giustizia Europea del 13 Maggio 2014, par. 92.

82 Articolo 7 "Rispetto della vita privata e della vita familiare" :

Ogni individuo ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni."

Articolo 8 "Protezione dei dati di 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 Ł soggetto al controllo di un'autorità indipendente ".

tramite un sistema di indicizzazione di risultati.
Sulla scorta di quanto appena detto, il rispetto della vita familiare e la protezione dei dati prevalgono in linea generale *"non soltanto sull'interesse economico del gestore del motore di ricerca, ma anche sull'interesse di tale pubblico a trovare l'informazione suddetta in occasione di una ricerca concernente il nome di questa persona".,* ad eccezione del caso in cui le informazioni riguardino un personaggio che ricopra un ruolo nella vita pubblica: in tal caso, l'ingerenza nei suoi diritti fondamentali può essere più netta in quanto giustificata dal preminente interesse del pubblico ad avere accesso all'informazione[83].

E' utile infine evidenziare che il termine diritto all'oblio viene utilizzato solo nelle conclusioni dall'Avvocato Generale, ma non dai giudici. Per questo talora si preferisce utilizzare l'espressione diritto alla de-indicizzazione dei dati in luogo dell'espressione diritto all'oblio: a parere di chi scrive, tale puntualizzazione appare oramai quasi irrilevante alla luce delle evoluzioni giurisprudenziali e normative sul tema.

2.3 Luci ed ombre della Sentenza Google Spain

Considerato l'impatto mediatico sollevato dal caso che coinvolgeva l'azienda di Mountain View, le reazioni della dottrina e degli esperti del settore alla sentenza non sono tardate ad arrivare.

83 Causa C-131/12 della Corte di Giustizia Europea del 13 Maggio 2014, par. 97. Tale punto è stato già prima affrontato al paragrafo 81 della medesima sentenza, che si ritiene utile riportare in nota: *"...poiché la soppressione di link dall'elenco di risultati potrebbe, a seconda dell'informazione in questione, avere ripercussioni sul legittimo interesse degli utenti di Internet potenzialmente interessati ad avere accesso a quest'ultima, occorre ricercare, in situazioni quali quelle oggetto del procedimento principale, un giusto equilibrio segnatamente tra tale interesse e i diritti fondamentali della persona di cui trattasi derivanti dagli articoli 7 e 8 della Carta. Se indubbiamente i diritti della persona interessata tutelati da tali articoli prevalgono, di norma, anche sul citato interesse degli utenti di Internet, tale equilibrio può nondimeno dipendere, in casi particolari, dalla natura dell'informazione di cui trattasi e dal suo carattere sensibile per la vita privata della persona suddetta, nonché dall'interesse del pubblico a disporre di tale informazione, il quale può variare, in particolare, a seconda del ruolo che tale persona riveste nella vita pubblica..."*

E' indubbio affermare che la sentenza è stata il punto cardine della nuova accezione di diritto all'oblio che tiene conto in forma differente del fattore temporale. Se dapprima il diritto ad essere dimenticati tradizionalmente nella sua "versione domestica" entrava in gioco nel momento in cui una notizia fosse riproposta o ripubblicata senza alcuna esigenza di attualità, con l'avvento della rete tale calcolo temporale perde ogni sua ragione d'essere: una volta immessa una notizia nel web, essa risulterà sempre fruibile. Tutto ciò risulta ulteriormente amplificato dalla diffusione oramai capillare degli smartphone e all'utilizzo dei social network, fenomeni che coinvolgono l'immissione nella disponibilità dei gestori di tali attività di un gran quantitativo di dati. Sul punto la questione che emerge è l'inconsapevolezza, da parte degli utenti, del valore economico dei loro dati, valore celato dall'apparente gratuità dei servizi. Nel suo libro "Presente continuo[84]", lo scrittore Douglas Rushkoff afferma che *"se un servizio è gratis, il prodotto sei tu",* constatando efficacemente con tale espressione come la fruizione di tali servizi online nasconda in realtà il sacrifico della propria privacy. I dati degli utenti sono divenuti *"il nuovo petrolio della società digitale"[85].* Ne discende l'esigenza di tutelare l'individuo anche da queste nuove forme di ingerenza della privacy: il diritto all'oblio si invoca per chiedere la cancellazione di quelle tracce lasciate inevitabilmente nel web nel momento in cui il soggetto ha deciso volontariamente di immetterle nel sistema.

Si delinea quindi una sorta di compartecipazione dell'individuo nella condivisione dei propri dati personali. Su questo aspetto, occorre citare la sentenza della Corte di Cassazione n. 5525 del 5 Aprile 2012[86], pronuncia interessante sotto vari punti di vista. In primis, perché a detta dei giudici il D. Lgs. n. 196 del 2003 *"ha sancito il passaggio da una concezione statica a una concezione dinamica della tutela della riservatezza".* In particolare, *"L'interessato ha diritto a che l'informazione oggetto*

84 Per una lettura tecnica sull'argomento, si invita alla lettura Rushkoff, D., Presente continuo, Quando tutto accade ora, Codice Edizioni, Torino, 2014. Si segnala anche l'interessante romanzo distopico di Patterson, J., *The Store,* Longanesi, Milano, 2017.

85 Pizzetti, F., *Il caso del diritto all'oblio*, pag. 41.

86 Il caso muove da una controversia instauratasi tra un politico del Partito socialista, arrestato all'inizio degli anni '90 per corruzione, ma poi prosciolto, ed il quotidiano Corriere della Sera, nel cui archivio on-line era possibile rinvenire ancora la notizia senza trovare alcun aggiornamento sull'esito positivo della vicenda.

di trattamento risponda a criteri di proporzionalità, necessità, pertinenza allo scopo e coerenza con la sua attuale ed effettiva identità personale o morale.

In secondo luogo, offre una concezione estensiva del diritto all'oblio che "*salvaguarda in realtà la proiezione sociale dell'identità personale, l'esigenza del soggetto di essere tutelato dalla divulgazione di informazioni lesive in ragione della perdita di attualità delle stesse, sicché il relativo trattamento viene a risultare non più giustificato ed anzi suscettibile di ostacolare il soggetto nell'esplicazione e nel godimento della propria personalità".*

In terzo luogo, la Suprema Corte interpreta il diritto ad essere dimenticati come diritto alla contestualizzazione delle informazioni presenti sul web, attribuendo al gestore della pagina contenente il fatto l'obbligo di provvedere, con apposti strumenti, all'aggiornamento della notizia. Peraltro, vi è da considerare l'impossibilità di garantire una rappresentazione completa e attuale di un soggetto visti gli alti costi che ne deriverebbero dal continuo aggiornamento di tali dati[87].

L'importanza di tale sentenza, che sembra aver ispirato i giudici europei nel caso *Google Spain*, risiede nel fatto che per la prima volta i giudici non si siano confrontati con la riproposizione di una notizia, bensì con il problema della permanenza della stessa su Internet[88].

Tornando alle valutazioni sulla sentenza Google Spain, ciò che emerge con più chiarezza e che interessa maggiormente ai fini di questo lavoro, è la dichiarata preminenza dell'interesse del cittadino alla propria privacy a scapito degli interessi economici del provider e/o editore e del diritto all'informazione degli utenti del web. La sentenza, unitamente alla sentenza Digital Rights, permette di sostenere l'affermarsi di un *digital right to privacy,* con l'obbligo di fatto imposto ai motori di ricerca di applicare la normativa europea in materia di dati personali[89]. Il riconoscimento di tale diritto legittima la teoria della libertà informatica[90], enunciata agli inizi degli anni '80, nella sua duplice accezione. La libertà informatica negativa consiste nel non rendere pubbliche determinate informazioni di carattere riservato,

87 Panico, C. R., *Da internet ai social network*, Maggioli Editore, Santarcangelo di Romagna (RN), 2013, pag. 81

88 *Ibidem,* cit., pag. 85

89 Alpa G., Conte, G. (a cura di), *Orientamenti della corte di giustizia dell'Unione Europea in materia di responsabilità civile,* Giappichelli editore, Torino, 2018, pag. 147.

privato e personale, mentre quella positiva rappresenta la facoltà di un soggetto di pretendere il controllo di dati personali, che usciti dall'orbita della propria privacy, hanno per divenire "elementi di input" di un programma elettronico[91]. Da una parte vi è quindi il diritto ad informare e a essere informati e dall'altra il diritto ad avere il controllo sui propri dati personali.

In materia di protezione di dati personali non è la prima volta che la CGE si confronta in opere di bilanciamento tra interessi e diritti contrapposti. Come menzionato, nella sentenza Digital Rights Ireland dell'8 Aprile, i giudici europei sono stati chiamati a pronunciarsi su una questione pregiudiziale relativa alla validità della direttiva 2006/24/CE (*data retention directive o direttiva sulla conservazione dei dati*) sulla base di quanto stabilito dagli articoli 7, 8 e 11 della Carta dei diritti fondamentali dell'Unione Europea. La pronuncia nasce in realtà dalla riunione di due cause (C-293/12 e C-594/12): la prima era stata sollevata dinanzi l'High Court irlandese dall'impresa irlandese Digital Rights Ltd., la quale metteva in discussione la legittimità di alcune misure legislative e amministrative sulla conservazione di dati relativi a comunicazioni elettroniche, chiedendo nello specifico di dichiarare la nullità della direttiva nella parte in cui impone ai fornitori di servizi di telecomunicazione di conservare i dati relativi al traffico e all'ubicazione per un determinato tempo stabilito dalle legge; la seconda causa invece faceva riferimento a numerosi ricorsi presentati dinanzi al Verfassungsgerichtshof (tribunale costituzionale austriaco) che chiedevano

90 Tale dottrina nacque nel 1981 come tentativo di soluzione al problema relativo alla protezione della riservatezza con riferimento alle banche dati. Di matrice ideologica liberale, il nuovo ipotetico diritto veniva promosso quale evoluzione del tradizionale diritto alla libertà personale in quanto tale nuova esigenza scaturiva dalla salvaguardia della persona dalla minaccia rappresentata dalla "degenerazione del nuovo potere sociale, economico e giuridico", vale a dire da quel potere informatico, che in quegli anni si manifestava nella capacità di accumulazione, memorizzazione ed elaborazione di dati informatici personali. In tal senso, si consiglia la lettura di Frosini, T. E., La libertà informatica: brevi note sull'attualità di una teoria giuridica in Informatica e Diritto, Vol. XVII, 2008, n.. 1-2 , pp. 87-97.

91 Resta, G. , Zencovich, V. Z., *Il diritto all'oblio su internet dopo la sentenza Google Spain,* cit. pag. 2. Per una visione più ampia, si consideri anche Codiglione, G., *Libertà d'impresa, concorrenza e neutralità della rete nel mercato transnazionale dei dati personali* in Diritto dell'Informazione e dell'Informatica, fasc. 4-5, 2015, pag. 909.

l'annullamento dell'articolo 102 bis introdotto dalla legge federale austriaca sulle telecomunicazioni, atto che aveva recepito la direttiva 2006/24/CE.

Tramite l'imposizione ai provider di servizi di telecomunicazioni dei dati di traffico e localizzazione, la *data retention directive* mirava a garantire la fruizione di tale informazioni agli organi di sicurezza degli Stati al fine della prevenzione, individuazione e perseguimento di reati gravi, in particolare criminalità organizzata e terrorismo.

I giudici stabilirono che l'obbligo di conservazione dei dati nel settori delle comunicazioni elettroniche costituiva un'ingerenza particolarmente grave nei diritti garantiti dall'articolo 7, nonché nel diritto alla protezione dei dati personali sancito dall'articolo 8, dal momento che tale previsione si configurava come un'ipotesi di trattamento dei dati personali. Sebbene il perseguimento della lotta al terrorismo e alla criminalità organizzata fosse da considerare un fine di interesse generale, la Corte, procedendo alla verifica del rispetto del principio di proporzionalità, reputò che tale interesse non poteva giustificare un'ingerenza di tal misura in quanto la direttiva imponeva un tempo di conservazione eccessivo[92]. Per giunta, consta menzionare il fatto che la pronuncia in questione costituisca il primo caso di annullamento di una direttiva per contrasto con la Carta[93].

Proprio con riferimento al peso e all'interpretazione data dalla CGE agli articoli 7 e 8 della Carta anche nella sentenza Google Spain, è possibile sollevare qualche critica.

Indubbiamente uno degli aspetti di rilievo della sentenza è la portata innovativa che viene data all'articolo 8 della Carta. Oltre a essere in un certo senso "costituzionalizzato" il diritto alla protezione dei dati, l'articolo viene emancipato

92 Così i giudici nella sentenza della Corte di Giustizia Europea (Grande Sezione)del 8 Aprile 2014, Cause riunite C-293/12 e C-594/12, par. 65 *"Da quanto precede deriva che la direttiva 2006/24 non prevede norme chiare e precise che regolino la portata dell'ingerenza nei diritti fondamentali sanciti dagli articoli 7 e 8 della Carta. Pertanto, è giocoforza constatare che tale direttiva comporta un'ingerenza nei suddetti diritti fondamentali di vasta portata e di particolare gravità nell'ordinamento giuridico dell'Unione, senza che siffatta ingerenza sia regolamentata con precisione da disposizioni che permettano di garantire che essa sia effettivamente limitata a quanto strettamente necessario. ".*

93 Nascimbene B., Anrò, I., *La tutela dei diritti fondamentali nella giurisprudenza della Corte di Giustizia: nuove sfide, nuove prospettive* in Rivista italiana di Diritto Pubblico Comparato, fasc. 2, 1 Aprile 2017, pag. 323 e ss.

definitivamente dalla dimensione economica che lo caratterizzava nell'originaria normativa della direttiva 95/46: la protezione dei dati personali non va più ricondotta alle logiche e alle esigenze di libera circolazione dei dati in funzione del mercato interno[94]. Nelle sentenze precedenti a quelle analizzate in tema di *data retention* e diritto all'oblio, l'atteggiamento dei giudici verso gli articoli 7 e 8 della Carta si esprimeva in una considerazione cumulativa del dettato delle due disposizioni, una sorta di approccio omnicomprensivo dei giudici comunitari alla protezione della privacy. Con le due sentenze citate, la condotta dei giudici cambia radicalmente. Viene proposta una lettura orientata a prendere in considerazione quasi esclusivamente i diritti degli articoli 7 e 8 della Carta nell'opera di bilanciamento che le è richiesta. Infatti, come anticipato nel caso Google Spain, l'Avvocato Generale nel suo reasoning[95] aveva per l'appunto menzionato la necessità di valutare non solo gli altri 7 e 8 della Carta, ma anche gli articoli 11 e 16 della Carta, riguardanti rispettivamente la libertà d'espressione e la libertà d'iniziativa economica[96].

94 Pollicino, O., U*n digital right preso (troppo) sul serio dai giudici di Lussemburgo? Il ruolo degli artt. 7 e 8 della Carta di Nizza nel reasoning di Google Spain* in Diritto dell'informazione e dell'informatica, n.4-5, 2014, pag. 10 e 11.

95 Appare opportuno riportare il passaggio argomentativo in questione (si veda Conclusioni dell'Avvocato Generale Niilo Jaaskinen presentate il 25 giugno 2013 Causa C 131/12:
"Per quanto riguarda i criteri che rendono legittimo il trattamento dei dati in mancanza del consenso della persona interessata [articolo 7, lettera a), della direttiva], appare evidente che la prestazione di servizi di motori di ricerca su Internet persegue, in quanto tale, interessi legittimi [articolo 7, lettera f), della direttiva], ossia (i) facilitare l'accesso alle informazioni per gli utenti di Internet; (ii) migliorare l'efficacia della diffusione delle informazioni caricate su Internet; e (iii) consentire diversi servizi della società dell'informazione offerti dal fornitore di servizi di motore di ricerca su Internet che sono accessori al motore di ricerca, come l'offerta di pubblicità tramite parole chiave. Questi tre obiettivi si rapportano, rispettivamente, a tre diritti fondamentali tutelati dalla Carta, vale a dire la libertà di informazione e la libertà di espressione (sancite entrambe all'articolo 11) e la libertà d'impresa (articolo 16). Pertanto, un fornitore di servizi di motore di ricerca su Internet persegue interessi legittimi, ai sensi dell'articolo 7, lettera f), della direttiva, quando tratta dati, compresi dati personali, messi a disposizione su Internet. "

96 Si riporta il testo della Carta dei diritti fondamentali dell'Unione Europea:
Articolo 11 Libertà di espressione e d'informazione
"1. Ogni individuo ha diritto alla libertà di espressione. Tale diritto include la libertà di opinione e la libertà di ricevere o di comunicare informazioni o idee senza che vi possa essere ingerenza da parte delle autorità pubbliche e senza limiti di frontiera.

Tuttavia nell'incedere argomentativo dei giudici non vi è nessuna valutazione e nessun riferimento agli articoli 11 e 16 della Carta. Si finisce quindi per promuovere un bilanciamento tra diritti contrastanti, che già a priori risulta essere asimmetrico e incline a favorire le ragioni della tutela della privacy digitale. In sintesi, la regola sembra essere la soccombenza del diritto all'informazione e della libertà d'impresa, derubricati a meri interessi, rispetto alla tutela dei dati personali, mentre l'eccezione è la loro possibile prevalenza solo in determinati casi e condizioni[97] (nel terzo capitolo ci si concentrerà su quest'aspetto in relazione al caso Manni).

Da quanto analizzato alla fine del precedente paragrafo, ne consegue che con la decisione dei giudici, si finisce per attribuire ai gestori dei motori di ricerca e alle Autorità di controllo l'onere di stabilire in quali casi la libertà d'informazione debba soccombere rispetto all'interesse privato: il rischio concreto sembra essere quello che le imprese al fine di evitare responsabilità e oneri di una così complessa attività di bilanciamento, preferiscano dar seguito positivo alle richieste di cancellazione degli utenti a scapito però del patrimonio informativo contenuto nel web e quindi di fatto limitando la libertà d'informazione[98]. Dal punto di vista economico invece, tale operazione probabilmente non comporta un aggravio di costi per le grandi società di capitali quali Google o Facebook, mentre non si può dire quanto questo adattamento al diritto europeo alla luce anche degli adempimenti subentrati con il GDPR, costituirà un aggravio per le imprese europee[99].

In contrasto con la visione di Pollicino più volte citata nel paragrafo 2.3, Alessandro Mantelero sostiene che nonostante la libertà d'impresa sia riconosciuta

2. La libertà dei media e il loro pluralismo sono rispettati."

Articolo 16 Libertà d'impresa

"E¨ riconosciuta la libertà d'impresa, conformemente al diritto comunitario e alle legislazioni e prassi nazionali".

97 Pollicino, O., U*n digital right preso (troppo) sul serio cit.,* pag. 14-15

98 Otranto, P., *Internet nell'organizzazione amministrativa: reti di libertà*, Cacucci Editore, Bari, 2015 pag. 33.

99 Alla luce dell'introduzione del GDPR, vi sono dei costi che le imprese dovranno sostenere: l'inserimento di nuove risorse per la gestione delle procedure in materia di privacy, lo sviluppo e aggiornamento delle procedure interne, la formazione e aggiornamento delle procedure interne, controllo e audit della gestione della privacy. Messina, A. C., La riforma della privacy. Guida pratica per l'applicazione del nuovo regolamento europeo (GDPR), Class Editori, Milano, 2018, pag. 20

all'interno delle carte fondamentali, essa rimane sempre subordinata alla protezione degli interessi della persona: secondo la sua visione devono essere *"i modelli di business a doversi adeguare al rispetto dei diritti fondamentali e non viceversa"*[100]*.* Ma l'autore va anche oltre, affermando che quando le corti supreme si ritrovano "a tu per tu" con casistiche che coinvolgono le strategie dei grandi operatori economici e le dinamiche dei mercati, è inevitabile che le loro decisioni possano trascendere la mera applicazione del diritto, sfociando in decisioni dal valore eminentemente politico nel tentativo di dare risposta a istanze sociali. La CGE avrebbe quindi rifiutato l'Exit strategy offerta dall'Avvocato Generale, che avrebbe garantito la continuazione dello *status quo,* per lanciare un messaggio e aprire un dibattito sul controverso articolo 17 del GDPR, al tempo ancora in discussione. Mantelero si dice critico anche nei confronti della reazione di Google[101]. La società americana all'indomani della sentenza ha

100 Mantelero, A, *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, n. 4-5, 2014, pag. 127.

101 Sul punto vi è da segnalare un aspetto curioso. La volontà del signor Gonzalez di far cadere nell'oblio la notizia dei suoi inadempimenti tributari che si è conclusa con l'esito positivo della sentenza in commento, in realtà si è trasformata in un'arma a doppio taglio giacché la sentenza è divenuta molto più celebre rispetto agli articoli di cui veniva chiesto il *delisting.* Per questa ragione, il sig. Gonzalez ha chiesto nuovamente all'autorità spagnola per la tutela dei dati personali di procedere all'anonimizzazione dei suoi dati personali e i testi online che trattano la sentenza. Tuttavia l'azienda americana ha negato tale possibilità, motivando piccata il diniego: *"Come stabilito dalla Sentenza della Corte di giustizia dell'Unione europea del 13 Maggio 2014, il diritto alla protezione dei dati deve cedere il passo alla libertà di espressione e di informazione quando le informazioni delle quali si chiede la deindicizzazione si riferiscono a questioni che sono di interesse generale. In questo senso, non può tacersi che il signor Gonzalez è parte della storia recente, essendo parte in un procedimento giudiziario di particolare interesse e di interesse pubblico. In particolare, il suo nome sarà per sempre associato ad un'importante sentenza della Corte di giustizia dell'Unione Europea. Non va trascurato, inoltre, che il signor Gonzalez non ha mai mostrato scrupoli ad esporsi pubblicamente, rilasciando interviste ed esprimendo il suo parere sui procedimenti giudiziari in cui era una parte interessata. Il fatto che il signor Gonzalez ha deliberatamente deciso di contribuire attivamente al dibattito pubblico attraverso la sua continua partecipazione alle interviste con i media in forma scritta, la radio e la comunicazione audiovisiva, determina che il legittimo interesse della società in materia di accesso a informazioni e opinioni su di lui, anche attraverso i motori di ricerca quando si cerca dal suo nome dovrebbe prevalere sul diritto alla protezione dei dati."* Si veda il seguente link: *https://www.ilfattoquotidiano.it/2015/10/09/costeja-gonzalez-negato-*

promosso la costituzione di un comitato consultivo di personalità internazionali chiamate a dibattere sulle soluzioni da adottare per raggiungere un bilanciamento tra diritto all'oblio e diritto del pubblico a sapere[102]. Inoltre, ha predisposto un sistema online con cui gli utenti possono avanzare le proprie richieste di cancellazione dei propri dati personali dai risultati delle ricerche del provider. L'effetto voluto di questa strategia sarebbe quella di dimostrare l'onere derivante dalla sentenza in capo a Google e di accrescerne il ruolo discrezionale e valutativo in relazione a quali richieste privilegiare[103].

2.4 Sviluppi recenti in tema di diritto all'oblio e ambito di applicazione: Google vs. CNIL

La sentenza Google Spain della CGE ha rilevato che la protezione dei dati personali rappresenta un diritto che svolge una ruolo da protagonista all'interno della società globale e digitale. Soprattutto segna in particolar modo l'agire delle imprese non europee che operano nel mercato unico dell'Unione Europea: al fine di perseguire l'obiettivo di una concorrenza leale, anche tali imprese vengono di fatto assoggettate alle norme sulla tutela dei dati personali, proiettando di fatto al di fuori dell'UE la concezione europea della dignità dell'uomo. Per questa ragione, dinanzi a dei criteri di applicazione territoriale della Direttiva 95/46 non idonei a soddisfare gli obiettivi di tutela della realtà odierna, la Corte nella sentenza in esame finisce per ampliare in

loblio-alluomo-che-lo-ha-regalato-alleuropa-2/2111057/ (aggiornato al 15 Dicembre 2018). L'autorità spagnola per la tutela dei dati personali non ha accolto le richieste del sig. Gonzalez.

102 Resta, G. , Zencovich, V. Z., *Il diritto all'oblio su internet dopo la sentenza Google Spain,* cit. pag. 4

103 Esemplificativo dell'insufficiente trasparenza nel processo di richiesta di rimozione, è quello relativo a un articolo di Robert Peston pubblicato sul sito della BBC e che trattava la vicenda finanziaria della Merrill Lynch. Al di là del fatto che la rimozione non era stata richiesta dal legittimo interessato, bensì da persona terza, la notorietà e attualità della notizia ad ogni modo avrebbe dovuto ad ogni modo garantire la permanenza della notizia nell'indice della ricerca. Mantelero, A, *Il futuro regolamento EU sui dati personali e la valenza "politica" del caso Google: ricordare e dimenticare nella digital economy* cit., pag. 134

maniera forzosa il concetto di stabilimento convertendolo in un concetto economico e funzionale[104].

Di fatto quindi società straniere come Google sono tenute ad adeguare i propri servizi alla normativa europea sui dati personali esclusivamente in relazione ai servizi offerti all'interno del mercato unico attraverso le relative succursali. Nell'ambito della causa intentata da Google Inc contro il CNIL (Commision Nationale de l'informatique et des libertés), il Consiglio di Stato francese ha sollevato alcune questioni pregiudiziali alla Corte di Giustizia Europea. Il conflitto è nato da una richiesta formale inoltrata dal CNIL a Google Inc affinché gli effetti della cancellazione siano estesi a tutte le versioni del motore di ricerca e quindi anche a quelle raggiungibili al di fuori del contesto europeo. A seguito della sentenza del 2014 la società americana aveva infatti provveduto alla de-indicizzazione dei risultati solamente in relazione alle ricerche effettuate dalla Spagna, mentre la stessa ricerca svolta da un server operante in uno stato diverso consentiva la visualizzazione dei suddetti risultati di cui era stata chiesta la rimozione. Tale soluzione di Google di de-indicizzare solo i risultati degli utenti localizzati nel territorio da cui proviene la richiesta di cancellazione, non ha trovato i favori del CNIL che nel 2016 ha disposto una sanzione di 100000 euro nell'ambito di varie controversie sollevate da cittadini francesi. La multa è stata impugnata da Google e ora la questione è all'analisi della CGE. Il quesito sottoposto all'organismo europeo è se il diritto alla cancellazione sancito con la sentenza Google Spain debba essere interpretato nel senso che il gestore di un motore di ricerca, ricevuta la domanda di cancellazione, sia tenuto a eseguire tale operazione indipendentemente dal luogo dal quale viene effettuata la ricerca[105]. Da un lato quindi, l'autorità francese sostiene una visione globale del diritto alla de-indicizzazione dei dati, mentre il colosso americano sostiene una visione incentrata sull'individuazione di quello che si può definire come "territorio reputazionale" circoscritto al territorio francese o europeo. Tale visione potrebbe portare a un paradosso. Si pensi al caso da cui ha preso le mosse il caso Google Spain: le notizie relative al pignoramento subito dal Sig. Costeja non sarebbero reperibili da un server

104 Alvarez Rigaudia, C., *La sentencia Google Spain y el derecho al olvido* in Actualidad Juridica, 2014, Vol. 38, pag. 118.

105 Si rimanda alle Conclusioni dell'Avvocato General Maciej Szpunar nella Causa C-507-17 (Google Inc c. CNIL).

europeo vista l'ingiunzione al *de-listing*, però potrebbero rimanere visibili qualora si acceda da un server extra-europeo.

In attesa della pronuncia dei giudici europei, recentemente l'Avvocato Generale Szpunar ha depositato le sue conclusioni, in cui ha sostenuto l'impossibilità di obbligare il motore di ricerca a garantire il diritto all'oblio in territorio extra-UE. Il rischio evidenziato è quello che la normativa europea limiti il diritto d'accesso alle informazioni alle persone che utilizzano i motori di ricerca da paesi extra-UE: siffatta ingerenza giustificherebbe questi paesi a limitare, per motivi di reciprocità, la stessa libertà di accesso alle informazioni per i cittadini europei. Il pericolo è quello di creare un pericoloso *casus belli* che porterebbe a un quasi inevitabile abbassamento del livello di tutela della libertà d'espressione a livello europeo e globale[106]. Tuttavia l'Avvocato Generale ha tenuto a precisare che la generale applicazione della direttiva 95/46 al solo territorio dell'Unione, non possa subire delle eccezioni quando si presentino situazioni in cui l'interesse dell'Unione lo richieda[107].

Tuttavia la Corte di Giustizia Europea potrà discostarsi anche questa volta dal parere dell'Avvocato Generale. Le linee che potrebbero determinare tale scostamento sono essenzialmente due.

La prima risiede nell'esistenza di una giurisprudenza consolidata in ambito antitrust[108], per cui un'impresa che partecipa a un accordo anticoncorrenziale, sebbene operi da un paese terzo, non è esente dall'applicazione delle regole in tema di tutela della concorrenza stabilite dagli articoli 101 e 102 TFUE, nel caso in cui tale accordo esplichi i suoi effetti nel territorio dell'Unione Europea[109]. Parimenti le stesse

106 *Ibidem*, par. 60 e 61.

107 *Ibidem*, par. 62. L'Avvocato Generale puntualizza che nel caso di specie tale eccezione non sembra essere ravvisabile.

108 In tal senso tra le altre si segnalano le seguenti pronunce: sentenza della CGE del 25 Novembre 1971, Causa 22-71 (Beguelin Import c. S.A.G.L: Import Export); sentenza della CGE DEL 14 Luglio 1972, Causa 48/69 (Imperial Chimical Industries Ltd. c. Commissione delle Comunità Europee. Sentenza della CGE del 25 Marzo 1999, causa T-102/96 (Gencor LTD c- Commissione),

109 L'applicazione extra-territoriale della normativa antitrust ha sollevato numerosi problemi, specie in relazione all'obbligo di non ingerenza negli affari interni di altri stati. L'aspetto più complicato della questione è l'asimmetria normativa tra i vari paesi: alcuni comportamenti ritenuti illegali in uno stato, possono essere legittimi in un altro. I giudici europei hanno sempre giustificato l'estensione degli effetti del diritto comunitario, sebbene tale estensione sia stata motivata talvolta

considerazioni possono ravvisarsi in relazione al tema della tutela dei marchi e brevetti[110]: se non si applicassero anche al di fuori dello spazio del mercato unico le norme in materia di proprietà industriale solo per il fatto che un'impresa operi tramite una pagina web con un server situato in uno Stato terzo, si potrebbero avere gravi ripercussioni sugli interessi economici delle imprese europee.

La seconda invece si riferisce all'applicazione extra-territoriale della CEDU in materia di diritti fondamentali. Ci si riferisce a quei casi in cui l'applicazione della CEDU è avvenuta in territori diversi da quelli degli Stati firmatari, qualora venissero in gioco diritti e libertà fondamentali, quali ad esempio il diritto alla vita (art.2) e il divieto di tortura (art.3)[111]. Tale principio di applicazione extra-territoriale, sembrerebbe trovare un riscontro analogico nella giurisprudenza europea, la quale nella sentenza *Caldararu* ha affermato il carattere assoluto dell'articolo 4 della Carta di Nizza evidenziando il collegamento manifesto con l'articolo 3 CEDU e con la relativa interpretazione[112].

Resta da capire quindi se anche il diritto alla protezione dei dati personali e il relativo diritto all'oblio possano rappresentare eccezioni così rilevanti da permettere un'applicazione della direttiva 95/46 anche al di fuori del territorio dell'Unione Europea.

Tali situazioni descritte in particolare quelle riguardanti il mondo delle imprese, a parere dell'Avvocato Generale, rappresentano eccezioni che si basano sugli effetti del mercato interno, ove la tutela di questo specifico territorio sancito dai trattati è interesse preminente delle istituzioni dell'Unione Europea; al contrario essendo

---

sulla cosiddetta teoria degli effetti, altre volte sulla teoria dell'unità del gruppo di imprese. Per una riflessione più approfondita si rinvia a Pace, F. L. (a cura di), Dizionario sistematico del diritto della concorrenza, Jovene Editore 2013, Napoli, pag. 145 e ss..

110 Si rimanda alle considerazioni della sentenza CGE (Grande Sezione) del 12 Luglio 2011, C-324/09 (Causa L'Oreal SA vs. Ebay International).

111 Si vedano sentenza CEDU del 7 Luglio 1989, n. 14038/88 (Causa Soering c. Royaume Uni); sentenza CEDU del 11 Luglio 2000, n. 40035/98 (Causa Jabari c. Turquie); sentenza CEDU del 15 Marzo 2001, n. 58128/00, (causa Ismaili c. Allemagne), sentenza CEDU del 4 Settembre 2014, n.140/10, (Causa Trabelsi c. Belgique).

Internet, per sua natura, uno spazio globale e presente ovunque, l'Avvocato Szpunar reputa difficile compiere analogie e confronti in relazione al caso di specie[113].

Tuttavia sarà la risposta dei giudici di Lussemburgo che determinerà se i governi nazionali e i garanti della privacy dei vari paesi avranno il potere di far valere le regole sulla de-indicizzazione anche nel resto del mondo, o se viceversa, Internet continuerà a manifestare e riaffermare la propria caratteristica di spazio sovranazionale. Un aspetto quest'ultimo che fa ben comprendere, che uno dei principali problemi nella tutela dei diritti fondamentali nel mondo digitale, consista nella mancanza di una governance dello cyberspazio.

Anche in questo caso, la CGE sarà chiamata a svolgere un'opera di bilanciamento, prestando attenzione, nel caso in cui decida di non condividere le conclusioni dell'Avvocato Generale, a non espandere eccessivamente il raggio di applicazione del diritto all'oblio, finendo per ledere sia gli interessi economici dei motori di ricerca vista la conseguente necessità di predisporre misure tecniche per garantire il rispetto della nuova configurazione dell'oblio, sia l'interesse della "comunità degli internauti" che sarebbero privati di un libero accesso alle informazioni[114].

Si tratta di decidere da che lato si vuol far pendere la bilancia: da un lato, dare piena e completa effettività alla de-indicizzazione, dall'altro limitare la rimozione ai soli domini europei, adottando un criterio di stretta necessità. Il grande interrogativo è quindi comprendere se l'estensione globale del diritto all'oblio costituisca una garanzia necessaria o una misura eccessiva[115].

112 Sentenza della Corte di Giustizia Europea (Grande Sezione) del 5 Aprile 2016, Cause riunite C-404/15 e C-659/15 PPU, par. 85 e 86.

113 Conclusioni dell'Avvocato General Maciej Szpunar nella Causa C-507-17 (Google Inc c. CNIL),par. 53.

114 Si pensi alle ripercussioni che si potrebbero avere in paesi caratterizzati dalla presenza di regimi autoritari.

115 Pecora, C., Diritto all'oblio: il problema della estensione extraeuropea della de-indicizzazione tra effettività della rimozione e libertà di informazione, consultabile nel sito http://www.medialaws.eu/diritto-alloblio-il-problema-della-estensione-extraeuropea-della-deindicizzazione-tra-effettivita-della-rimozione-e-liberta-di-informazione/ (aggiornato al 10/01/2019)

A parere di chi scrive, è da condividersi la prospettiva offerta dall'Avvocato Generale. L'ipotetico prevalere di un diritto alla de-indicizzazione su scala globale mal si coniugherebbe con l'esigenza di bilanciamento descritta in questo lavoro. Risulterebbe complicato stabilire il vero valore da attribuire al diritto di accesso alle informazioni, considerato che l'interesse del pubblico a una determinata informazione varierà necessariamente da uno Stato terzo all'altro.

La grande sfida dell'attualità è quella di trovare un quadro regolatore della privacy adeguato a garantire un effettivo equilibrio tra gli interessi in gioco: gli interessi economici delle imprese, l'innovazione e lo sviluppo, la libertà d'espressione e informazione, gli interessi dei cittadini a salvaguardare la privacy e la sicurezza nazionale. Nella sostanza la privacy non deve rappresentare un ostacolo alla crescita e allo sviluppo economico.

3° CAPITOLO: Il caso Manni: la prevalenza della tutela del mercato sull'oblio dei dati personali del registro delle imprese

Sommario: • 3.1 Il caso Manni: il fatto e le questioni pregiudiziali • 3.2 La visione offerta dalla Cassazione • 3.3 La sentenza della Corte di Giustizia Europea • 3.4 Considerazioni e valutazioni sulla sentenza Manni • 3.5 Alcune riflessioni: il fattore tempo.

Nei capitoli precedenti si è evidenziato come il diritto alla protezione dei dati personali sia sorto inizialmente come una delle misure idonee a garantire la realizzazione e il funzionamento dei principi introdotti con la Convenzione di Schengen, delineando così un certo collegamento con la dimensione economica dello spazio in cui tali dati vengono scambiati.

Si è poi presa in considerazione la visione di Pollicino, il quale ha sostenuto che, con le due sentenze Digital Rights e Google Spain, la Corte di Giustizia Europea abbia sostanzialmente fatto venir meno l'originario legame tra dati personali e libera circolazione degli stessi all'interno del mercato, giacché il suddetto diritto è stato elevato a diritto fondamentale[116]. Il diritto all'oblio, quale strumento declinatorio del diritto alla protezione dei dati personali, sembrava aver ottenuto, grazie alla pronuncia della CGE sul caso Google, una "consacrazione" e quindi una relativa prevalenza rispetto ad altri diritti fondamentali riconosciuti dall'ordinamento giuridico europeo.

Nella sentenza Manni che si sta per esaminare, tale orientamento sembra mitigato dalla Corte, la quale compie un altro passo verso la definizione più precisa del contenuto del diritto all'oblio, attraverso un'analisi ponderata degli interessi in gioco: da un lato, la richiesta di oblio del soggetto, dall'altra parte l'interesse generale dei terzi ad accedere ai dati contenuti nel registro delle imprese allo scopo di ottenere

116 Pollicino, O., De Gregorio, G., *Privacy or Transparency? A New Balancing of Interests for the 'Right to be Forgotten' of Personal Data Published in Public Registers* in The Italian Law Journal n.2, 2017, pag. 648 e ss.

informazioni veritiere in funzione della trasparenza e lealtà nelle relazioni commerciali.

3.1 Il caso Manni: il fatto e le questioni pregiudiziali

Nel 2007, il sig. Salvatore Manni, amministratore unico dell'impresa "Italiana Costruzioni s.r.l.", convenne in giudizio la Camera di Commercio di Lecce, lamentando l'impossibilità di vendere i complessi abitativi costruiti a causa di alcune informazioni presenti all'interno del registro delle imprese: in particolare, dal registro il sig. Manni risultava essere stato in precedenza l'amministratore unico e il liquidatore di un'altra società immobiliare fallita nel 1992 e cancellata, in seguito alla liquidazione, nel 2005. Secondo il ricorrente, le sue difficoltà nel reperire acquirenti derivavano proprio da tali informazioni ricavabili dal registro delle imprese e utilizzate da una società commerciale (Cerves Business Information spa) specializzata nella raccolta e nell'elaborazione di informazioni di mercato e valutazione del rischio.

Nonostante la richiesta di cancellazione o anonimizzazione dei dati presentata dal sig. Manni in data 10 Aprile 2006, la Camera di Commercio di Lecce non aveva provveduto alla cancellazione.

Con sentenza 1° Agosto 2011, il Tribunale di Lecce accolse le domande, ordinando alla Camera di Commercio la trasformazione in forma anonima dei dati e la condanna a € 2000,00, oltre al pagamento di interessi e spese processuali. Nel merito, i giudici sostennero che fosse *"difficilmente sostenibile la necessità e l'utilità dell'indicazione nominativa dell'amministratore unico della società al tempo del fallimento"*, considerato che, oltre all'intervenuta cancellazione della società già due anni prima, si trattava di fatti avvenuti ben dieci anni prima. Per queste ragioni, "*la memoria storica dell'esistenza della società e delle vicissitudini che l'hanno interessata può essere ampiamente realizzata mediante dati anonimi*", giacché *"le iscrizioni che collegano il nominativo di una persona fisica ad una fase patologica della vita dell'impresa come il fallimento non possono essere perenni, in mancanza di uno specifico interesse generale alla loro conservazione e divulgazione".* Infine i giudici concludevano affermando la sussistenza di un danno all'immagine, in quanto l'attore

aveva dimostrato che varie trattative con potenziali acquirenti erano state interrotte a causa delle informazioni assunte[117].

La Camera di Commercio adì la Corte di legittimità ex art 152, co. 13 del D. lgs. 30 Giugno 2003, n. 196[118]. Tra i vari motivi del ricorso, la parte soccombente in particolare lamentava: in primo luogo, l'insufficiente od omessa motivazione circa il mancato rilevamento del difetto di legittimazione passiva della Camera di Commercio di Lecce, la quale imputava la responsabilità della rielaborazione e della diffusione dei dati del Sig. Manni in capo alla società specializzata in indagini di mercato; in secondo luogo, evidenziava che la parte ricorrente avesse già esperito inutilmente ricorso ai sensi dell'articolo 2191 c.c. al giudice del registro delle imprese al fine di ottenere la cancellazione dei dati, invocando il vizio di *ne bis in in idem;* in terzo luogo, la Camera evidenziava che la sentenza del Tribunale di Lecce finiva per *"negare la funzione istituzionale di pubblicità legale del registro delle imprese, che costituisce una banca dati pubblica".* Per quanto concerne la legittimazione passiva della Camera di Commercio, la Cassazione smentì le argomentazioni addotte affermando che la legittimazione della Camera sussisteva in quanto ente designato dalla legge a conservare il registro delle imprese e la relativa pubblicazione e mantenimento dei dati riferiti al signor Manni.
Stesso esito negativo fu fornito dai giudici al secondo quesito relativo alla presunta violazione del principio del *ne bis in idem*.

Relativamente invece al terzo punto, esso costituì il punto centrale della controversia che spinse la Corte a sollevare due questioni giurisprudenziali: 1) se il principio di conservazione dei dati personali che imponeva il loro trattamento per un arco di tempo non superiore a quello necessario al conseguimento delle finalità, previsto dall'articolo 6, lett. e), della direttiva 46/95/CE, avesse dovuto imporsi al sistema di pubblicità attuato con il registro delle imprese, previsto dalla Prima

117 Per un approfondimento sulle questioni di fatto, si rimanda all'ordinanza di rinvio della Corte di Cassazione Civile (prima Sezione), n. 15096/15 del 21 Maggio 2015, pervenuta in cancelleria il 23 Luglio 2015. E' reperibile al sito http://www.ipsoa.it/~/media/Quotidiano/2015/07/22/Registro-delle-imprese--conservazione-dei-dati-e--oblio---questione-alla-Corte-UE/15096-15%20pdf.pdf (ultimo aggiornamento 10 Dicembre 2018.)

118 Tutte le controversie che riguardano l'applicazione del codice in materia di dati personali non sono appellabili, ma è ammesso il ricorso per cassazione.

direttiva 68/151/CE e dal diritto nazionale all'articolo 2188 c.c., laddove esso esigeva, che qualsiasi persona potesse conoscere senza limiti di tempo i dati relativi alle persone fisiche; 2) se l'articolo 3 della prima direttiva 68/151/CE consentiva che, in deroga alla durata illimitata e ai destinatari indeterminati dei dati pubblicati sul registro, i dati stessi non fossero più soggetti a pubblicità, ma fossero invece disponibili per un tempo limitato deciso discrezionalmente dal gestore del dato.

La Corte di Giustizia Europea venne così investita di una questione concernente il diritto all'oblio, anche se, a differenza del caso Google, in questo caso il tema prendeva le mosse dalla conservazione di dati all'interno di un registro pubblico, riportando così il tema dell'oblio dal mondo digitale a quello reale[119].

3.2 La visione offerta dalla Cassazione

Dal punto di vista normativo, le norme di riferimento per la risoluzione della questione sono state varie. Nel contesto dell'Unione Europea, la prima direttiva 68/151/CE disciplina la pubblicità obbligatoria degli atti delle società a responsabilità limitata in un'ottica di coordinamento e armonizzazione delle garanzie richieste all'interno degli stati membri. L'articolo 3 impone che in ciascun stato membro venga costituito un fascicolo presso un registro centrale, o presso il registro di commercio o registro delle imprese, in cui vengano trascritti tutti gli atti e le indicazioni soggetti a pubblicità[120] di tutte le società iscritte. Nel 2003 è intervenuta

119 Sileoni, S., *"Il diritto alla cancellazione dei dati e le attività economiche: una nuova visione del tempo. A margine della sentenza Camera di commercio c. Manni"* in Media Laws, n.1, 2017, pag. 143-146.

120 Relativamente a quali atti debbano essere trascritti all'interno del registro delle imprese, essi vengono elencati dall'articolo 2 della suddetta direttiva: l'atto costitutivo e lo statuto e relative modifiche intercorse nel tempo, la nomina, la cessazione dalle funzioni delle persone che hanno il potere di obbligare la società di fronte ai terzi e di rappresentarla in giudizio o di coloro che partecipano all'amministrazione, all'ispezione o al controllo della società, l'importo del capitale sottoscritto almeno una volta all'anno, il bilancio e il conto profitti e perdite di ogni esercizio, il trasferimento della sede sociale, lo scioglimento della società, la sentenza che dichiara la nullità della società, la nomina e la generalità dei liquidatori e relativi poteri, la chiusura della liquidazione e la cancellazione dal registro. Si veda il testo integrale dell'articolo 2 per una disamina più specifica.

la direttiva n. 58 che ha provveduto a inserire l'articolo 3-bis che ha esteso la normativa della direttiva 68/151 all'archiviazione elettronica dei dati societari. Tale direttiva fu particolarmente interessante perché per la prima volta venne introdotto un criterio temporale in forza del quale gli Stati, relativamente a taluni o tutti i tipi di atti registrati fino al Dicembre 2006, potevano decidere di non renderli più disponibili e accessibili dal registro in via elettronica, qualora risultasse decorso un determinato periodo (almeno dieci anni) tra la data della registrazione e la richiesta d'accesso[121]. Desta poi un certo interesse il fatto che nell'analisi delle fonti europee, i giudici della Cassazione, oltre all'ovvia menzione dell'articolo 8 della Carta di Nizza e alla direttiva n. 46/95, richiamarono anche l'articolo 8 della CEDU[122], riferimento quest'ultimo, che come si è visto precedentemente, non era stato invece preso in esame dai giudici europei nella sentenza Google Spain.

Sul fronte della normativa interna, la Suprema Corte citò innanzitutto l'articolo 2188[123] del Codice Civile e la successiva integrazione dettata dall'articolo 8 della l. n. 580 del 1993, che ha istituito di fatto presso le camere di commercio gli uffici del registro delle imprese disciplinati dagli articoli 2188 e ss. del codice. I giudici ci tennero a sottolineare che "*l'innovazione fu di rilievo, perché coincise con il passaggio da un regime di pubblicità frammentario ad un regime completo ed organico degli*

121 Tale possibilità tuttavia è subordinata esclusivamente all'accesso al registro elettronico, con la conseguenza che tali dati possono essere sempre visibili dal registro cartaceo. Alpa, G., Conte, G. (a cura di), *Casi decisi dalla Corte di Giustizia dell'Unione europea sui diritti fondamentali in materia contrattuale,* Giappichelli Editore, Torino, 2018, pag. 55

122 Di seguito l'articolo 8 della CEDU:

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

2. Non può esservi ingerenza della pubblica autorità nell'esercizio di tale diritto se non in quanto tale ingerenza sia prevista dalla legge e in quanto costituisca una misura che, in una società democratica, è necessaria per la sicurezza nazionale, l'ordine pubblico, il benessere economico del paese, la prevenzione dei reati, la protezione della salute o della morale, o la protezione dei diritti e delle libertà altrui."

123 In tal senso l'articolo 8, co. 6 della l. 29 Dicembre 1993, n.580, La predisposizione, la tenuta, la conservazione e la gestione, secondo tecniche informatiche, del registro delle imprese ed il funzionamento dell'ufficio sono realizzati in modo da assicurare completezza e organicità' di pubblicità' per tutte le imprese soggette ad iscrizione, garantendo la tempestività' dell'informazione su tutto il territorio nazionale.

imprenditori individuali e delle società: tutti i soggetti socio-economici che operano sul mercato imprenditoriale, indipendentemente dalla loro struttura, sono soggetti a pubblicità". Dall'enunciato dell'art. 2188, co 2., secondo cui *"il registro è pubblico"*, la Cassazione ne dedusse la sostanziale prevalenza dell'interesse dei terzi sulle esigenze di riservatezza dei *"mercatores".* I pubblici registri, come in questo caso il registro delle imprese, "*hanno enorme importanza, economica e sociale, in quanto producono o fanno circolare delle "speciali forme di sicurezza circa eventi, che direttamente o indirettamente rendono sicuri, o quanto meno più agevoli, i rapporti economici e sociali*"[124]. Ne deriva che i registri delle imprese, conservati presso le Camere di Commercio – le quali ai sensi dell'art. 1 co. 1 della legge n.580 del 1993 sono definite enti autonomi di diritto pubblico - mirano a garantire la certezza giuridica necessaria ai fini degli scambi sul mercato attraverso la reperibilità di informazioni giuridicamente attendibili, accessibili a tutti e opponibili ai terzi. L'attuazione di tale pubblicità atta a regolamentare i rapporti economici è uno dei compiti attribuiti alla pubblica amministrazione[125].

L'art 2196 del Codice civile definisce poi le informazioni che devono essere riportate all'interno del registro: a) nome e cognome, luogo e data di nascita e cittadinanza dell'imprenditore, b) la ditta, c) l'oggetto dell'impresa, d) la sede dell'impresa, e) nome e cognome degli institori e procuratori. Per quanto riguarda la cancellazione dell'iscrizione dal registro, l'articolo 2191 c.c. prevede che il giudice del registro possa disporre la cancellazione d'ufficio solo quando essa sia avvenuta senza che esistano le condizioni richieste dalla legge[126]. Non sembra quindi sussistere un obbligo legale imposto all'autorità pubblica di provvedere alla cancellazione d'ufficio trascorso un determinato periodo di tempo.

Se da un lato le informazioni contenute all'interno del registro delle imprese sono essenziali alla configurazione di un sistema economico di scambi commerciali

124 Corte di Cassazione Civile (prima Sezione), ordinanza n. 15096/15 del 17 Luglio 2015, par. 4.4.1.

125 Cariglino, F., *Pubblicità obbligatoria e diritto all'oblio come si conciliano?*, nota a ordinanza n. 15096/15 della Corte di Cassazione Civ., rintracciabile al sito https://www.altalex.com/documents/news/2015/12/09/diritto-a-oblio-pubblicita-obbligatoria

126 Nello specifico si provvede alla cancellazione d'ufficio quando si certifichi che tale iscrizione: non avrebbe dovuto essere effettuata per la non corrispondenza del fatto dichiarato o perché non necessaria ai fini del regime della pubblicità; non avrebbe dovuto essere effettuata in quel registro delle imprese; non avrebbe dovuto essere effettuata in quella sezione del registro delle imprese.

regolamentato e improntato alla certezza e alla trasparenza dei rapporti giuridici, dall'altro lato è necessario comprendere la posizione di quei soggetti, che pur avendo "fallito" in passato, si ripresentano come attori all'interno del mercato. E' su questa divergenza di posizioni e interessi, che si instaura il tema del diritto all'oblio. La Cassazione rilevò infatti che il problema di fondo consiste nel conciliare il conflitto tra verità storica e identità attuale. Agli occhi dei giudici, l'oblio appare un diritto strumentale ad altri diritti quali la riservatezza, l'identità personale e il diritto alla protezione dei dati personali. Il bene giuridico tutelato è sempre quello dell'identità, e la necessità che traspare è quella di bilanciarlo *"con altri diritti costituzionali e diritti fondamentali dell'Unione Europea, quali quelli della libertà d'informazione, di espressione, di accessibilità universale alle informazioni su internet e d'impresa*[127]*".* E sembra essere proprio la libertà d'impresa il concetto da prender in maggior in considerazione: *"trasparenza dei traffici e diritto alla protezione dei dati personali sembrano interessi destinati a conoscere il primato di un diritto sull'altro a seconda dei frangenti storici*[128]*"*

D'altronde il diritto alla protezione dei dati personali sancito dall'articolo 8 della Carta dei diritti fondamentali dell'Unione Europea, alla luce di quanto espresso dall'articolo 52 della stessa Carta, può essere suscettibile di limitazioni previste dalla legge purché esse rispettino il nucleo essenziale di tale diritto e siano necessarie e proporzionate a rispondere a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere diritti e libertà di terzi[129]. Questa opera di bilanciamento deve attuarsi anche con i diritti e le libertà sanciti della Costituzione italiana, al fine di evitare "*l'illimitata espansione di uno dei diritti, che diverrebbe "tiranno" nei confronti delle altre situazioni giuridiche costituzionalmente riconosciute e protette*[130]*"*. E tale assunto vale anche nei confronti della tutela dei dati personali[131]

127 Corte di Cassazione Civ. (prima Sezione), ordinanza n. 15096/15 del 17 Luglio 2015, par. 4.4.3.

128 *Ibidem.*

129 La protezione di dati personali non va considerata una prerogativa assoluta, ma va considerato alla luce della sua funziona sociale. Tale affermazione si evince dalla pronuncia della Corte di Giustizia dell'Unione Europea, 12 giugno 2003, causa C-112/00, Schimeberg, punto 80.

130 Vedasi il testo della Corte costituzionale, sent. n. 85/2013 del 9 Aprile 2013, par. 9.

131 "*Il diritto ad esigere una corretta gestione dei propri dati personali, pur se rientrante nei diritti fondamentali di cui all'art. 2 Cost., non è un totem al quale possano sacrificarsi altri diritti altrettanto rilevanti sul piano costituzionale".* Così Cassazione Civ. , n. 10280 del 20 Maggio 2015, par. 8.1.

Bisogna tener presente che la questione della cancellazione dei dati dal registro delle imprese è stata più volte oggetto dell'attenzione del Garante per la protezione dei dati personali, il quale ha sempre dato esito negativo a tali richieste, escludendo che possa ritenersi illegittima la pubblicità nel registro delle imprese[132].

Sul piano pratico, i giudici di legittimità sono consci delle difficoltà del legislatore nello stabilire a priori un termine congruo per la conservazione del dato.

Il sistema di registrazione non si basa unicamente sul momento dell'iscrizione, bensì anche su tutte le successive modifiche che possono intervenire sull'assetto societario. E' un sistema che si fonda su un meccanismo che non prevede l'eliminazione definitiva del dato originario, anche quando il secondo dato registrato smentisca o renda obsoleto il primo. Peraltro, nel suo ragionamento la Corte ha avanzato l'ipotesi per cui la conservazione dei dati per scopi storici dettata dall'art. 99 Codice Privacy[133], se interpretata estensivamente, potrebbe giustificare la conservazione permanente di dati oramai risalenti a vecchie vicende all'interno delle visure storiche del registro[134],

132 In tal senso, ad esempio, il provvedimento del 6 Ottobre 2005 (doc. web. 1185197, consultabile al sito *https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1185197*). Il caso, simile a quello oggetto di studio in questa sede, riguardava l'ex liquidatore di una società dichiarata fallita nel maggio 1999 e cancellata dal registro delle imprese nel 2000. Il ricorrente chiedeva la cancellazione del proprio nominativo. Il garante ha risposto adducendo che "*il trattamento di dati personali dell'interessato posto in essere dalla camera di commercio resistente è consentito per lo svolgimento di funzioni istituzionali, nei limiti stabiliti dalla legge e dai regolamenti. Nel caso di specie non sono comprovati elementi che facciano ritenere illecito o non corretto il trattamento in relazione alla specifica disciplina allo stato vigente in materia e, in particolare, alle disposizioni del codice civile che regolano le modalità di tenuta del registro delle imprese (art. 2188 c.c.)*.

133 Art. 99 D. Lgs. n. 196, del 30 giugno 2003 *(Compatibilità' tra scopi e durata del trattamento): "1). Il trattamento di dati personali effettuato per scopi storici, statistici o scientifici e' considerato compatibile con i diversi scopi per i quali i dati sono stati in precedenza raccolti o trattati. 2). Il trattamento di dati personali per scopi storici, statistici o scientifici puo' essere effettuato anche oltre il periodo di tempo necessario per conseguire i diversi scopi per i quali i dati sono stati in precedenza raccolti o trattati.*

3) Per scopi storici, statistici o scientifici possono comunque essere conservati o ceduti ad altro titolare i dati personali dei quali, per qualsiasi causa, e' cessato il trattamento."

134 La visura è un documento informativo contenente tutte le notizie relative l'impresa, la quale esercitando un'attività economica, ha dovuto obbligatoriamente iscriversi presso il registro imprese della Camera di Commercio della provincia in cui ha sede l'azienda.

riportando per iscritto così tutte le vicende imprenditoriali significative agli occhi degli operatori economici[135]. Dall'articolo 120 della Legge fallimentare, che recita *"Con la chiusura cessano gli effetti del fallimento sul patrimonio del fallito e le conseguenti incapacità personali...",* dovremmo dedurre che la durata della pubblicità commerciale debba coincidere con l'operatività della società stessa. Tuttavia la natura del registro delle imprese è quella di fornire in modo durevole tali informazioni dal momento che l'esigenza di conoscerle può prolungarsi nel tempo: "*gli scopi o finalità della pubblicità commerciale sono quelli di rendere noto, oppure opponibile, oppure esistente un certo fatto giuridico, al fine ultimo della sicurezza del mercato*"[136]. La Cassazione affermò inoltre che "*in ragione della funzione svolta, della pluralità indeterminata dei destinatari, della rilevanza potenzialmente senza limiti di tempo di quegli effetti, del susseguirsi infinito dei commerci, la pubblicità commerciale mal si presta ad una valutazione in termini di non perdurante utilità: fino a quando esiste un mercato, al quale il soggetto dei cui dati si tratta è permesso di permanere o entrare, sussiste l'esigenza di espletare la funzione della pubblicità, di per sé idonea a costituire una causa di giustificazione per il trattamento di dati*".

Nella pronuncia in questione i giudici italiani non nascosero quindi che nel bilanciamento tra l'interesse del singolo alla riservatezza dei dati e l'interesse del mercato, l'orientamento da seguire sarebbe stato quello di far prevalere quest'ultimo: richieste quali quelle avanzate dal Sig. Manni, non sarebbero perciò condivisibili.

Nonostante questa ricostruzione, la Corte di Cassazione ammise la possibilità che il diritto all'oblio potesse essere considerato uno strumento irrinunciabile per tutelare l'identità personale anche nei confronti dei dati conservati nel registro delle imprese. Vale a dire che il principio di conservazione dei dati non oltre il tempo necessario al conseguimento delle finalità originarie, disciplinato dall'art. 6 della direttiva 95/46 e ripreso dall'art. 11 del Codice della Privacy, avrebbe potuto suggerire l'individuazione di un tempo massimo di reperibilità delle informazioni nel registro delle imprese, a cui si sarebbe potuto affiancare un ulteriore criterio volto alla limitazione dei destinatari dell'informazione. Ammessa tale ipotesi, la Corte sollevò la questione relativa a chi dovesse farsi carico di tale valutazione: escluso sicuramente

135 Corte di Cassazione Civ. (prima Sezione), ordinanza n. 15096/15 del 17 Luglio 2015, par. 4.4.7.

136 *Ibidem,* par. 4.4.9

che tale giudizio potesse essere svolto dalla Camera di Commercio, la Suprema Corte propose che fossero proprio i giudici a stabilire di volta in volta se quei dati non dovessero più risultare pubblici. Tale valutazione avrebbe dovuto effettuarsi attraverso una valutazione probabilistica ponderata sulla necessità che il dato permanesse nel registro alla luce di tutte le possibili richieste e finalità, comprese quelle in cui vi fosse in gioco l'interesse dei terzi. Tuttavia, in assenza di una legge ad hoc, il rischio evidenziato era che il verificarsi di una difformità troppo marcata tra le valutazioni dei giudici[137]. Per tali ragioni, la Corte di legittimità decise di rimettere la questione alla Corte di Giustizia Europea ex art 267 TFUE, determinando la sospensione del procedimento.

3.3 L'iscrizione al registro delle imprese

Come si è accennato nel paragrafo precedente, il registro delle imprese è regolato dagli articoli 2188 e ss. del Codice Civile. L'articolo 2195 indica quali siano i soggetti obbligati a compiere l'iscrizione, vale a dire *"gli imprenditori che esercitano un'attività industriale diretta alla produzione di beni o servizi; un'attività intermedia nella circolazione dei beni; un'attività di trasporto per terra, per acqua o per aria; un'attività bancaria o assicurativa; altre attività ausiliarie delle precedenti."* L'iscrizione di questi soggetti al registro delle imprese soggiace a tre principi: il primo riguarda la tassatività delle iscrizioni, che impone l'iscrizione dei soli atti previsti dalla legge; il secondo si riferisce il rapporto fra opponibilità e conoscibilità, nel senso che sono opponibili ai terzi solo quei fatti di cui essi possono venire a conoscenza tramite il registro; per ultimo, vale il principio dell'esclusività dello strumento di opponibilità, per cui il registro rappresenta l'unico strumento per opporsi a terzi in relazione al catalogo degli atti per cui è prevista la registrazione.

L'iscrizione nel registro delle imprese e la relativa pubblicità delle informazioni può adottare tre differenti forme di pubblicità: costitutiva, dichiarativa e pubblicità-notizia.

Si ha pubblicità costitutiva quando la pubblicità concorre al perfezionamento dell'atto scritto; nel caso di pubblicità dichiarativa, la pubblicità rende l'atto iscritto opponibile ai terzi. La differenza tra le due casistiche risiede nell'elemento dell'effettiva

137 *Ibidem*, par. 4.5

conoscenza del terzo, poiché ex art 2193 " i fatti dei quali la legge prescrive l'iscrizione, se non sono stati iscritti, non possono essere opposti a terzi", a meno che non si provi che i terzi ne abbiano avuto conoscenza.

Quando invece si parla di pubblicità-notizia, l'atto viene reso conoscibile in ottica puramente informativa e riguarda normalmente l'iscrizione alle sezioni speciali. Di norma, l'iscrizione al registro delle imprese ha efficacia dichiarativa[138], salvo possibili eccezioni previste dalla legge[139].

Ai fini di questa trattazione, appare utile chiarire quale efficacia vada ricondotta al caso della cancellazione dell'impresa dal registro. Prima della riforma introdotta con decreto legislativo n.6 del 2003, non era chiaro se all'istituto della cancellazione dovesse essere ricondotta un'efficacia costitutiva in relazione all'estinzione di una società, o se viceversa andasse attribuita un'efficacia dichiarativa per cui l'estinzione si produceva solo quando si fossero esauriti tutti i rapporti giuridici pendenti della società.

Con la riforma , l'articolo 2495 c.c. ha previsto che *"Approvato il bilancio finale di liquidazione, i liquidatori devono chiedere la cancellazione della società dal registro delle imprese. Ferma restando l'estinzione della società, dopo la cancellazione i creditori sociali non soddisfatti possono far valere i loro crediti nei confronti dei soci, fino alla concorrenza delle somme da questi riscosse in base al bilancio finale di liquidazione, e nei confronti dei liquidatori, se il mancato pagamento è dipeso da colpa di questi. La domanda, se proposta entro un anno dalla cancellazione, può essere notificata presso l'ultima sede della società".* Tuttavia sull'articolo modificato si ravvisavano comunque due orientamenti: il primo affermava che a seguito della procedura di liquidazione, la cancellazione non determinava comunque l'estinzione della persona giuridica, comportando il fatto che la responsabilità processuale e sostanziale della società

138 Essa non può essere ricondotta pienamente alla pubblicità in materia di trascrizione ex. Articolo 2644 c.c., dal momento che la pubblicità d'impresa è principalmente indirizzata a risolvere conflitti in merito alle vicende organizzative della società e non controversie relative all'attribuzione di un bene immobile. E' per questa ragione che all'assenza dell'adempimento pubblicitario è possibile sopperire con la dimostrazione della conoscenza del fatto non pubblicizzato nel registro.

139 Ha efficacia costitutiva ad esempio l'iscrizione dell'atto costitutivo delle società di capitali. Si rinvia alle considerazioni e agli esempi riportati da Ibba C, Il registro delle imprese: effetti in Diritto On Line, tratto dalla pagina http://www.treccani.it/enciclopedia/registro-delle-imprese-2-effetti_(Diritto-on-line)/#1funzionidelregistroedeffettidelliscrizione-1.

rimaneva in capo ai soggetti che la rappresentavano prima della cancellazione. Viceversa, una seconda visione sosteneva che l'estinzione della società doveva essere ricondotta alla cancellazione anche qualora sussistessero crediti insoddisfatti.

La Corte di Cassazione, con sentenza n.4060 del 2010[140], ha avallato questa seconda ipotesi, determinando sostanzialmente l'estinzione della società al momento della cancellazione dal registro delle imprese. Sul punto tuttavia sussistono alcune perplessità. Sebbene sia stata sancita l'efficacia costitutiva dell'istituto della cancellazione, ciò non toglie che possano sussistere ugualmente rapporti pendenti. Per questa ragione, l'importanza della funzione pubblicistica del registro non viene meno dal momento che talune azioni nei confronti degli ex soci e amministratori possono essere ancora rilevate in giudizio. Ne consegue che le informazioni sulle vicende personali di un soggetto amministratore di una società di capitali siano legittimamente conservate all'interno del registro, pur sussistendo altrettanti dubbi sulla possibilità di individuare un termine per la loro definitiva eliminazione.

3.4 La sentenza della Corte di Giustizia Europea

La CGE fu chiamata a sbrogliare la complicata matassa costituita dal bilanciamento tra diritti contrapposti: da un lato prendendo in considerazione la "sete" di regolamentazione e di informazione degli operatori economici in virtù dei principi orientati alla trasparenza e allo sviluppo del mercato, dall'altro lato non ostacolando l'interesse al reinserimento di quei soggetti che in precedenza avevano svolto un'attività economica[141]. Il compito era quello di stabilire quali fossero i termini e i limiti dell'esposizione dei dati personali. In prima analisi, i giudici europei presero in esame la direttiva 68/151 CE. L'obiettivo di tale direttiva è quello di *"facilitare e accelerare l'accesso delle parti interessate alle informazioni sulle società, semplificando in modo significativo le formalità relative alla pubblicità cui le stesse sono tenute[142]".* Essa fornisce "*una garanzia giuridica per le relazioni tra la società ed i terzi, in previsione di un incremento degli scambi commerciali fra gli Stati membri in seguito*

140 Sentenza della Corte di Cassazione (Sezioni Unite) n. 4060 del 22 Febbraio 2010.

141 Cariglino, F., *Pubblicità obbligatoria e diritto all'oblio come si conciliano?*, cit.

142 Sentenza della Corte di Giustizia Europea (Seconda Sezione), Causa C-398/15 del 9 Marzo 2017

all'istituzione del mercato comune"[143]. Il bene tutelato dal registro delle imprese è la certezza dei rapporti giuridici e risponde agli interessi dei creditori, che sono i soggetti maggiormente interessati a conoscere il quadro completo della vita di un'impresa[144]. Ma risponde anche agli interessi di coloro che operando nel mercato si servono delle informazioni del registro delle imprese per valutare l'attendibilità delle persone fisiche attraverso un controllo delle loro attività economiche precedenti[145].

Il secondo passaggio della Corte si concentrò sull'analisi della direttiva 95/46, evidenziando i principi enunciati dall'articolo 6 (principio di qualità dei dati, tra cui il principio di conservazione) e gli articoli 12 e 14 relativamente al diritto di accesso e al diritto di opposizione della persona interessata, tra cui rientra anche la *"rettifica, la cancellazione o il congelamento dei dati il cui trattamento non è conforme alle*

143 Sentenza della Corte di Giustizia Europea, Causa 32/74 (Haaga GmbH) del 12 Novembre 1974, punto 6.

144 A tal proposito così si è espressa la stessa Corte (Terza Sezione) nella Sentenza Compass-Datenbank (C-138/11) del 12 luglio 2012. Il caso prendeva le mosse dall'attività svolta dalla Compass Datenbank, società a responsabilità limitata di diritto austriaco. Nel 1984 tale società aveva messo a punto una banca elettronica di dati economici, che veniva costantemente aggiornato e integrato attraverso la consultazione del Firmenbuch, il registro delle imprese austriache. In seguito a una procedura d'appalto indetta dalla repubblica austriaca nel 1999, era stato stabilito che fosse affidata a varie imprese l'istituzione di agenzie intermediarie per la trasmissione, a pagamento (tasse + costo del servizio), dei dati del Firmenbuch. Nel 2001 la Repubblica Austriaca aveva adito il tribunale commerciale di Vienna al fine di vietare alla società l'uso dei dati del Firmenbuch, compresa la memorizzazione, riproduzione o trasmissione ai terzi. Giunti dinanzi alla Corte di Giustizia Europea per un rinvio pregiudiziale vertente sull'interpretazione dell'art. 102 TFUE (divieto di abuso posizione dominante), al fine di comprendere se tale articolo debba estendersi anche le imprese pubbliche esercitanti un'attività economica.

145 Sileoni, S., *"Il diritto alla cancellazione dei dati e le attività economiche: una nuova visione del tempo,* cit. In merito alla nozione di "terzi", la Corte definì già nella Causa Daihatsu Deutschland (C-97/96) del 4 Dicembre 1997 cosa dovesse intendersi con tale espressione alla luce della direttiva 68/151. La corte statuì che *"Le disposizioni dell'art. 3 della direttiva, che prevedono la tenuta di un registro pubblico nel quale devono essere registrati tutti gli atti e le indicazioni soggetti all'obbligo della pubblicità nonché la possibilità per chiunque di ottenere copia dei conti annuali per corrispondenza, confermano l'intento di consentire a qualsiasi interessato di ottenere informazioni.*" Nella Causa Springer (Cause riunite C-435/02 e C-103/03 del 23 Settembre 2004). al paragrafo 29 e 33 i giudici hanno poi specificato che alla luce dell'art. 54 n. 3 let g) del Trattato CE (soppressione dei limiti alla libertà di stabilimento), la nozione di terzi vada interpretata in senso estensivo, *"senza distinguere o escludere talune categorie"*, giacché *"non può limitarsi...ai soli creditori della società"*

disposizioni della presente direttiva, in particolare a causa del carattere incompleto o inesatto dei dati" (art. 12 co.1, lett b). Da contraltare a questi diritti in capo all'interessato, i giudici menzionarono l'articolo 7 che stabilisce che gli Stati possano disporre che il trattamento di dati personali possa effettuarsi solo in presenza di una delle seguenti circostanze: *"a) la persona interessata ha manifestato il proprio consenso in maniera inequivocabile; b) è necessario all'esecuzione del contratto concluso con la persona interessata o all'esecuzione di misure precontrattuali prese su richiesta di tale persona; c) è necessario per adempiere un obbligo legale al quale è soggetto il responsabile del trattamento; d) è necessario per la salvaguardia dell'interesse vitale della persona interessata; e) è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il responsabile del trattamento o il terzo a cui vengono comunicati i dati; f) è necessario per il perseguimento dell'interesse legittimo del responsabile del trattamento oppure del o dei terzi cui vengono comunicati i dati, a condizione che non prevalgano l'interesse o i diritti e le libertà fondamentali della persona interessata, che richiedono tutela ai sensi dell'articolo 1, paragrafo 1.*"

Passando alla risoluzione delle questioni pregiudiziali sollevate dalla Corte di Cassazione italiana, innanzitutto la Corte volle chiarire alcuni aspetti.
In primo luogo, richiamò l'articolo 2, par.1, lett. d) della direttiva 68/151 relativa agli atti societari su cui insiste l'obbligo di pubblicità (si rimanda alla lettura della nota 118) e l'articolo 3, par. 1-3 (obbligo tenuta registro imprese per ogni Stato membro). In relazione alle indicazioni relative alle generalità delle persone del summenzionato articolo 2, in quanto esse rappresentano informazioni concernenti persone fisiche identificate o identificabili, costituiscono dati personali e da ciò ne deriva che la loro trascrizione, comunicazione ed eventuale comunicazione a terzi implica lo svolgimento di un trattamento di dati personali, per cui l'autorità si rende "responsabile".

In secondo luogo, i giudici ripresero quanto affermato nella sentenza Google Spain, ribadendo che la direttiva 95/46 mira a garantire un elevato livello di tutela delle libertà e dei diritti fondamentali, in particolare il diritto alla vita privata, con riferimento al trattamento dei dati personali: quest'ultimo deve rispondere sia al

principio di qualità dei dati (art. 6), sia essere conforme al principio relativo alla legittimazione dei trattamenti dei dati (art. 7)[146].

E proprio sull'articolo 7 la Corte fece "perno" per giustificare la conformità dell'azione dell'autorità pubblica nel trattamento dei dati personali presente nel registro delle imprese: tale attività di raccolta dei dati della vita delle imprese risponde non solo a un obbligo legale (lett c art. 7), ma anche all'esecuzione di un compito di interesse pubblico[147] (lett e art 7) e al perseguimento di un interesse legittimo dei terzi (lett f art 7). La questione era stabilire se per i fini elencati all'articolo 3 della direttiva 68/15, fosse necessario che i dati personali delle persone fisiche restassero indicati e accessibili per qualunque terzo anche dopo la cessazione dell'attività e lo scioglimento della società. Preso atto che tale direttiva non specificava nulla al riguardo, i giudici assecondarono la prospettiva descritta nelle conclusioni dell'avvocato generale, per cui è da considerarsi *"pacifico, che anche dopo lo scioglimento di una società, possano residuare diritti e rapporti giuridici ad essa relativi",* tanto da risultare necessario la possibilità di accedere e reperire i dati del registro, qualora ad esempio si questioni la legittimità di un atto compiuto a nome

146 Sentenza della Corte di Giustizia Europea (Seconda Sezione), Causa C-398/15 del 9 Marzo 2017, par. 41.

147 Come già sancito dalla sentenza Sentenza Compass-Datenbank (C-138/11) del 12 luglio 2012., par. 40 e 41. Consta segnalare poi che la CGE già si era espressa in merito al rapporto tra poteri dell'autorità e dati personali dei singoli nel precedente caso Worten (Sentenza della CGE (Terza Sezione) Causa C-342/12 del 30 Maggio 2013). La controversia tra la Worten, società portoghese, e l'ACT, Autorità di vigilanza sulle condizioni di lavoro nasceva da un'ispezione effettuata nello stabilimento dell'impresa che aveva però presentato alcune irregolarità, su tutte l'impossibilità da parte dell'ACT di consultare immediatamente il registro dell'orario di lavoro. La Corte sancì che le disposizioni della direttiva 95/46 *"non ostano ad una normativa nazionale che impone al datore di lavoro l'obbligo di mettere a disposizione dell'autorità nazionale competente in materia di vigilanza sulle condizioni di lavoro il registro dell'orario di lavoro al fine di consentire la consultazione immediata, nella misura in cui tale obbligo sia necessario ai fini dell'esercizio da parte di detta autorità delle sue missioni di vigilanza dell'applicazione della disciplina in materia di condizioni di lavoro, in particolare per quanto riguarda l'orario di lavoro".* Due le differenze rispetto al caso Manni. Nel primo caso ci si riferisce a dati consistenti in fatti privati del dipendente e soggetti a un autorità pubblica che detiene poteri di controllo e sanzione, mentre nel secondo caso i dati consistono in informazioni societarie, pubblicate in un registro pubblico ai fini della realizzazione di une mera funzione di pubblicità. Sul punto, si veda Alpa, G., Conte, G. (a cura di), *Casi decisi dalla Corte di Giustizia dell'Unione europea sui diritti fondamentali in materia contrattuale* cit., pag. 47.

della società o nel caso in cui i terzi intendano avviare un'azione contro i membri degli organi della società o contro i liquidatori[148]. Stante la diversità di termini di prescrizione applicabili nei diversi Stati membri per esperire le azioni civili e commerciali, la diversità di interessi che i terzi possono "nutrire" per ottenere la consultazione dei registri e la possibile esistenza di rapporti giuridici coinvolgenti soggetti di diversi Stati Membri, non appare adeguato predisporre un termine univoco entro il quale tali interessi siano da considerarsi venuti meno[149]. Per tale motivo, la CGE sancì che *"gli Stati Membri, in virtù dell'articolo 6, paragrafo 1, lettera e), e dell'articolo 12, lettera b), della direttiva 95/46, non sono tenuti a garantire alle persone fisiche di cui all'articolo 2, paragrafo 1, lettere d) e j), della direttiva 68/151 il diritto di ottenere, in ogni caso, decorso un certo periodo di tempo dallo scioglimento della società di cui trattasi, la cancellazione dei dati personali che le riguardano ...o il congelamento degli stessi nei confronti del pubblico".*

Questa interpretazione degli articoli citati, sempre a detta della Corte, non provoca un'ingerenza sproporzionata nei diritti fondamentali delle persone interessate espressi dagli art. 7 e 8 della Carta. Tale asserzione si giustifica con il fatto che la direttiva 68/151 impone la pubblicità limitatamente a taluni dati personali, quali l'identità e le rispettive funzioni delle persone in grado di obbligare la società (lettere *d* e *j* art 2.). Questa esigenza appare adeguata alla luce del rischio economico che i terzi si trovano ad affrontare, dal momento che nelle società per azioni e nelle società a responsabilità limitata l'unica garanzia a loro favore è costituita dal patrimonio sociale[150].

L'esigenza di tutelare l'interesse dei terzi nei confronti delle società per azioni e delle società a responsabilità limitata e di garantire la certezza del diritto, la trasparenza nelle transazioni commerciali e il buon funzionamento del mercato interno, può tuttavia trovare un limite, qualora in via eccezionale sussistano particolari situazioni in cui "ragioni preminenti e legittime", che impongano un accesso ristretto ai dati personali, sia dal punto di vista soggettivo (ai terzi che dimostrino un interesse

148 Sentenza Compass-Datenbank (C-138/11) del 12 luglio 2012., par. 53.

149 Si vedano le Conclusioni dell'Avvocato Generale Yves Bot, Causa C-398/15, 8 Settembre 2016. par. 80

150 Sentenza della Corte di Giustizia Europea (Seconda Sezione), Causa C-398/15 del 9 Marzo 2017, par. 58-59

specifico) sia dal punto di vista oggettivo (decorso un periodo di tempo sufficientemente lungo dopo lo scioglimento della società)[151]. Ne deriva che ex articolo 14, co.1 let a) della direttiva 95/46, la decisione finale in merito alla possibilità che le persone fisiche ottengano una limitazione all'accesso dei dati personali, spetta ai legislatori e di rimando ai giudici nazionali, in base a una valutazione caso per caso[152] e a un'analisi delle normative in vigore sul tema.

La CGE concluse affermando in primo luogo che sarebbe spettato al giudice di rinvio decidere in merito al caso di specie; in secondo luogo tuttavia rilevava che il solo presumere che gli immobili di un complesso turistico non venissero venduti per la presenza dei dati del sig. Manni all'interno del registro delle imprese, non soddisfaceva il requisito della ragione "preminente e legittima".

Rimessa la questione al giudice italiano, la Cassazione ha provveduto con sentenza non solo a cassare la sentenza del Tribunale di Lecce, ma anche a decidere nel merito la causa[153] – non essendo necessari ulteriori accertamenti in fatto -, con il rigetto delle domande proposte contro la Camera di commercio[154]. Il principio di diritto affermato dalla sentenza in questione è il seguente: "*Alla stregua del quadro normativo e dei compiti istituzionalmente perseguiti dalle Camere di commercio con la tenuta del registro delle imprese, è legittima, rispondendo ad un obbligo legale, l'iscrizione e la conservazione nel registro stesso delle informazioni relative alla carica di amministratore e di liquidatore, ricoperta da un soggetto in una società, ove pure in seguito questa sia stata dapprima dichiarata fallita e, poi, cancellata dal registro delle imprese, prevalendo le esigenze della pubblicità commerciale sull'interesse del privato*

151 *Ibidem*, par. 60

152 *Ibidem*, par. 61

153 Si ricorda che ex art. 384 c.2 c.p.c. , la Corte di Cassazione quando accoglie il ricorso ha due possibilità: rinvia la causa ad altro giudice, il quale dovrà uniformarsi al principio di diritto e a quanto statuito da essa stabilito oppure decide la causa nel merito qualora non sia necessario compiere ulteriori accertamenti in fatto.

154 La Corte di Cassazione accolse il primo motivo di ricorso (rigettando gli altri sei) sollevato dalla Camera di Commercio di Lecce in merito alla violazione degli art. 18 e 19, 3° co. del d. lgs 30 giugno 2003 nella parte in cui finisce per negare la funzione istituzionale della pubblicità legale del registro delle imprese. Si veda Cassazione Civile (Prima Sezione), sentenza n. 19761 del 9 Agosto 2017, par. 7.

ad impedirla, in funzione delle ragioni di certezza nelle relazioni commerciali che l'istituzione del registro delle imprese soddisfa"[155].

Il punto centrale della sentenza che conclude la vicenda Manni sembra però essere un altro. Per la Corte di legittimità, nell'opera di bilanciamento tra interesse del singolo e interesse della comunità, il principio guida è quello rappresentato dall'articolo 2 della Costituzione. La Corte stigmatizza che *"in epoche in cui l'accento, pur in sé corretto, posto sui diritti ha gradualmente indotto a guardare ai doveri come ad un puro e fastidioso accidente, l'eccesso d'individualismo finisce per soffocare l'interesse comune della generalità, nella ricerca confusa ed esclusiva di una gratificazione personale che tuttavia nega, a lungo andare, la premessa: la tutela di ogni diritto fondamentale non può ignorare la dimensione collettiva del bene comune e l'esistenza di un correlativo obbligo"*[156]. Ciò sta a significare che, sebbene le prerogative relative alla protezione dei dati personali siano legittime, esse devono confrontarsi con il principio di solidarietà sancito dall'articolo 2 della Costituzione in un'opera di mediazione tra esigenze individuali e esigenze della collettività, a maggior ragione quando il soggetto opera ed estrinseca la propria personalità all'interno del mercato.

3.5 Considerazioni e valutazioni sulla sentenza Manni

Come è stato espresso nella sentenza Google Spain, il diritto all'oblio talvolta può subire limitazioni, quando per ragioni particolari, come il ruolo ricoperto dal soggetto nella vita pubblica, l'ingerenza nei suoi diritti fondamentali è giustificata in virtù dell'interesse preponderante del pubblico ad avere accesso a determinate informazioni.

Il caso Manni e il caso Google Spain presentano indubbiamente alcune similitudini. In primo luogo, in entrambi la controversia sollevate dalle corti nazionali si è basata sulla possibilità da parte dei soggetti di richiedere la rimozione o il blocco dei loro dati o informazioni personali nei confronti di soggetti terzi che si occupano del trattamento dei loro dati. In entrambi i casi la Corte di Giustizia Europea ha riconosciuto che tanto i motori di ricerca (soggetto privato) quanto le Camere di

155 *Ibidem*, par. 5.3.6.

156 *Ibidem*, par. 5.3.6

Commercio (ente pubblico) che curano i registri delle imprese sono responsabili del controllo dei dati di cui dispongono: essi svolgono attività che rientrano senz'alcun dubbio all'interno della definizione "trattamento di dati personali" descritta dall'art. 2 lett. b) della direttiva 95/46.

Esistono anche alcune differenze tra le due vicende che meritano di essere analizzate. Innanzitutto sul versante dei diritti in gioco, nel caso Google Spain il diritto alla vita privata e la tutela dei dati personali si trovano in conflitto sia con la libertà di garantire la libertà di informazione ed espressione al fine di assicurare il pubblico accesso alle informazioni, sia con la libertà d'impresa in relazione all'attività del motore di ricerca; nel caso Manni l'interesse in conflitto con la tutela e il controllo dei propri dati consiste nella garanzia di trasparenza nei rapporti commerciali, nella certezza del diritto e nel buon funzionamento del mercato interno.

Altra differenza consistente si riflette sullo scopo per cui vengono raccolti i dati in questione. L'attività dei motori di ricerca non è indirizzata al perseguimento di un interesse pubblico riconosciuto o imposto dalla legge come quello ravvisabile per la conservazione delle informazioni all'interno del registro delle imprese. Anzi si può dire che la raccolta, la conservazione, la memorizzazione e la messa a disposizione di dati rappresenta il *core business* dei motori di ricerca, dal momento che il ricorso al loro utilizzo dipende dalla quantità e qualità dei dati rintracciabili da parte degli utenti. Il fatto che tale attività non rivesta una funzione pubblica, non deve indurre a pensare che essa non sia oggetto di tutela alla luce dei diritti prima menzionati, seppur indubbiamente costituisca una tutela di entità minore.

Inoltre, al fine di valutare il pubblico interesse all'accesso delle informazioni rileva anche il ruolo pubblico che riveste il soggetto a cui appartengono: nella vicenda spagnola il signor Gonzales era un privato cittadino e per questa ragione la Corte di Giustizia Europea ha considerato sproporzionato il mantenimento di vecchie vicende personali tra i risultati della ricerca web; nella vicenda italiana invece sebbene il sig. Manni non sia una figura nota al pubblico o che rivesta un ruolo pubblico, l'informazione conservata nei registri è assicurata dalla legge in ordine alla garanzia di trasparenza tra società e terzi che intende perseguire il registro delle imprese[157].

157 Pollicino, O, De Gregorio, G, *Privacy or Transparency? A new balacing of interests for the right to be forgotten of personal data published in public registers* in The Italian Law Journal 3 (2), Dicembre 2017, cit. pag. 658-659

Assunta tale distinzione, la domanda che sorge spontanea è se l'associazione di una persona all'infelice esito di una vicenda societaria debba essere perpetua o se vi debba essere un momento in cui sia giusto restituire l'immacolatezza alla quale il soggetto ambisce[158]. In un contesto quale quello immobiliare italiano, colpito pesantemente dalla crisi economica, da una scarsa propensione agli investimenti e dal luogo comune che considera un fallimento nella vita di un imprenditore come un "peccato capitale non emendabile"[159], l'accessibilità indiscriminata e temporalmente indefinita dei dati afferenti a processi di fallimento e liquidazioni risalenti a quindici anni prima costituisce un danno non indifferente sotto il profilo dell'immagine imprenditoriale allorché il soggetto intenda intraprendere una nuova attività.

Quest'aspetto risulta non da meno enfatizzato dalla progressiva digitalizzazione che ha consentito una rapida e ampia circolazione dei dati estratti dal registro delle imprese, dando luogo potenzialmente a effetti discriminatori sul piano personale: si pensi ad esempio alle conseguenze che tali informazioni possono dettare sulla concessione o meno di un finanziamento o sull'influenza che possono avere all'interno di un processo di selezione per una posizione lavorativa[160]. D'altronde, a differenza di quanto sancito dai giudici europei, l'Avvocato General Yves Bot ha sostenuto che *"la circostanza che una società sia stata dichiarata fallita può costituire, dal punto di vista dell'acquirente, un elemento determinante all'atto di acquisto[161]".* In via generale, ancorché sia giustificabile una limitazione dei diritti dei soggetti che hanno deciso di operare attivamente nel mondo degli affari assumendone le relative responsabilità, appare al contrario meno giustificabile un annullamento pressoché totale dei diritti di protezione dei dati personali, se il rischio è quello che vadano ad inficiare in modo perdurante la garanzia di altri diritti di rilevanza costituzionale,

158 Pappalardo, M. , *L'accesso al registro delle imprese tra garanzia di trasparenza e diritto all'oblio* in Le Società, 2017, n.7, p. 820 e ss.

159 Musselli, L., *Trasparenza versus privacy nella pubblicazione dei dati personali nel registro delle imprese* in DPCE Online, v. 31, n.3, Ottobre 2017, pag. 734.

160 Pappalardo, M., *L'accesso al registro delle imprese tra garanzia di trasparenza e diritto all'oblio* cit., pag. 832.

161 Conclusioni dell'Avvocato Generale Yves Bot, Causa C-398/15, 8 Settembre 2016. par. 79

quali il diritto al lavoro (art. 4 Cost. e la libertà di iniziativa economica (art. 41 Cost)[162].

Per altro verso, lo stesso Avvocato Generale ha condiviso l'opinione del governo tedesco, il quale ha sottolineato il fatto che quando un soggetto intende partecipare agli scambi commerciali mediante l'utilizzo di una società commerciale, è conscio di dover essere disposto a condividere pubblicamente determinate informazioni; ed è pure conscio che queste informazioni verranno iscritte nel registro delle imprese, finendo per divenire disponibili a prescindere dagli eventi che contrassegnano le vicende della società[163]. Inoltre, come riportato prima dall'Avvocato Generale poi anche dalla sentenza conclusiva della Suprema Corte, il fatto che una società sia stata assoggettata al regime della procedura concorsuale o al fallimento non implica necessariamente una lesione all'onorabilità o alla reputazione dell'amministratore che l'ha rappresentata, in quanto il fallimento ben può dipendere da circostanze esterne, quali un trend economico negativo o un calo della domanda nel settore in cui la società opera. A testimonianza di questo mutamento del sentire sociale, basti guardare alle riforme in materia di diritto fallimentare dell'ultimo decennio[164].

Ulteriore problema, soltanto sfiorato dalla Corte di legittimità nel caso Manni, è quello relativo al trattamento effettuato da società specializzate in valutazioni di rischio. All'origine della doglianza del ricorrente pare esserci in fin dei conti non tanto la conoscibilità delle informazioni del registro, bensì il successivo trattamento a fini commerciali che i dati hanno subito[165]. Nell'ordinanza di rimessione, in un *obiter*

162 In tal senso va l'opinione di Pappalardo, M., *L'accesso al registro delle imprese tra garanzia di trasparenza e diritto all'oblio* cit., pag. 832.

163 "Si tratta della contropartita dell'esercizio di un'attività sotto forma di una società che gode di personalità giuridica". Si rimanda ancora una volta a Conclusioni dell'Avvocato Generale Yves Bot, Causa C-398/15, 8 Settembre 2016. par. 84.

164 A tal proposito proprio in questi mesi è stata approvata dal governo da parte del governo della legge delega n.155 del 19 Ottobre 2017 in materia di riforma delle procedure concorsuali. Oltre alla previsione di alcune norme orientate alla concedere benefici all'imprenditore nel caso in cui l'imprenditore si attivi prontamente a segnalare la crisi aziendale (art. 324 – Esenzioni dai reati di bancarotta), il vero principio manifesto della riforma consiste nella sostituzione dell'espressione "fallimento" con il termine "liquidazione giudiziale": l'obiettivo è proprio quello di evitare il discredito sociale e personale che normalmente si accompagna alla parola "fallito".

165 La sola consultazione del registro non avrebbe permesso di collegare il dato del fallimento al nominativo dell'interessato, se non si fosse conosciuta già la ragione sociale della società di cui il

dictum la Cassazione ha evidenziato che *"sulla base della normativa europea ed interna, sembrerebbero, invero, individuabili periodi di tempo massimi di permanenza dei dati rispetto alle finalità perseguite unicamente ove trattati dai soggetti privati che utilizzano i medesimi a fini di informazione commerciale per così dire derivata e rielaborata, decorsi i quali determinati dati dovrebbero quindi essere consultabili solo nel registro delle imprese*[166]*".* I giudici sembrano propensi a individuare un regime differente per quanto concerne il riuso delle informazioni personali per finalità commerciali ad opera di privati[167]: secondo tale indirizzo, la società commerciale menzionata nel caso (Cerved Business Information), diversamente dalla Camera di Commercio, potrebbe essere tenuta a cancellare o trasformare in forma anonima le informazioni personali del richiedente, qualora esse siano diventate obsolete e prive del carattere di attualità funzionale all'interesse commerciale di conoscenza dei terzi[168]. Lo stesso orientamento sembra essere apprezzato anche dal Garante per la protezione dei dati personali, che nel settembre 2015 ha varato il "Codice di deontologia e di buona condotta per il trattamento dei dati personali effettuato a fini di informazione commerciale". Tale documento ha l'aspirazione di regolare i dati presenti all'interno dei pubblici registri e il trattamento di questi nel caso essi vengano utilizzati da agenzie specializzate a fini commerciali per la vendita a soggetti terzi. Per quanto concerne i tempi di conservazione, il Codice deontologico dispone vari criteri temporali da seguire a seconda della natura delle informazioni di cui si entra in possesso.

Le informazioni relative a fallimenti o procedure concorsuali possono essere conservati per un tempo non superiore a 10 anni dalla data di apertura della procedura fallimentare. Trascorso questo periodo, le informazioni possono essere ulteriormente utilizzate dal fornitore, solo quando risultino presenti altre informazioni riguardanti un ulteriore fallimento o nel caso in cui risulti avviata una

---

sig. Manni era liquidatore, dal momento che all'epoca non era possibile effettuare una ricerca diretta in base al nominativo del soggetto. Mantelero, A., *Diritto all'oblio e pubblicità del registro delle imprese* in Giurisprudenza Italiana, 2015, pag. 2658

166 Corte di Cassazione Civ. (prima Sezione), ordinanza n. 15096/15 del 17 Luglio 2015, par. 4.4.9.

167 Mantelero, A., *Diritto all'oblio e pubblicità del registro delle imprese* cit., pag. 2655 e ss.

168 Berti, A. S., *La pubblicità legale dei registri delle imprese prevale sul diritto all'oblio dei dati personali ivi inseriti,* in Giustizia Civile. Com (periodico online), vol. 4. fascicolo 7, 2017, pag. 7.

nuova procedura fallimentare o concorsuale riferita al soggetto o ad altro soggetto connesso: in questo caso il trattamento può prolungarsi di altri dieci anni.
Per le informazioni relative ad atti pregiudizievoli ed ipocatastali le informazioni possono essere utilizzate decorso un periodo di 10 anni dalla trascrizione o iscrizione, salva l'intervenuta cancellazione prima di tale termine che limita a un periodo di 2 anni la conservazione dei relativi dati[169].
Ad ogni modo, parte della dottrina ritiene che non si possa trascurare il fatto che la pubblica disponibilità del dato attraverso l'accesso al registro sia di per sé idonea a esporre il soggetto al rischio che tali informazioni possano essere usate in modo improprio anche a distanza di anni[170]. Secondo Pappalardo, l'indicazione di precisi limiti temporali nel codice deontologico, dovrebbe suggerire al legislatore l'adozione del medesimo criterio per disciplinare l'accesso al registro delle imprese[171].

3.6 Alcune riflessioni: il fattore tempo

Nel bilanciamento tra diritto alla protezione dei dati personali e tutela del mercato, la Corte ha statuito che soltanto in via eccezionale e in caso di interesse legittimo e preminente, il singolo può vantare l'oblio dei suoi dati personali raccolti nel registro pubblico delle imprese. Questa temperamento "caso per caso" attribuisce un ruolo importante alle autorità incaricate della tenuta dei registri, le quali ove le normative nazionali lo permettano, e in coerenza con le linee guide suggerite dalle Autorità Garanti per la protezione dei dati, potranno procedere all'anonimizzazione o al blocco dei dati societari concernenti vicende societarie oramai superate. Ciò non toglie che si rende auspicabile un intervento del legislatore nazionale, sebbene comunque il GDPR

169 Il testo integrale del Codice è rinvenibile al sito https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/4298343

170 In tal senso Pappalardo, M. , *L'accesso al registro delle imprese tra garanzia di trasparenza e diritto all'oblio* cit. pag. 832*; Mantelero, A., Diritto all'oblio e pubblicità del registro delle imprese cit., pag. 2655 e ss.*

171 Pappalardo, M. , *L'accesso al registro delle imprese tra garanzia di trasparenza e diritto all'oblio* cit. pag. 833.

– come si vedrà nel quarto capitolo – abbia perlomeno marcato il territorio entro il quale il diritto all'oblio debba operare.

La chiave di volta dell'intero sistema è senza dubbio il fattore tempo. I rapporti e le relazioni non possono consumarsi automaticamente con lo scioglimento della società stessa. La scelta di un soggetto di impegnarsi nella vita economica tramite una società commerciale, implica accettare un'esigenza di permanente trasparenza[172] La giurisprudenza quindi non ha promosso l'adozione di un diritto all'oblio generalizzato: dinanzi al dogma della certezza del diritto, l'oblio deve cedere il passo.

Tuttavia nella sentenza della Corte di Giustizia Europea è ravvisabile un'espressione che può destare alcune riflessioni, o meglio alcune preoccupazioni. Nella massima della sentenza, la Corte ha infatti esibito cautela nel delineare la sua interpretazione, aggiungendo l'espressione "allo stato attuale del diritto dell'Unione" e alludendo quindi alla possibilità che in futuro tale interpretazione possa essere soggetta a *overrulling*[173].

Il timore è che con il passare del tempo l'oblio acquisisca forza in funzione di un'interpretazione sempre più estesa e *tranchant* dell'articolo 8 della CEDU, specie nella parte in cui richiede la minor ingerenza possibile da parte dell'autorità nei confronti dei dati sensibili dell'individuo attraverso l'adozione di misure adeguate al rispetto della vita privata anche nell'ambito delle relazioni commerciali. Ciò significa che anche la "vita professionale privata" potrà essere preso sotto l'ala dell'articolo 8, generando laddove accada forti dubbi in merito alla possibilità di negare la cancellazione di dati personali contenuti nel registro dell'autorità pubblica. L'articolo 8, nato come strumento per difendere il singolo dalla prepotenza di chi detiene il potere, se trasposto erroneamente nei rapporti d'impresa, potrebbe divenire "una vera e propria arma per scardinare le norme e i limiti non graditi al singolo individuo"[174].

172 Si rimanda alla lettura dell'articolo Loruso, D. S., Gentile, N., (a cura di) Registro delle imprese e trattamento dei dati personali in Ventiquattore Avvocato (Il Sole 24 ore), n.12, dicembre 2016, pag. 52.

173 R. Pardolesi, *L'ombra del tempo e (il diritto al)l'oblio*, in "Questione giustizia", Riv. Trim., n.1, 2017, p. 85

174 Loruso, D. S., Gentile, N., (a cura di) Registro delle imprese e trattamento dei dati personali, pag. 54

Vista in tale ottica, si giungerebbe a una manipolazione del portato dell'articolo 8, che finirebbe per tradirne lo spirito originario trasformandolo in un mezzo per imporre l'interesse individuale sull'interesse della generalità: "un'arma impropria per proteggersi dalla concorrenza".[175] Per questa ragione, a parere di chi scrive diviene fondamentale che il bilanciamento tra i diversi interessi in gioco debba svilupparsi tenendo sempre bene a mente il dettato costituzionale dell'articolo 2, come già saggiamente osservato dalla Corte Costituzionale.

175 Carraro, G., Pubblicità commerciale e diritto all'oblio nella prospettiva dei diritti dell'uomo in La nuova giurisprudenza civile commentata, 2016, v. 32, fascicolo 4, pag. 641.

Capitolo IV: L'introduzione del GDPR: riflessi e considerazioni sull'attività delle imprese.

4.1 L'impatto del GDPR nella vita di un'impresa • 4.2 L'informativa sul consenso al trattamento dei dati personali • 4.3 Il fenomeno del *Data breach* • 4.4 La nomina di un Data Protection Officer • 4.5 Il registro dei trattamenti • 4.6 L'impresa e il rispetto dei diritti dell'interessato • 4.7 In particolare GDPR e Oblio: un bilanciamento tecnico nelle mani delle imprese • 4.8 I costi dell'adeguamento delle imprese al GDPR • 4.8.1 Una prima visione d'insieme • 4.8.2 Valutazione dei costi del GDPR nelle PMI • 4.9 Riflessioni sul principio di responsabilizzazione delle imprese nella gestione dei dati personali

4.1 L'impatto del GDPR nella vita di un'impresa

Con l'introduzione del GDPR tutte le imprese che trattano i dati dei cittadini dell'Unione Europea devono adempiere agli obblighi previsti dalla nuova disciplina. Si può dire che le imprese a partire dalla fatidica data del 25 Maggio 2018, devono prestare particolare attenzione ai seguenti temi: l'informativa del consenso al trattamento dei dati, il cosiddetto fenomeno del *data breach,* la nomina di un Data Protection Officer, i diritti dell'interessato (diritto all'oblio compreso), il registro dei trattamenti. Dopo aver esaminato quanto sopra si comprenderà come il Regolamento fondamentalmente stabilisca il principio generale della responsabilizzazione delle imprese nella gestione dei dati personali.

4.2 L'informativa sul consenso al trattamento dei dati personali

Spesso tra i consumatori o i fruitori di servizi vi è una certa superficialità nella lettura dell'informativa relativa al trattamento dei dati personali. E' opportuno precisare invece che l'informativa costituisce invece uno dei cardini del sistema di

protezione dei dati personali: esso indica come verranno utilizzati i dati, per quanto tempo e per quali finalità, le generalità del soggetto che si accinge a raccogliere ed usare i dati, gli eventuali destinatari. L'informativa risponde non solo al rispetto del diritto individuale ad essere informato, ma anche al dovere del titolare di trattare in forma trasparente e corretta i dati fin dal processo di acquisizione degli stessi. L'informativa ha inoltre lo scopo di permettere che l'interessato possa rilasciare un valido consenso, il quale costituisce la base giuridica del trattamento[176].

Ogni qualvolta vi sia un trattamento di dati, è necessario raccogliere il consenso attraverso l'informativa, a meno che il trattamento non riguardi dati anonimi o dati afferenti enti o persone giuridiche (i cui dati non sono soggetti alla disciplina del GDPR). Il testo originario del Codice Privacy includeva in realtà nella definizione di dati personale *"qualunque informazione relativa a persona fisica, persona giuridica, ente o associazione."* Tale previsione è però venuta meno con il Decreto Legge n.201 del 2011, con cui si è recepito il principio secondo il quale le imprese, gli enti e le associazioni non debbano essere considerati come interessati al trattamento, con la conseguenza che oggi non possono far valere i diritti dell'interessato previsti dagli art. 12 e ss del GDPR[177]. L'obiettivo del legislatore è senz'alcun dubbio quello di semplificare la gestione dei dati nell'ambito dei rapporti tra le imprese, in ossequio al principio di libera circolazione dei dati: di conseguenza le informazioni riguardanti persone giuridiche, enti o associazioni possono essere raccolti, trattati e comunicati a terzi, senza la necessità di una base giuridica.

Esiste tuttavia una zona *border line*, ove il dato personale può riferirsi tanto alla sfera della persona fisica quanto a quella della persona giuridica. Si pensi ad esempio, quando il nome della persona fisica viene ricompreso in parte o totalmente nel nome della denominazione sociale[178]. In tal caso, il considerando n. 14 del GDPR chiarisce che il regolamento non si applica ai dati relativi alle persone giuridiche, compresi

176 Si invita alla lettura della pagina web: https://protezionedatipersonali.it/informativa.

177 Sul fatto che tale disciplina si applichi solo alle persone fisiche, lo si ricava sia dall'articolo 4 del GDPR, che definisce il dato personale come *"qualsiasi informazione riguardante una persona fisica identificata o identificabile."*

178 Si veda l'articolo 2326 c.c. che può ritenersi rinvii alla disciplina della ditta, di cui all'articolo 2563 c.c, secondo il quale la ditta consiste in un segno distintivo che corrisponde al nome commerciale dell'imprenditore quando esercita un'attività economica.

quelli che si riguardano il nome e la forma della persona giuridica e i suoi dati di contatto. In via generale, quando si è in presenza di casi come questo, è utile seguire le indicazioni fornite dal Working Party[179] nel parere 4/2007, ove si invita a seguire i criteri di contenuto, scopo e risultato per stabilire se le informazioni personali si debbano relazionare o meno alla persona giuridica. Certo è, che a parere di chi scrive, qualora ci si trovi dinanzi a tali situazioni di confine, è opportuno nella maggior parte dei casi trattare i dati conformemente al dettato del Regolamento.

In relazione al consenso, altra situazione che merita di essere accennata è quella che si verifica quando la raccolta di dati avviene per "uso strettamente personale", svincolata quindi da connessioni con un'attività o un fine economico. La nozione di uso strettamente personale va interpretata nel senso che è consentito il trattamento di dati senza consenso quando esso viene effettuato nella sfera esclusivamente personale o domestica della persona che procede al trattamento: va da sé quindi che la sola pubblicazione di foto sul web costituisce trattamento soggetto alla disciplina in materia di data protection[180]. Al considerando n. 18 del GDPR si afferma che *"le attività a carattere personale o domestico potrebbero comprendere la corrispondenza e gli indirizzari o l'uso dei social network e attività online intraprese nel quadro di tali attività".* Se da un lato con questa disposizione il legislatore europeo ha inteso estendere l'applicabilità dell'eccezione, dall'altro lato non si comprende perché lo stesso considerando afferma l'applicabilità del GDPR *"ai titolari del trattamento o ai responsabili del trattamento che forniscono i mezzi per trattare i dati personali nell'ambito di tali attività a carattere personale o domestico".*

Ancora una volta si addossa all'impresa privata (il provider dei servizi in questo caso) un ruolo che va oltre le legittime aspettative di controllo: il controllo sulle pubblicazioni degli utenti implica di fatto chiedersi se sarà compito del provider

179 Il Gruppo dell'articolo 29 per la tutela dei dati (o Article 29 Working Party) era un organismo consultivo costituito da un rappresentante delle varie autorità nazionali, dal garante europeo della protezione dei dati e da un rappresentante della Commissione Europa. Era incaricato di formulare pareri e raccomandazioni non vincolanti sull'adozione o sull'interpretazione di norme relative al trattamento dei dati personali e alla privacy. Oggi è stato sostituito dal Comitato Europeo per la protezione dei dati ex art- 68 GDPR.

180 In tal senso, la già citata sentenza Lindqvist, C.101/01 della Corte di Giustizia Europea del 6 Novembre 2003.

garantire la correttezza, l'esattezza e l'aggiornamento nonché il diritto all'oblio di dati pubblicati nell'ambito di attività a carattere personale e domestico.
Infine, rispetto alla precedente normativa il GDPR ha introdotto criteri più stringenti in relazione alla forma e alle modalità con cui viene rilasciato il consenso. Ex art 4, par. 11, per "consenso dell'interessato" si intende *"qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento."*

Vale a dire che in primo luogo il consenso per essere libero non deve essere inserito all'interno di una parte non negoziabile di termini e condizioni generali di contratto /servizio: ad esempio, se un'applicazione mobile per la riproduzione di contenuti musicali subordina l'accesso al servizio alla condivisione della localizzazione GPS, pur non essendo necessario per la fruizione del servizio, in tal caso il consenso non può ritenersi prestato liberamente. Il regolamento vuole evitare che l'autorizzazione al trattamento dei dati personali di un soggetto finisca per divenire una controprestazione contrattuale da offrire (o da dover sacrificare) per l'esecuzione di un contratto o l'erogazione di un servizio. L'impresa deve quindi prestar ben attenzione a non accorpare due momenti che devono rimanere ben distinti: il consenso all'utilizzo dei dati di un soggetto e l'esecuzione del contratto[181]. Per evitare queste situazioni di accorpamento, è fondamentale che il titolare del trattamento applichi il principio della minimizzazione dei dati personali, nel senso che vanno raccolti e utilizzati soltanto quei dati necessari al raggiungimento dello scopo per i quali sono stati richiesti (art 5 e 6 GDPR). A maggior ragione l'attenzione verso la liceità del consenso va tenuta in considerazione stante l'onere della prova in capo al titolare del trattamento sancito dall'articolo 7, co. 1 del Regolamento.

In secondo luogo, per consenso specifico si intende che in caso di un servizio che comporta più scopi, esso deve essere liberamente presentato per ciascuno scopo. Non è più possibile, come spesso avveniva nell'era pre-GDPR, sottoporre agli interessati consensi generici afferenti a distinti trattamenti di dati personali. Si parla quindi di

181 Si vedano le "Linee guida sul consenso ai sensi del regolamento UE 2016/679" (wp259rev.01) adottate dal Gruppo di lavoro Articolo 29, pag 8-9 rintracciabili al sito https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051 (aggiornato al 20 Gennaio 2019)

granularità del consenso, per cui qualora una società commerciale intenda inviare comunicazioni di marketing tramite posta elettronica, essa è obbligata ad ottenere un consenso specifico differente da quello rilasciato dall'utente per la fruizione dei suoi servizi o per l'acquisto dei suoi beni[182].

In terzo luogo, il GDPR richiede che il consenso sia informato, nel senso che sia ispirato al principio di trasparenza. Sul punto, la novità introdotta dal GDPR si individua sulla comprensibilità del linguaggio utilizzato: esso deve apparire chiaro, semplice, accessibile. L'interessato deve comprendere gli elementi pertinenti per compiere una scelta ponderata e informata sulle conseguenze derivanti dal suo consenso.

Infine, il consenso deve essere inequivocabile, cioè manifestato con un'azione o una dichiarazione positiva inequivocabile quale una dichiarazione scritta, la compilazione di un modulo elettronico, l'invio di una mail, il caricamento di un documento scansionato firmato, la registrazione di una dichiarazione orale, la verifica del consenso tramite sistema a due fasi.

4.3 Il fenomeno del *Data breach*

Con il termine *data breach* ci si riferisce a una violazione di sicurezza che comporta accidentalmente o illecitamente la perdita, la distruzione, la modifica, la divulgazione o accesso non consentiti di dati personali trasmessi, conservati o trattati. L'articolo 33 del GDPR ha introdotto un obbligo di notifica tale per cui in caso si verifichi tale violazione, il titolare del trattamento deve notificare la violazione all'autorità di controllo competente (in Italia il Garante della Privacy) senza ingiustificato ritardo e quando possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, salvo che appaia improbabile che la violazione possa rappresentare un rischio per i diritti e le libertà delle persone fisiche. La notifica deve contenere la natura della violazione, le categorie e il numero degli interessati (ove possibile), la comunicazione dei dati di contatto del responsabile della protezione dei dati, la descrizione delle possibili conseguenze della violazione, la descrizione delle misure

182 Per un'analisi approfondita sul tema della "granularità" del consenso, si rimanda a https://www.privacy.it/2018/01/18/consenso-gdpr-linee-guida-garanti-europei/

adottate per porre rimedio alla situazione in modo da attenuare le conseguenze negative. Ex art. 34, se la suddetta violazione è tale da provocare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento deve comunicare all'interessato o agli interessati la violazione senza ingiustificato ritardo. Tale comunicazione può essere evitata qualora il titolare del trattamento abbia adottato misure tecniche atte a rendere incomprensibili i dati personali violati (es: cifratura dei dati) o quando, a violazione già avvenuta, si sia adoperato per evitare l'insorgenza di rischi elevati per i diritti e le libertà degli interessati. Qualora invece la violazione richieda sforzi sproporzionati, in tal caso si deve procedere tramite comunicazione pubblica o misura equivalente, tramite la quale gli interessati siano in grado di venire a conoscenza di tale violazione.

Resta comunque salvo l'obbligo sancito dal par. 5 dell'art. 33 del Regolamento di raccogliere all'interno dell'apposito Registro delle violazioni tutti i casi di data breach subiti (con relative misure e provvedimenti adottati), anche quando non si sia ritenuto necessario notificarlo alle Autorità di controllo o ai diretti interessati.

Una violazione di sicurezza all'interno di un'impresa può avvenire per svariati motivi. Si pensi a situazioni dettate da errori quali ad esempio l'errata consegna di informazioni sensibili a un destinatario sbagliato, l'errata pubblicazione di notizie private in una pagina web, la mancata o errata distruzione dei dati non più necessari. Altre violazioni possono invece provenire da attacchi informatici, di solito attraverso tecniche di phishing volte all'ottenimento di credenziali di accesso. Per prevenire tali situazioni, l'impresa dovrebbe tracciare il comportamento degli utenti allo scopo di identificare comportamenti sospetti, curare in maniera dettagliata la progettazione delle applicazioni web nonché rafforzare misure e metodi di autenticazione. Altro motivo di violazione può consistere nell'infedeltà di un dipendente che in forza dei privilegi concessi, può accedere e trasmettere dati sensibili. In questo caso le precauzioni da adottare consistono in una gestione precisa dei diritti di accesso di ciascun dipendente o utente con relativa tracciabilità delle attività nelle aree ritenute più a rischio.

Alla luce dei rischi prospettati, le imprese possono adottare piccoli accorgimenti tecnici, ma anche di principio per evitare casi di data breach. Innanzitutto, occorre rafforzare e rivolgere grande attenzione anche alla sicurezza fisica, dal momento che

secondo il Verizon Data Breach Report del 2016 su 2274 casi analizzati di violazioni alla sicurezza, circa il 10 % è imputabile a sottrazioni fisiche di materiale contenente dati personali[183]. Ciò non toglie che la maggior parte delle violazioni avvenga attraverso l'utilizzo di strumenti informatici. Anche una protezione di base costituita dalla crittografia dei dati sensibili, dall'autenticazione a due fattori, dall'applicazione costante e rapida delle patch una volta individuate delle vulnerabilità nella sicurezza di un programma informatico, possono essere essenziali per limitare o perlomeno scoraggiare eventuali attacchi informatici.

Altri due aspetti su cui un'impresa, anche di piccole o medie dimensioni, dovrebbe concentrarsi sono la formazione del personale e l'istituzione di un comitato data breach. La formazione adeguata e costantemente aggiornata del personale dipendente appare una misura quanto mai basilare: gli addetti ai lavori incaricati di gestire e trattare dati personali devono essere il primo anello della catena di sicurezza di un'azienda. Accanto a questo, è necessario tuttavia stabilire anche ruoli e responsabilità dei processor (responsabili del trattamento) tramite adeguate clausole contrattuali con il titolare del trattamento. L'istituzione di un comitato per il data breach composto da persone con competenze trasversali (legal, IT, Marketing…) costituisce senz'alcun dubbio una soluzione concreta per reagire in maniera rapida e corretta al fenomeno del data breach[184]. Come anticipato, sarà l'impresa che dovrà valutare l'eventuale comunicazione della violazione all'autorità. E su questo aspetto pesa non solo la mitigazione della sanzione nel caso la violazione sia comunicata o comunque "riparata" da opportuni interventi, ma anche l'influenza che avrà la perdita dei suddetti dati, i quali costituiscono un asset strategico per l'azienda[185].

E' notizia recente la pubblicazione da parte del Garante dei dati relativi alle segnalazioni di data breach avvenute nel periodo 25 maggio 2018 – 31 Dicembre

183 Secondo il rapporto Verizon, compagna di telecomunicazioni statunitense, ogni anno stila un rapporto riportante statistiche e dati relativi a casi di data breach volontariamente riportati dalle aziende, analizzandone cause, effetti e ragioni. Si invita alla lettura del rapporto dell'anno 2016 al sito http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf (aggiornato al 25 Gennaio 2019).

184 Sulla questione, si veda l'interessante spunto offerto da Diego Padovan (DPO e amministratore DPO Compliance Consulting) nella sua guida *Data Breach e GDPR: gestire la crisi con procedure corrette* rinvenibile alla pagina web https://www.cybersecurity360.it/legal/data-breach-le-procedure-corrette-per-gestire-la-crisi.

2018: sono state ben 630 le notificazioni a riguardo, segno che il tema è quanto mai attualissimo e richiede alle imprese un sforzo di adeguamento al GDPR e ai suoi principi (privacy by design e privacy by default su tutti), che deve avvenire anche nel loro stesso interesse[186].

4.4 La nomina di un Data Protection Officer

Tra gli adempimenti più onerosi previsti dal GDPR, vi è quello della nomina di un Responsabile per il trattamento dei dati, o Data Protection Officer. Tale figura, in realtà, non è altro che l'evoluzione del privacy officer previsto dalla direttiva 95/46, che all'articolo 18 permetteva agli Stati la designazione di un soggetto indipendente per l'applicazione della normativa. L'articolo 37 prevede i casi in cui la nomina di tale figura è obbligatoria: sempre all'interno delle pubbliche amministrazioni, salvo per le autorità giurisdizionali quando esercitano funzioni giurisdizionali; quando la attività principali dell'impresa consistono in trattamenti che per loro natura, ambito o finalità richiedono un monitoraggio costante degli interessati su larga scala; quando le attività consistono nel trattamento su larga scala di dati sensibili relativi a salute, vita sessuale, genetici, biometrici e giudiziari.

Lo scopo del DPO sarà quello di osservare, valutare e mettere a punto un sistema di gestione dei dati personali all'interno dell'impresa in conformità a quanto dettato

185 Si pensi al più comune degli attacchi, il ransomware,. Questo tipo di malware infetta i dati del dispositivo cifrando i file in esso contenuti, i quali possono essere recuperati di norma solo attraverso il pagamento di un riscatto. Ad esempio, la criptazione dei dati personali dell'intero database clienti potrebbe rappresentare un costo altissimo in termini di denaro per un'impresa. Anche in termini reputazionali, un'impresa nel momento in cui subisce un attacco di questo tipo pregiudicando i dati dei propri utenti, subisce un grave danno di immagine sul mercato, specie quando questo viene amplificato dal web.

186 Nel suo sito il Garante traccia il bilancio del 2018: 43269 sono state le comunicazioni dei dati di contatto dei Responsabili della Protezione dei Dati (o Data Protection Officer), 4704 i reclami e le segnalazioni, 13825 i contatti con l'Ufficio Relazioni con il Pubblico. I valori riportati hanno subito tutti un aumento rispetto allo stesso periodo del 2017, a testimonianza degli effetti che sta producendo il GDPR. I dati sono consultabili alla pagina web (aggiornata al 30 Gennaio 2019) https://www.garanteprivacy.it/documents/10160/0/REGOLAMENTO+UE+Il+bilancio+di+applicazione+nel+2018

dal nuovo regolamento, informando e fornendo così consulenza al titolare e al responsabile del trattamento. E' incaricato di sensibilizzare e formare il personale incaricato di trattare dati personali all'interno dell'impresa e rappresenta il punto di contatto per l'autorità del controllo qualora si evidenzino criticità in merito al trattamento (art. 38 GDPR). Si assicura inoltre che all'interno dell'impresa venga tenuto il registro dei trattamenti e vengano conservate le richieste degli interessati, nonché vengano raccolte tutte le casistiche di data breach avvenute all'interno dell'impresa.

Circa i criteri di designazione del DPO; dal Regolamento è possibile evincere solamente che la persona che riceve la nomina deve essere in possesso di *"una conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati"* (art. 37 par. 5). Sul punto, una recente sentenza del TAR del Friuli Venezia Giulia, ha puntualizzato che il profilo del DPO debba essere **"***eminentemente giuridico***"**[187]. La controversia è sorta in merito ai requisiti richiesti da un avviso pubblico di un'Azienda sanitaria della regione per il conferimento dell'incarico di DPO. Tra i requisiti, oltre al titolo di laurea in giurisprudenza, informatica, ingegneria informatica o equipollenti, si chiedeva anche il possesso di una particolare certificazione Lead Auditor per i Sistemi di Gestione per la Sicurezza delle informazioni. Il TAR non ha voluto circoscrivere la nomina ai soli giuristi, ma ha semplicemente voluto evitare la predisposizione di barriere illogiche al procedimento di selezione: il punto essenziale consiste nella possibilità da parte del DPO incaricato di dimostrare le proprie competenze e conoscenze specifiche sulla materia, al di là del possesso di eventuali certificazioni o attestati.

Uno dei criteri che devono definire il DPO è indubbiamente quello dell'indipendenza, nel senso che egli deve svolgere la propria attività in piena autonomia e in assenza di conflitto di interessi: ciò significa che se all'interno dell'impresa egli ricopre altre funzioni, esse non possono influenzare l'attività di sorveglianza e controllo sul trattamento dei dati personali (art 38, par. 6). Stante questa previsione, appare inopportuno che tale posizione sia ricoperta da un individuo che contestualmente opera ai vertici aziendali (ad esempio amministratore delegato, responsabile finanziario, direttore marketing…). Il DPO è incaricato di proteggere i dati personali,

187 TAR Friuli Venezia Giulia, Sez. I, sentenza n. 287 del 5 settembre 2018, rinvenibile alla pagina https://www.privacy.it/2018/09/13/tar-friuli-dpo-iso-27001/

non gli interessi economici dell'impresa.

In virtù di questo, si può affermare che il ruolo del DPO riflette l'approccio responsabilizzante del GDPR nei confronti delle imprese: in tal senso parte della dottrina[188] ha affermato che il DPO esplica funzioni di tipo pubblicistico, considerato che l'assolvimento dei suoi compiti è indirizzato a soddisfare un interesse pubblico. Infatti, il DPO può essere contattato dagli interessati per tutte le questioni inerenti la gestione dei propri dati personali e l'esercizio dei diritti previsti dal regolamento (art. 38, par. 4).

Dal punto di vista dell'inserimento della figura del DPO all'interno dell'organigramma aziendale, tale incarico in realtà può essere affidato a uno dei dipendenti dell'azienda o esternalizzato a un fornitore esterno tramite apposito contratto di servizio. A parere di chi scrive, sulla questione vi è un evidente paradosso dovuto dal fatto che il requisito dell'indipendenza del DPO dalle influenze dei vertici aziendali mal si concilia con gli obblighi, e in generale con la situazione di subordinazione, derivanti da un rapporto di lavoro dipendente. Per altro verso, è anche vero che ex art. 38, par. 3, il DPO non può essere rimosso o penalizzato dal titolare del trattamento.

Per quanto concerne invece le responsabilità del DPO, egli non è responsabile dell'inosservanza delle previsioni in materia di dati personali, dal momento che è il titolare del trattamento ad essere incaricato di predisporre misure tecniche e organizzative congrue. Il DPO può solo rispondere della sua attività di consulenza e assistenza nei confronti del titolare, il quale potrà avanzare pretese risarcitorie basate unicamente sulla responsabilità contrattuale.

4.5 Il registro dei trattamenti

Ex. art. 30 del GDPR, le imprese sono tenute a redigere un registro dei trattamenti, la cui funzione è quella di tenere traccia delle attività dell'organizzazione

188 Di Resta, F., *La nuova "privacy europea". I principali adempimenti del regolamento UE 2016/679 e profili risarcitori*, Giappichelli Editore, Torino, 2018, pag. 109; Pizzetti, F., *Privacy e il diritto europeo alla protezione dei dati personali* cit., pag. 282

sui dati personali degli interessati[189]. Tra le informazioni minime essenziali che il registro deve contenere (a cui vanno aggiunte tutte quelle che si ritengono necessarie) ci sono: il nome e i dati di contatto del titolare del trattamento, del contitolare del trattamento e del responsabile della protezione dei dati, le finalità del trattamento, la descrizione delle categorie di interessati e delle categorie di dati personali, le categorie di destinatari, i termini previsti per la cancellazione delle diverse categorie di dati (ove possibile), una descrizione generale delle misure tecniche e organizzative per la sicurezza, eventuali trasferimenti di dati personali verso paesi terzi. Il registro deve essere tenuto in forma scritta o in forma elettronica e deve essere reso disponibile all'Autorità di controllo in caso di verifiche.

Tuttavia una delle maggiori difficoltà che le imprese, o meglio i titolari o i responsabili del trattamento stanno riscontrando è l'individuazione chiara di quali siano le attività di business che implicano la raccolta dei dati, nonché la conseguente catalogazione dei dati in base alle finalità. In relazione a quest'ultimo punto, occorre far presente che altre fondamentali informazioni da inserire all'interno del registro sono il criterio di liceità e la base giuridica in forza dei quali si giustifica il trattamento (art.6 GDPR).

Sono esentate dall'obbligo di tenuta del registro le imprese o le organizzazioni con meno di 250 dipendenti, salvo che il trattamento effettuato: possa rappresentare un rischio per i diritti e le libertà degli interessati; non sia occasionale; includa il trattamento di categorie di dati sensibili o giudiziari (art. 30 par. 5 GDPR). Il gruppo di lavoro Articolo 29 ha chiarito che è sufficiente ricorra anche una sola delle tre casistiche indicate affinché si attivi l'obbligo di tenere un registro anche per le imprese con meno di 250 dipendenti. Tale interpretazione collide, a ben vedere, con il considerando n. 13 del GDPR, in cui si afferma che "Per tener conto della specifica situazione delle micro, piccole e medie imprese, il presente regolamento prevede una deroga per le organizzazioni che hanno meno di 250 dipendenti per quanto riguarda la conservazione delle registrazioni." Se si accoglie l'interpretazione del Gruppo di Lavoro, l'interrogativo che sorge spontaneo è quello di comprendere chi non sia sottoposto alla tenuta di questo registro. Anche accantonando le ipotesi di rischio

189 Al paragrafo 2 dell'articolo 30, si prevede che anche i responsabili del trattamento abbiano l'obbligo fi tenere un registro simile, documentando tutte le attività messe in atto per conto del titolare.

elencate all'articolo 30, le imprese utilizzando risorse umane si trovano quotidianamente a trattare dati personali. Si pensi ai dati relativi allo stato di salute dei dipendenti: essi possono essere raccolti per il controllo delle assenze, per l'assunzione di personale appartenente alle categorie protette, per la gestione degli infortuni[190]. Esempio calzante quello appena citato, visto che lo stesso Gruppo di Lavoro afferma che il semplice trattamento dei dati dei propri dipendenti non può considerarsi occasionale[191].

Per generare ancora più confusione sulla questione, nella sua Guida all'applicazione del GDPR il Garante italiano ha avallato un'interpretazione più soft dell'articolo 30, ammettendo di fatto che l'impiego di un numero inferiore a 250 dipendenti e l'assenza di rischi nel trattamento garantisce l'esenzione dalla tenuta del registro[192].

Al di là degli ulteriori dubbi in merito a quale delle due interpretazioni debba prevalere, si può comunque affermare che l'istituzione del registro dei trattamenti rappresenta un adempimento indubbiamente utile anche qualora tale obbligo non sussistesse, specie se letto quale strumento di accountability[193]. D'altro canto, sono anche comprensibili le reticenze da parte delle piccole e medie imprese nell'adempimento di un simile onere, considerati già i molteplici sforzi profusi per il rispetto della nuova normativa. Il rischio è un aggravio eccessivo in termini di impegno e costi che mal si coniuga con il trattamento a basso rischio che viene

190 Massimini, M., Il registro dei trattamenti GDPR e la deroga fantasma per le PMI, rintracciabile al sito https://www.privacy.it/2018/04/27/massimini-registro-trattamenti-gdpr-deroga/ (aggiornato al 03/02/2019),

191 Vedasi il Position Paper on the derogations from the obligation to maintain records of processing activities pursuant to Article 30 GDPR del Gruppo di Lavoro Articolo 29. Il documento si può trovare alla pagina https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51422.

192 Ciò nonostante anche il Garante italiano caldeggia tutti i titolari di trattamento e i responsabili a dotarsi di tale registro, a prescindere dalle dimensioni dell'organizzazione. Si veda Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali, rinvenibile alla pagina https://www.garanteprivacy.it/regolamentoue/approccio-basato-sul-rischio-e-misure-di-accountability-responsabilizzazione-di-titolari-e-responsabili.

193 Massimini, M., *Il registro dei trattamenti GDPR* cit.

effettuato dalle attività di tali soggetti.

4.6 L'impresa e il rispetto dei diritti dell'interessato

I diritti dell'interessato rappresentano uno dei cardini del nuovo impianto sulla protezione dei dati personali. L'interessato può rivolgersi direttamente al titolare del trattamento, anche in un momento successivo al consenso. Nello specifico l'interessato può chiedere: informazioni su quali dati sono trattati dal titolare; di accedere ai dati in possesso del titolare (diritto di accesso); la revoca del consenso prestato, l'opposizione ai trattamenti automatizzati, l'esercizio dell'opposizione al trattamento, la cancellazione dei dati in possesso del titolare, l'aggiornamento o la rettifica dei dati conferiti; la trasformazione in forma anonima dei dati, il blocco o la limitazione dei dati trattati, la portabilità dei dati.
In questo paragrafo ci si soffermerà su alcuni di questi diritti e in particolare sulle novità introdotte dal testo del regolamento.

Per quanto riguarda la modalità di esercizio di tali diritti, il titolare del trattamento ha l'obbligo di fornire all'interessato le informazioni relative all'azione intrapresa senza ingiustificato ritardo e comunque entro un mese dalla richiesta. Tale termine può essere prorogato solo nel caso in cui la richiesta presenti un elevato grado di complessità[194](art. 12 par. 3 GDPR).

Il rilascio di informazioni da parte del titolare è a titolo gratuito, a meno che il titolare non dimostri che le richieste dell'interessato siano manifestamente infondate, ripetitive o eccessive: in questo caso può essere addebitato all'interessato un contributo spese ragionevole o può essere respinta la richiesta (art. 12 par. 5 GDPR).
Ad ogni modo la risposta fornita all'interessato deve avvenire in forma scritta o elettronica, mentre la possibilità di rilasciare una risposta orale può accettarsi solo qualora la richiesta dell'interessato lo preveda. Seguendo le stesse logiche impartite per la realizzazione dell'informativa sul consenso, il regolamento prevede che la risposta fornita all'interessato debba essere intellegibile, concisa, trasparente e che utilizzi un linguaggio semplice e chiaro.

194 I motivi della proroga vanno comunque comunicati all'interessato entro un mese dalla richiesta.

Per quanto riguarda il diritto di accesso previsto dall'articolo 15 GDPR, esso presenta alcune piccole novità rispetto alla precedente normativa.
In primo luogo, il diritto di accesso prevede che in qualsiasi caso all'interessato venga rilasciata una copia dei propri dati personali oggetto del trattamento.
In secondo luogo, viene chiesto al titolare di indicare il periodo di conservazione previsto, o laddove non fosse possibile, di rendere noti i criteri usati per la definizione di tale periodo.

L'articolo 18 rappresenta un'estensione rispetto all'articolo 7, comma 3 del Codice della privacy, che prevedeva il blocco del trattamento. Si introduce un diritto alla limitazione del trattamento, tale per cui l'interessato ha diritto di ottenere che i suoi dati vengano utilizzati limitatamente a quanto sia necessario ai fini della conservazione (specifica introdotta dal GDPR). Si tratta quindi di una sorta di sospensione temporanea del trattamento in corso che può verificarsi qualora si verifichi una delle seguenti circostanze: l'interessato contesta l'esattezza dei dati personali; il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e richiede invece che ne sia limitato l'utilizzo; il titolare non necessiti più di questi dati, ma l'interessato ne abbia necessità per l'accertamento o la difesa di un diritto in sede giudiziaria; l'interessato si sia opposto al trattamento e sia in attesa di capire se i motivi legittimi del titolare del trattamento prevalgano su quelli dell'interessato. Sul punto il considerando 67 riporta anche alcuni esempi non tassativi per far comprendere cosa debba intendersi per limitazione del trattamento: ad esempio rendere inaccessibili agli utenti i dati personali dell'interessato o rimuovendo temporaneamente i dati pubblicati in una pagina web.

L'articolo 20 infine introduce un vero e proprio nuovo diritto: il diritto alla portabilità dei dati[195]. Esso consente all'interessato di ricevere i dati personali dal titolare del trattamento e di trasferirli senza alcun impedimento a un diverso titolare. Si tratta indubbiamente di uno strumento essenziale nella prospettiva della libera circolazione dei dati personali nell'UE e quindi in ragione di una libera concorrenza fra le imprese in un'ottica di creazione di nuovi servizi all'interno del mercato unico digitale. Tramite l'introduzione di questo diritto si cerca quindi di riequilibrare il

195 In realtà si tratta di un diritto già conosciuto dai consumatori all'interno dei servizi di telefonia: si pensi infatti alla portabilità del proprio numero telefonico da un operatore all'altro.

rapporto fra interessati e titolari del trattamento, stimolando di fatto gli interessati a un controllo più stringente sui dati che li riguardano[196].

I dati resi all'interessato devono essere resi in un formato strutturato, di uso comune e leggibile elettronicamente. Per tale ragione i dati portabili devono essere stati trattati attraverso strumenti automatizzati (non registri cartacei) e devono essere stati forniti consapevolmente dall'interessato e trattati sulla base del suo consenso o in forza di un contratto (art. 20 par.1 GDPR). Sono ricompresi anche i dati osservati forniti dall'interessato mediante l'utilizzo di un dispositivo o la fruizione di un servizio (es. la cronologia delle ricerche web).

In tutto questo, l'esercizio del diritto ex art. 20 non deve ledere i diritti e le libertà altrui. Tale ipotesi si verificherebbe ad esempio nell'ambito del trasferimento della rubrica contatti e dei relativi messaggi di un soggetto da un servizio di posta elettronica ad un altro nel caso in cui il secondo titolare del trattamento che riceve i dati dell'interessato, utilizza i dati afferenti persone terze per finalità diverse da quelle per cui le conserva (es. marketing).

Ne consegue che i titolari del trattamento, e quindi le imprese, dovrebbero elaborare dei meccanismi in grado di consentire agli interessati che richiedono la portabilità, di selezionare quali dati desiderano trasmettere e quali dati di terzi preferiscono escludere. Allo stesso modo, sarebbe auspicabile l'implementazione di un sistema per la raccolta del consenso da parte di altri interessati coinvolti nel processo di portabilità, in modo da rendere più celere e agevolata la trasmissione dei dati nel caso in cui tali soggetti terzi si dicano favorevoli al trasferimento (basti pensare ai social network)[197].

4.7 In particolare GDPR e Oblio: un bilanciamento tecnico nelle mani delle imprese

196 Ancora una volta si rimanda alle Linee guida sul diritto alla portabilità dei dati (WP 242 rev.01) adottate il 13 dicembre 2016 dal Gruppo di Lavoro Articolo 29 per la protezione dei dati. Il documento si può trovare sul sito https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233.

197 *Ibidem*

Nel novero dei diritti dell'interessato elencati dal Regolamento n. 2016/679, all'articolo 17 si trova anche il diritto alla cancellazione dei dati. Grazie a tale norma, il diritto all'oblio ha trovato pieno riconoscimento giuridico a livello europeo. Considerata l'attenzione che è stata riposta sul tema dell'oblio all'interno di questo lavoro, appare opportuno analizzare le novità introdotte dal GDPR.

Da un lato la disposizione prevede il diritto dell'interessato ad ottenere la cancellazione dei dati che lo riguardano senza ingiustificato ritardo, dall'altro lato fa coincidere in capo al titolare del trattamento il corrispettivo dovere di adempiere alla cancellazione senza giustificato ritardo. Tuttavia la disciplina non riconosce il diritto all'oblio, ma lo rende attivabile solo in quelle situazioni in cui sia presente una ragione giustificatrice: i dati non sono più necessari rispetto alle finalità per cui sono stati raccolti o trattati; il consenso al trattamento è stato revocato; l'interessato si oppone al trattamento dei dati e non sussiste nessun motivo legittimo prevalente per procedere al trattamento oppure si oppone al trattamento per finalità di marketing diretto; i dati sono stati trattati illecitamente; i dati devono essere cancellati in forza di un obbligo giuridico; i dati sono stati raccolti relativamente all'offerta di servizi della società dell'informazione. Tuttavia l'articolo 17 ha positivizzato pure i limiti entro i quali esso debba operare, o meglio i diritti fondamentali dinanzi ai quali il diritto all'oblio deve cedere: a) l'esercizio del diritto alla libertà di espressione e di informazione; b) l'adempimento di un obbligo giuridico che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento; c) per motivi di interesse pubblico nel settore della sanità pubblica disciplinati dall'articolo

9, par. 2 lett h) ei)[198] e dell'articolo 9 par. 3[199]; d) ai fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità all'articolo 89, par. 1, nella misura in cui il diritto all'oblio rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento; e) l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Già nel 2012, l'Enisa (European Network and Information Security Agency) nel suo rapporto annuale[200] si era occupata della possibilità tecnica di realizzare in rete una tutela del diritto all'oblio. L'agenzia evidenziava le note problematiche più volte riportate in questo progetto: in un sistema aperto e globale come internet è sostanzialmente impossibile localizzare tutti i dati personali relativi ad un soggetto, e ancor di più avere la pretesa di cancellarli. Da ciò deriva la previsione del paragrafo 2 dell'articolo 17 che intima al titolare del trattamento dei dati personali di adottare le misure ragionevoli per procedere alla cancellazione di qualsiasi link, copia o riproduzione dei suoi dati personali, tenendo conto della tecnologia disponibile e dei

198 Art. 9, par. 2 lett h) e i) Regolamento 2016/67:

" h) il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità, fatte salve le condizioni e le garanzie di cui al paragrafo 3; i) il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale; "

199 Art 9, par. 3 Regolamento 2016/679:

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

200 Si rimanda alle conclusioni del rapporto ENISA 2012 "The right to be forgotten – between expectations and practice" , rintracciabile alla pagina web https://www.enisa.europa.eu/publications/the-right-to-be-forgotten (aggiornato al 28/12/2018.

costi di attuazione[201]. Ciò significa che una richiesta de-indicizzazione dei link contenenti dati personali inoltrata a un motore di ricerca, obbliga quest'ultimo a comunicare anche ai siti sorgente che tali informazioni otterranno una minore visibilità. Questi siti-sorgente tuttavia non saranno giuridicamente obbligati a procedere alla cancellazione, salvo diretta richiesta dell'interessato.

E' indubbiamente un'assoluta novità rispetto alla precedente normativa, poiché né la direttiva 95/46/CE né la sentenza Google Spain affermavano un obbligo in tal senso. Uno dei problemi irrisolti rimane tuttavia la questione relativa a chi debba occuparsi del bilanciamento tra interesse del singolo e interessi dei terzi o della generalità. La sentenza Google Spain autorizza infatti i privati a richiedere ai motori di ricerca la rimozione di link contenenti dati personali, qualora essi, pur essendo leciti e veritieri, appiano inadeguati, irrilevanti o non più rilevanti a rappresentare l'identità personale del soggetto. Tuttavia l'accento sulla prerogativa individuale del soggetto rispetto all'interesse collettivo, ha finito per avvicinare la materia della privacy alle ipotesi di diffamazione, in quanto ambedue proteggono la reputazione. Il potere decisionale in merito al suddetto bilanciamento è delegato in prima battuta alle imprese private. Esse tuttavia non solo hanno né gli strumenti né la professionalità per giungere a compiere valutazioni di questo tipo, ma difettano anche dei requisiti di indipendenza ed imparzialità necessari: fino a poco tempo fa il fine primario di un'impresa privata era rappresentato esclusivamente dal profitto. E' anche vero che oggigiorno, tra le imprese è maturata una crescente sensibilità in merito a taluni aspetti di carattere etico-sociale, esigenza dettata dal fatto che i consumatori sono divenuti sempre più consapevoli delle scelte che operano nel mercato, prendendo in considerazione anche fattori extra economici. Pertanto in tema di diritto all'oblio, alle imprese non è richiesta una "banale operazione tecnica", ma dovranno compiere una valutazione capace di ponderare memoria collettiva e vicende individuali, giudizio pubblico e identità personale, diritti e doveri.[202]

201 Si veda Considerando n. 66 del Regolamento 2016/679.

202 Per ulteriori considerazioni, si veda ila pagina web https://protezionedatipersonali.it/diritto-oblio (aggiornata al 29/12/2018).

4.8 I costi dell'adeguamento delle imprese al GDPR

4.8.1 Una prima visione d'insieme

Da quanto visto nei paragrafi precedenti l'impresa dovrà adempiere a determinati obblighi, più o meno vincolanti, in relazione soprattutto alla tipologia di attività svolta e di dati raccolti.

Secondo una ricerca della IAPP (*International Association of Privacy Professionals*) il 75% delle multinazionali europee investiranno circa 5 milioni di euro per l'adeguamento al GDPR assumendo nuovo personale da dedicare a tempo pieno alla gestione della privacy. Già nel 2016, anno dell'approvazione del regolamento, il valore medio dell'investimento delle aziende europee era stato di circa 350.000 euro per salire poi nel 2017 a circa 500.000 euro. Tali costi derivavano in particolare dall'introduzione del DPO, dall'utilizzo di consulenti esterni, dagli investimenti in IT (Information Technology, d'ora in avanti IT) per adempiere alla normativa[203].

Per quanto riguarda l'Italia, Confesercenti aveva a suo tempo indicato in circa 2 miliardi di euro l'impatto che il GDPR avrebbe avuto sulle aziende italiane. Nello specifico pesavano sulla stima l'obbligo di notifica in caso di *data breach* entro le 72 ore e l'implementazione di soluzioni IT per la crittografia e l'anonimizzazione dei dati. Ad ogni modo questi numeri fanno capire come l'introduzione del GDPR possa rappresentare un costo non indifferente per le aziende e al tempo stesso un'opportunità per i consulenti in materia[204].

Ciò premesso dobbiamo però anche considerare che la realtà italiana è alquanto diversa da quella europea data la presenza massiccia di PMI che rappresentano l'ossatura principale del nostro sistema economico. Risulta quindi difficilmente ipotizzabile che una PMI con fatturato inferiore a 4-5 milioni di euro possa investire decine di migliaia di euro per l'adeguamento e successivamente per la gestione della privacy.

---

203 Si veda "IAPP – EY Annual Governance Report 2017, rintracciabile al sito https://iapp.org/resources/article/iapp-ey-annual-governance-report-2017/ (aggiornata al 09/02/2019)

204 Si rimanda a https://www.confesercenti.it/blog/privacy-confesercenti-per-pmi-il-gdpr-e-stangata-da-almeno-2-miliardi-di-euro/

Talune aziende hanno quindi preferito adeguarsi alle disposizioni del GDPR lavorando più sugli aspetti formali tramite accorgimenti quali la revisione delle informative e la semplice tenuta del registro dei trattamenti, tralasciando modifiche sostanziali in relazione al processo di gestione e controllo dei dati personali. Altre invece hanno colto l'occasione per aggiornare i propri sistemi informatici di conservazione e protezione dei dati, consapevoli che l'agevole circolazione dei dati rappresenta uno dei fattori di sviluppo all'interno di un mercato unico digitale.

4.8.2 Valutazione dei costi del GDPR nelle PMI

Valutare i costi del GDPR è impresa assai ardua. La ragione risiede nel fatto che il GDPR è entrato in vigore da un periodo relativamente breve e di conseguenza le imprese ancora non hanno fatto pienamente i conti con l'adeguamento necessario al rispetto della normativa. Bisogna inoltre sottolineare come dall'introduzione del GDPR si sia assistito alla nascita di una professione assolutamente inedita, con la conseguente proliferazione di studi e società di consulenza specializzati in materia che hanno riversato sul mercato un'offerta a dir poco variegata sia dal punto di vista dei servizi forniti che dei compensi richiesti.

In questa sede si cercherà comunque di darne una valutazione di massima, per quanto personale, in base agli adempimenti a cui l'impresa deve adeguarsi.
Ai fini di un corretto approccio l'azienda deve in primo luogo fare una valutazione quanto più precisa delle risorse già presenti al suo interno, sia in termini di competenze del personale dipendente sia in termini infrastrutture IT, al fine di ottimizzarne l'utilizzo e, ove necessario, implementarle.

Data la novità e specificità della materia in questione, a meno che le risorse umane competenti non siano già presenti al suo interno (cosa questa alquanto improbabile nella maggioranza dei casi) sarà necessario rivolgersi a degli studi di consulenza esterni specializzati in materia e competenti sia da un punto di vista legale che dal punto di vista della sicurezza informatica.

A seguito di questa analisi le società di consulenza potranno, a seconda del caso: fornire procedure e software per la gestione (acquisizione, trattamento e

conservazione) e protezione dei dati, per il controllo e aggiornamento a seguito di eventuali modifiche della normativa; procedere alla formazione del responsabile e degli incaricati al trattamento dei dati attraverso la tenuta di corsi di formazione; nel caso poi che l'azienda si trovasse nella situazione di dover nominare un DPO, lo studio potrebbe assumere tale incarico, fermo restando che ne sia garantita la necessaria indipendenza ed autonomia (motivi questi per cui ne è vivamente sconsigliata la nomina di un dipendente dell'azienda).

Pertanto l'entità del compenso dovuto alla società di consulenza dipenderà dalla quantità di servizi forniti. Proviamo ora a quantificare quello che potrebbe essere una stima dei costi che una piccola/media azienda dovrebbe sostenere nel caso di ricorso ad una società di consulenza esterna.

Per quanto riguarda l'aspetto di implementazione del livello di IT dell'azienda, si può considerare un costo iniziale valutabile nell'ordine di 10-20.000 euro (si pensi all'acquisto o allo sviluppo di un gestionale), ai quali andranno poi ad aggiungersi i costi da sostenere nel tempo per eventuali aggiornamenti e assistenza tecnica. E' però importante sottolineare come questo investimento possa rappresentare un'opportunità importante non solo per arrivare a trattare in materia adeguata ed efficiente i dati personali dei propri dipendenti/clienti/fornitori, ma anche per proteggere adeguatamente importanti dati relativi al proprio know-how aziendale che potrebbero essere vittima di eventuali atti illeciti messi in essere da dipendenti infedeli o da cyber-criminali.

Proseguendo nella disamina degli altri possibili costi relativi alla consulenza si può distinguere tra: a) le attività da svolgersi all'interno dell'azienda (audit, controlli e verifiche, corsi di formazione...) per le quali si può ipotizzare circa 30 ore annue ed un costo orario di circa 100/120 euro + IVA; attività da remoto (consulenza telefonica, controlli delle informative, comunicazioni al garante...) per le quali possiamo ipotizzare circa 20 ore annue ed un costo orario di circa 50/60 euro.

Ne deriverebbe quindi una spesa annua di circa euro 4.000 + IVA, importo questo che andrebbe a coprire quella che possiamo considerare come " spese di ordinaria amministrazione", fermo restando la possibile insorgenza di differenti problematiche. A parte il costo orario, è comunque importante stabilire a priori un piano di lavoro di massima (per quanto possibile dettagliato) prevedendo un monte

ore per ognuna delle attività sopraelencate in modo da quantificare il più possibile quello che sarà il costo complessivo dei servizi forniti e limitare al massimo eventuale sorprese a posteriori. In questo modo si arriverebbe a limitare sia per l'azienda sia per la società di consulenza il rischio d'impresa in quanto i reciproci costi/ricavi risulterebbero almeno in parte già definiti. Alla fine ne risulterebbe un costo, almeno per il primo anno, attorno ai 15-20.000 euro.

Se si va a considerare quelli che sono i possibili costi derivanti dalle sanzioni previste in caso di non adeguamento al GDPR, potrebbe trattarsi di un costo sostenibile anche per una piccola impresa se questo garantisse di essere al sicuro da qualsivoglia accertamento. Tuttavia però occorre ricordare che la responsabilità finale in caso di violazione del GDPR resta comunque sempre in capo a chi è il titolare del trattamento e, di conseguenza, ricadono su di lui anche le relative sanzioni.

Bisogna tener presente che i potenziali costi in caso di sanzioni non sono certo esigui. La normativa parla infatti, nei casi più gravi, di una sanzione di 20 milioni euro o del 4% del fatturato (che nel caso di un fatturato di 5 milioni sono ben 200.000 euro)[205]. Già questo semplice calcolo potrebbe quindi indurre l'azienda a considerare come sostenibile l'investimento di circa 20.000 euro portato come esempio in un'ottica di costi-benefici. Ad ogni modo la cifra minima appena prospettata può non costituisce un investimento trascurabile per alcune aziende di piccole dimensioni che fino ad oggi hanno pressoché sempre ignorato ogni problematica in ambito privacy. Tuttavia come si è detto più volte l'intento del GDPR è quello di cambiare la prospettiva con cui si trattano i dati delle persone. Considerato questo, è quindi auspicabile che tali soggetti non ricorrano a facile scorciatoie dettate da esigenze di mero risparmio: ci si riferisce in particolare all'acquisto di pacchetti e servizi forfettari erogati da società, che inducono i titolari delle imprese a ritenere che con piccoli accorgimenti pratici ed economici sia possibile conformarsi al nuovo regolamento.

Infine, un ultimo aspetto da considerare può essere quello dell'opportunità di stipulare polizze assicurative per ripararsi dalle eventuali nuove sanzioni. Tale possibilità però al momento sembra di difficile attuazione, dato che la situazione creata dall'introduzione del GDPR è in continuo divenire e conseguentemente risulterebbe difficilmente quantificabile il "premio" che una società assicuratrice

205 Si rimanda alla lettura integrale dell'articolo 83 GDPR.

dovrebbe richiedere all'azienda cliente. Fino a quando non esisteranno statistiche relative al numero e al valore delle sanzioni comminate, appare altamente improbabile che i gruppi assicurativi possano decidere di operare e fornire servizi anche in quest'ambito.

4.9 Riflessioni sul principio di responsabilizzazione delle imprese nella gestione dei dati personali

Come si è visto a più riprese, tra le novità introdotte dal GDPR vi è senz'ombra di dubbio il principio della "responsabilizzazione" (accountability) delle imprese: i titolari e i responsabili del trattamento dei dati personali all'interno di un'azienda devono adottare comportamenti e misure idonee ad assicurare l'applicazione del regolamento. Al di là degli adempimenti e dei cambi previsti dalla normativa che in maniera più o meno incisiva coinvolgono tutte le imprese che trattano dati personali (informativa, registro dei trattamenti, DPO...), quello che viene richiesto dal regolamento è un vero e proprio cambio di mentalità: se prima al centro della privacy vi erano i dati, ora vi sono i diritti della persona. Esclusa un'applicazione standardizzata del GDPR, le imprese devono compiere un'autovalutazione della propria attività, individuando quali sono i profili di rischio inerenti alla gestione dei dati personali che trattano, siano essi relativi ai propri clienti/utenti, ai propri fornitori, ai propri dipendenti. Sull'esito di questa auto-valutazione[206] pesano in particolare l'analisi dei rischi sull'impatto del trattamento dei dati sulle libertà e sui diritti degli interessati. Il titolare potrà decidere in autonomia se procedere al trattamento, dal momento che l'intervento del Garante della privacy potrà avvenire ex post, vista l'abolizione di alcuni istituti prima vigenti come la notifica preventiva dei trattamenti e il prior checking (art 17 del vecchio Codice della privacy). Ad ogni modo, il Garante continuerà ad avere un ruolo centrale nella protezione dei dati personali non solo per la sua attività di controllo, ma anche per il nuovo ruolo di educatore nella difficile transizione in atto.

206 Significativo in tal senso appare anche la disposizione dell'articolo 35 GDPR, che prevede che il titolare del trattamento prima di realizzare un trattamento deve compiere una valutazione d'impatto sulla protezione dei dati, consultandosi preventivamente con il DPO (laddove presente).

Ne discende che ogni procedura, meccanismo o misura adottata in relazione alla gestione dei dati personali deve essere credibile e giustificabile.
Il tentativo del GDPR, attraverso il sistema già citato della privacy by design and by default, è quello di dar fiducia alle imprese, lasciando discrezionalità e libertà d'azione nelle scelte. Il motivo è che l'educazione e la consapevolezza dei diritti e dei doveri rappresenta uno strumento più efficace e adeguato per assicurare un elevato standard di protezione, più della semplice minaccia delle sanzioni e più della semplice predisposizione di misure uguali che risultano infruttuose in ragione della natura e della tipologia dei dati trattati.

Ciò non toglie che le sanzioni rappresentano comunque un mezzo correttivo residuale da utilizzare nel momento in cui si presenti una grave violazione dei principi sopra descritti. E' anche vero tuttavia che in forza della discrezionalità lasciata in capo alle imprese, queste ultime potranno legittimamente contestare e mettere in discussione le sanzioni amministrative dell'Autorità, tanto nel merito quanto nell'entità della sanzione, dando così vita a un contraddittorio sulla valenza delle misure adottate. Ed è probabilmente qui che si gioca la partita decisiva, nel senso che in ultima istanza toccherà alla giurisprudenza decidere quali parametri utilizzare per valutare il rispetto del GDPR nel caso concreto. Sebbene appunto le controversie presenteranno profili diversi in merito alla natura dell'azienda, dei dati, delle attività svolte…, ciò non toglie che spetterà alla giurisprudenza definire determinate linee interpretative, in presenza di principi che sono di fatto molto generali e astratti.

A tale considerazione, si può aggiungere che l'operatività del GDPR, o meglio la sua efficacia, sarà determinata anche dalla presenza di controlli da parte dell'autorità di controllo, specie in questo momento iniziale in cui gli "interessati" ancora non sono a conoscenza dei nuovi diritti che possono vantare in virtù della nuova normativa.
Per concludere, si può dire che l'introduzione del meccanismo della responsabilizzazione delle imprese rappresenti sicuramente una tecnica innovativa per garantire il raggiungimento di un elevato livello di protezione dei dati personali, evitando la continua rincorsa normativa all'evoluzione dei mezzi tecnologici. Tuttavia, a parere di chi scrive, il GDPR prende in considerazione solo relativamente la situazione delle piccole medie imprese, anche in relazione alle perduranti difficoltà economiche di alcuni settori. Per quanto sia vero che gli obiettivi di tutela siano

variabili a seconda anche della dimensione organizzativa dell'impresa e siano parametrati "sullo stato dell'arte e sui costi di attuazione" rispetto ai rischi, è palese che alcuni accorgimenti quali ad esempio la notificazione di un data breach entro 72 ore rappresenti un'incombenza amministrativa non da poco per una piccola-media impresa. Il rischio è quindi che il GDPR venga percepito dalle aziende non solo come un aggravio in termini di costo, ma anche come un ulteriore ed eccessiva pratica burocratica da sbrogliare.

RIFLESSIONI CONCLUSIVE: il ruolo dei diversi soggetti coinvolti nell'applicazione del GDPR

Da quanto precedentemente esposto si evidenzia come l'uomo, in maniera più o meno marcata in base ai vari periodi storici, abbia sempre ambito ad avere una propria "vita privata", e a considerare la riservatezza come un bisogno essenziale.

Tale bisogno è via via aumentato d'intensità a seguito dell'introduzione di nuove tecnologie, inerenti in particolare alla trasmissione delle informazioni, che portavano invece al progressivo abbattimento di tutte le barriere che l'individuo era riuscito a crearsi attorno a tutela della propria sfera personale.

Questa sempre più marcata intromissione nella sfera più intima delle persone conseguente all'introduzione delle nuove tecnologie ha portato ad una sempre maggior richiesta di tutela da parte delle persone, richiesta alla quale i legislatori hanno cercato di rispondere a partire in particolare dagli anni '80.

Si è visto, inoltre, come l'evoluzione del concetto di riservatezza e privacy si sia inizialmente sviluppato in modo diverso in Europa rispetto agli Stati Uniti fino a quando, a causa dell'aumento esponenziale delle violazioni e intromissioni nella sfera personale degli individui che andava delineandosi, si è cercato di trovare delle soluzioni condivise per porre delle limitazioni alle nuove metodologie per il trasferimento di informazioni.

In particolare si giunse a comprendere appieno l'importanza che i dati personali iniziavano a rivestire nell'ambito economico e di conseguenza quanto importante fosse regolarne l'utilizzo in modo da tutelarli nel miglior modo possibile, senza con questo limitarne eccessivamente l'utilizzo che sarebbe andato a scapito di altri diritti ugualmente degni di tutela.

Tuttavia i tentativi da parte dei legislatori, a livello sia nazionale che sovranazionale, di arginare questa manipolazione generale delle identità personali non hanno portato inizialmente a risultati apprezzabili, soprattutto a causa dell'avvento negli ultimi anni della rete globale e dei social network.

Questo perché i legislatori si sono spesso trovati a legiferare su tematiche che nel frattempo erano ormai già divenute obsolete a causa della rapidità dei cambiamenti nelle modalità di circolazione delle informazioni.

In questa fase di rapida evoluzione un ruolo importante ed essenziale è stato ricoperto dai giudici che, in assenza di indicazioni legislative precise, hanno provveduto a colmare con le loro decisioni un evidente vulnus normativo. Decisioni che in alcuni casi si sono dimostrate di importanza fondamentale anche per lo sviluppo legislativo in materia come hanno ampiamente dimostrato le sentenze sul caso "Google Spain" e sul caso "Manni" di cui ci si è occupati in questo lavoro.

E' perciò grazie alla giurisprudenza degli ultimi anni che si è arrivati a definire per la prima volta una regolamentazione adeguata alle esigenze di un mercato dell'informazione che ha assunto ormai un ruolo strategico nell'ambito economico mondiale.

E' chiaro però che la reale efficacia di questo ragguardevole risultato raggiunto dal punto di vista normativo con l'approvazione del GDPR dovrà essere testata sul campo. Essendo il regolamento entrato in vigore solo da pochi mesi è ancora troppo presto per capire quali potranno essere i reali effetti in merito al bilanciamento tra diritto alla privacy e gli altri diritti fondamentali che rappresentano anch'essi il cardine della nostra società.

Se da un certo punto di vista questa normativa risulta essere assolutamente all'avanguardia e premonitrice di possibili nuovi scenari futuri (fatto questo assolutamente innovativo rispetto alle normative precedenti che si trovavano letteralmente ad inseguire l'evoluzione del mercato dell'informazione), è pur vero che il punto essenziale sarà dato dall'effettiva applicazione che verrà messa in atto dai principali soggetti del mercato ai quali è rivolto tale regolamento, le imprese.

Essenziale sarà la percezione che queste ultime avranno dell'utilità di questo strumento che, come già evidenziato in questo lavoro, deve essere visto non come un fastidioso obbligo di cui farsi carico, bensì come un'opportunità per addivenire ad una diversa concezione sull'utilizzo dei dati personali altrui.

Negli ultimi anni non possiamo certo dire che il mondo economico si sia fatto molti scrupoli in merito all'utilizzo selvaggio delle informazioni ,forte del fatto che attraverso l'approvazione di un generico consenso fornito dall'interessato, se ne garantiva l'uso indiscriminato per i fini più disparati. Il dato personale veniva visto non come un insieme di elementi più o meno critici per la definizione dell'individuo da trattare quindi in maniera diversa a seconda dell'utilizzo finale, bensì come un

ammasso unico di informazioni da sacrificare sull'altare del guadagno senza porsi alcuna domanda di tipo etico e morale.

Lo scopo principe del nuovo GDPR è quindi quello di portare una consapevolezza nuova tra i soggetti che operano nel mercato facendo loro capire che non deve essere visto unicamente come una nuova imposizione o, peggio, un costo inutile, ma che può invece rappresentare un punto di partenza per raggiungere quello che da sempre è lo scopo dell'impresa, cioè il profitto, senza tralasciare però gli aspetti etici e morali che dovrebbero contraddistinguere l'essere umano.

Risulta comunque chiaro che raggiungere tale scopo non sarà cosa semplice considerate le difficoltà che l'applicazione della normativa comporta. Proprio per questo il regolamento prevede anche delle sanzioni in caso di violazioni gravi delle norme, ed in quest'ambito un compito assolutamente essenziale sarà quello che dovranno svolgere coloro che detengono il potere di controllo (il Garante alla Privacy) ed il potere giurisdizionale (i giudici).

In particolare questi ultimi si troveranno in prima linea in quello che sarà l'arduo compito di coprire i vuoti normativi che sicuramente andranno via via a palesarsi soprattutto nei primi tempi dall'entrata in vigore del GDPR. Quest'ultimo infatti, per quanto sia stato redatto nel modo più esaustivo possibile, rappresenta pur sempre un sorta di "Legge Quadro" da riempire con il formarsi di una numerosa e quanto più articolata possibile giurisprudenza in materia.

In questo senso i casi esaminati in questo lavoro e le relative sentenze rappresentano una sorta di pilastri posati durante la costruzione della "casa della privacy" dove il GDPR ne rappresenta le fondamenta in quanto intervengono nell'essenziale diatriba del bilanciamento tra diritto alla privacy e diritto alle informazioni dell'esercizio dell'attività d'impresa.

A parere di chi scrive entrambe le sentenze in questione rappresentano dei passi fondamentali nel percorso intrapreso ai fini del raggiungimento di una adeguata e per quanto possibile equilibrata tutela dei vari diritti fondamentali garantiti in primo luogo dalla Costituzione (ex art.2).

Relativamente a quest'ultimo aspetto, la sentenza "Manni" risulta particolarmente importante ai fini del presente lavoro per la demarcazione degli equilibri tra sfera privata e interesse pubblico.

La sentenza pone infatti dei paletti a quella che negli ultimi tempi sembrava una continua deriva verso una tutela sempre più marcata dei diritti personali del singolo a scapito del diritto all'informazione che, invece, è da sempre e a maggior ragione nell'attuale periodo storico, condizione fondamentale e imprescindibile ai fini del corretto funzionamento di un sistema economico.

La stessa sentenza nel ribadire la necessità che talune informazioni, anche strettamente personali, siano da considerarsi essenziali ai fini di tutelare adeguatamente il diritto alle informazioni di cui i soggetti economici abbisognano nello svolgimento di un corretto processo decisionale, allo stesso tempo mette ulteriormente in rilievo come il ruolo pubblicitario svolto dal Registro delle Imprese nel mettere a disposizione di tutti, siano essi soggetti pubblici o privati, tali informazioni, risulta se possibile ancora più vitale oggi che in passato.

A questo proposito si deve anche notare come la sentenza in questione sia uscita successivamente all'approvazione del GDPR e pertanto nel decidere la CGE ha sicuramente tenuto in debito conto la normativa appena approvata anche se non ancora entrata in vigore. Da questa considerazione si può ricavare, se mai ce ne fosse bisogno, un ulteriore elemento rafforzativo del ruolo pubblicistico svolto dal Registro delle Imprese che, sebbene possa talvolta mettere eccessivamente in risalto i dati delle persone fisiche iscritte, conferma la tesi per la quale il sacrificio del diritto alla privacy è da considerarsi ampiamente giustificato dalle esigenze di un corretto funzionamento del sistema economico.

Vi è da dire però che nella sentenza la CGE ha lasciato facoltà ai singoli Stati membri di valutare caso per caso la possibilità di limitare l'accesso a determinati dati personali soltanto a determinati soggetti terzi che ne dimostrino un interesse specifico, come anche la possibile cancellazione di dati la cui permanenza non sia più ritenuta essenziale in quanto decorso un limite di tempo sufficientemente lungo dallo scioglimento della società.

Tutto questo ad ulteriore conferma del fatto della responsabilità che avranno i giudici negli anni a venire.

BIBLIOGRAFIA

- Alpa G., Conte, G. (a cura di), *Orientamenti della corte di giustizia dell'Unione Europea in materia di responsabilità civile,* Giappichelli editore, Torino, 2018

- Alpa, G., Conte, G. (a cura di), *Casi decisi dalla Corte di Giustizia dell'Unione europea sui diritti fondamentali in materia contrattuale,* Giappichelli Editore, Torino, 2018

- Alvarez Rigaudia, C., *La sentencia Google Spain y el derecho al olvido* in Actualidad Juridica, 2014

- Bellavista, A. , *Dignità e riservatezza del lavoratore* in Lambertucci, P. (a cura di), Dizionari del diritto privato. Diritto del lavoro, Giuffrè, Milano, 2010

- Berti, A. S., *La pubblicità legale dei registri delle imprese prevale sul diritto all'oblio dei dati personali ivi inseriti,* in Giustizia Civile. Com (periodico online), vol. 4. fascicolo 7, 2017

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

- Carraro, G., Pubblicità commerciale e diritto all'oblio nella prospettiva dei diritti dell'uomo in La nuova giurisprudenza civile commentata, 2016, v. 32, fascicolo 4.

- Cassano, G. , *Stalking, atti persecutori, cyberbullismo e tutela dell'oblio,* Wolters Kluver, Assago, 2017

- Chieco, P. , *Privacy e lavoro: la disciplina del trattamento dei dati personali del lavoratore*, Cacucci, Bari, 2000

- Codiglione, G., *Libertà d'impresa, concorrenza e neutralità della rete nel mercato transnazionale dei dati personali* in Diritto dell'Informazione e dell'Informatica, fasc. 4-5, 2015

- *Colomba, G. , Zanetti G., Aspetti problematici della nozione di privacy da un punto di vista filosofico-giuridico in* "Teoria e critica della regolazione sociale", n.1, 201

- De Cupis, A., *I diritti della personalità*, Giuffré Editore, Milano, 1973

- *De Stefani, F., Le regole della privacy: guida pratica al nuovo GDPR, Hoepli Editore, Milano, 2018*

- Di Rago, G., *La privacy e le imprese,* Halley Editrice, Matelica, 2005

- Di Resta, F., *La nuova "privacy europea". I principali adempimenti del regolamento UE 2016/679*

e profili risarcitori, Giappichelli Editore, Torino, 2018

- Fabris, F. , *Il diritto alla privacy tra passato, presente e futuro* in Rivista di Scienze della Comunicazione,n.2, 2009 Mantelero, A. , *Il costo della privacy tra valore della persona e ragione d'impresa*, Giuffré Editore, Torino, 2007,

- Falletti E., *L'evoluzione del concetto di privacy e della sua tutela giuridica* in Cassano, G., Scorza, G., Vaciago, G., *Diritto dell'internet. Manuale Operativo., Casi Legislazione, Giurisprudenza,* CEDAM, Milano, 2012

- Ferri, G.B., *Diritto all'informazione e diritto all'oblio* in Riv. Dir. Civ., n. I, 1990

- Finocchiaro G, *La protezione dei dati personali e la tutela dell'identità*, In Delfini F., Finocchiaro G., *Diritto dell'informatica*, Utet Giuridica, Milano, 2014

- Finocchiaro, G., Delfini, G. (a cura di), *Diritto dell'informatica*, Utet Giuridica, Milano, 2014

- Gardini, G., *Le regole dell'informazione: l'era della post-verità,* Giappichelli Editore, Torino, 2017

- Heidegger, M, *La questione della tecnica,* GoWare, Firenze, 2017

- Iaselli, M. , *Il Codice della Privacy: una lettura ragionata*, lulu.com, 2011

- L. Ferola, *Dal diritto all'oblio al diritto alla memoria sul web. L'esperienza applicativa italiana*, in Diritto dell'Informazione e dell'Informatica, Vol. 28, n°6, 2012

- *Lamanuzzi, M., Diritto penale e trattamento dei dati personali. Codice della privacy, novità introdotte dal regolamento UE 2016/679 e nuove responsabilità per gli enti in JusOnline, 2017*

- Mancini, A. , *La protezione dei dati personali* in Megale, M. (a cura di), *ICT e diritto nella società dell'informazione,* Giappichelli Editore, Torino, 2017

- Mantelero, A., *Diritto all'oblio e pubblicità del registro delle imprese* in Giurisprudenza Italiana, 2015

nuove sfide, nuove prospettive in Rivista italiana di Diritto Pubblico Comparato, fasc. 2, 1 Aprile 2017

- Mantelero, A, *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, n. 4-5, 2014

- *Musselli, L., Trasparenza versus privacy nella pubblicazione dei dati personali nel registro delle imprese in DPCE Online, v. 31, n.3, Ottobre 2017*

- Naldi, M., D'Acquisto G., *Big data e Privacy by design,* Giappicheli Editore, Torino, 2017

- Nascimbene B., Anrò, I., *La tutela dei diritti fondamentali nella giurisprudenza della Corte di Giustizia:*

- Otranto, P., *Internet nell'organizzazione amministrativa: reti di libertà*, Cacucci Editore, Bari, 2015

- Pace, F. L. (a cura di), Dizionario sistematico del diritto della concorrenza, Jovene Editore 2013

- Pagallo, U. *La tutela della privacy negli Stati Uniti D'America e in Europa*, Giuffré Editore, Torino

- Panico, C. R., *Da internet ai social network*, Maggioli Editore, Santarcangelo di Romagna (RN), 2013

- Pappalardo, M. , *L'accesso al registro delle imprese tra garanzia di trasparenza e diritto all'oblio* in Le Società, 2017, n.7

- Patterson, J., *The Store,* Longanesi, Milano, 2017

- Pizzetti, F. , *Privacy e il diritto europeo alla protezione dei dati personali: dalla Direttiva 95/46 al nuovo Regolamento Europeo,* Giappichelli editore, Torino, 2016

- Pizzetti, F., (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Giappichelli Editore, Torino, 2018

- Pizzetti, F., *Il caso del diritto all'oblio*, Giappichelli Editore, Torino, 2013

- Pollicino, O., De Gregorio, G., *Privacy or Transparency? A New Balancing of Interests for the 'Right to be Forgotten' of Personal Data Published in Public Registers* in The Italian Law Journal n.2, 2017

- Pollicino, O., U*n digital right preso (troppo) sul serio dai giudici di Lussemburgo? Il ruolo degli artt. 7 e 8 della Carta di Nizza nel reasoning di Google Spain* in Diritto dell'informazione e dell'informatica, n.4-5, 2014

- R. Pardolesi, *L'ombra del tempo e (il diritto al)l'oblio*, in "Questione giustizia", Riv. Trim., n.1, 2017

- R. Pardolesi, *L'ombra del tempo e (il diritto al)l'oblio*, in "Questione giustizia", Riv. Trim., n.1, 2017

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

- Rodotà, S. , *La privacy tra individuo e collettività,* in «Politica del Diritto», 1974

- Rushkoff, D., Presente continuo, Quando tutto accade ora, Codice Edizioni, Torino, 2014

- Sartor, G., Di Cocco, C., *Temi di diritto dell'informatica (terza Edizione),* Giappichelli Editore, Torino, 2017

- Sileoni, S., *"Il diritto alla cancellazione dei dati e le attività economiche: una nuova visione del tempo. A margine della sentenza Camera di commercio c. Manni"* in Media Laws, n.1, 2017

- Tavani, T. H. , *Ethics and Tecnology: Controversies, Questions, and Strategies for Ethical Computing,* John Wiley & Sons. Inc.,, Nashua, 2012

- Warren S., Brandeis, L. , *The right to privacy* in Harvard Law Reviews, vol. IV, n.5, 1980

- Zencovich G. , V. Z., *Il diritto all'oblio su internet dopo la sentenza Google Spain,* RomaTre-Press, Roma, 2015

- Ziccardi, G. , *Informatica giuridica: privacy, sicurezza informatica, computer forensics e investigazioni digitali (Seconda edizione),* Giuffrè Editore, Milano, 2012

MATERIALE GIURISPRUDENZIALE

CASSAZIONE CIVILE

- Cass. Civ. , sentenza n.990 del 20 aprile 1963
- Cass. Civ., sentenza n. 2129 del 27 Maggio 1975
- Cass. Civ. (Seconda Sezione), n. 3679 del 9 Aprile 1998.
- Cass. Civ. (Sezioni Unite) n. 4060 del 22 Febbraio 2010.
- Cass. Civ., sentenza n. 10280 del 20 Maggio 2015
- Cass. Civ. (Prima Sezione), ordinanza n. 15096/15 del 17 Luglio 2015
- Cass. Civ. (Prima Sezione), sentenza n. 19761 del 9 Agosto 2017

CORTE COSTITUZIONALE

- Corte Cost., sentenza n. 38 del 12 Aprile 1973
- Corte Cost., sentenza n. 85/2013 del 9 Aprile 2013

CORTE DI GIUSTIZIA EUROPEA

- Causa C-22/71, sentenza della CGE del 25 Novembre 1971, (Beguelin Import c. S.A.G.L: Import Export)
- Causa C-48/69, sentenza della CGE DEL 14 Luglio 1972, (sentenza Imperial Chimical Industries Ltd. c. Commissione delle Comunità Europee)
- Causa C-32/74, sentenza della CGE, del 12 Novembre 1974
- Causa T-102/96, sentenza della CGE del 25 Marzo 1999, (sentenza Gencor LTD c-Commissione)
- Causa C-112/00, sentenza della CGE, 12 giugno 2003, (sentenza Schimeberg)
- Causa C-101/01 della Corte di Giustizia Europea del 6 Novembre 2003 (sentenza Lindqvist)

- Causa C-324/09, sentenza CGE (Grande Sezione) del 12 Luglio 2011, (sentenza Causa L'Oreal SA vs. Ebay International)

- Causa C-138/11, sentenza della CGE (Terza Sezione) del 12 luglio 2012 (sentenza Compass-Datenbank)

- Causa C-342/12, sentenza della CGE (Terza Sezione) del 30 Maggio 2013

- Cause riunite C-293/12 e C-594/12, sentenza della CGE (Grande Sezione) del 8 Aprile 2014

- Causa C-131/12, sentenza della CGE del 13 Maggio 2014

- Causa C-230/14, sentenza della CGE del 1 Ottobre 2015

- Cause riunite C-404/15 e C-659/15 PPU, sentenza della CGE (Grande Sezione) del 5 Aprile 2016,

- Causa C-398/15, sentenza della CGE (Seconda Sezione) del 9 Marzo 2017

CORTE EUROPEA DEI DIRITTI DELL'UOMO (CEDU)

- Sent. CEDU del 7 Luglio 1989, n. 14038/88 (Causa Soering c. Royaume Uni)

- Sent. CEDU del 11 Luglio 2000, n. 40035/98 (Causa Jabari c. Turquie)

- Sent. CEDU del 15 Marzo 2001, n. 58128/00, (Causa Ismaili c. Allemagne)

- Sent. CEDU del 4 Settembre 2014, n.140/10, (Causa Trabelsi c. Belgique)

SITOGRAFIA

- www.diritticomparati.it/profili-storico-comparativi-del-diritto-alla-privacy

- www.privacy.it/archivio/cassaz20010630.html

- www.privacyitalia.eu/gdpr-rivoluzione-copernicana/7825/

- www.ilfattoquotidiano.it/2015/10/09/costeja-gonzalez-negato-loblio-alluomo-che-lo-ha- *regalato-alleuropa-2/2111057/ (aggiornato al 15 Dicembre 2018).*

- www.medialaws.eu/diritto-alloblio-il-problema-della-estensione-extraeuropea-della-deindicizzazione-tra-effettivita-della-rimozione-e-liberta-di-informazione/ (aggiornato al 10/01/2019)

- www.ipsoa.it/~/media/Quotidiano/2015/07/22/Registro-delle-imprese--conservazione-dei-dati-e--oblio---questione-alla-Corte-UE/15096-15%20pdf.pdf

- www.altalex.com/documents/news/2015/12/09/diritto-a-oblio-pubblicita-obbligatoria

- *www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1185197*).

- www.treccani.it/enciclopedia/registro-delle-imprese-2-effetti_(Diritto-on-line)/#1funzionidelregistroedeffettidelliscrizione-1.

- www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/4298343

- www.protezionedatipersonali.it/informativa

- www.ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051

- www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf

- www.cybersecurity360.it/legal/data-breach-le-procedure-corrette-per-gestire-la-crisi.

- www.privacy.it/2018/04/27/massimini-registro-trattamenti-gdpr-deroga/

- www.ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51422.

- www.garanteprivacy.it/regolamentoue/approccio-basato-sul-rischio-e-misure-di-accountability-responsabilizzazione-di-titolari-e-responsabili.

- www.ec.europa.eu/newsroom/article29/item-detail.cfm? item_id=611233.

- www.enisa.europa.eu/publications/the-right-to-be-forgotten

- www.protezionedatipersonali.it/diritto-oblio

- www.iapp.org/resources/article/iapp-ey-annual-governance-report-2017/

- *www.confesercenti.it/blog/privacy-confesercenti-per-pmi-il-gdpr-e-stangata-da-almeno-2-miliardi-di-euro/*

- www.privacy.it/2018/01/18/consenso-gdpr-linee-guida-garanti-europei/

- www.privacy.it/2018/09/13/tar-friuli-dpo-iso-27001/

–www.garanteprivacy.it/documents/10160/0/ REGOLAMENTO+UE+Il+bilancio+di+applicazione+nel+2018