

**DIPARTIMENTO DI GIURISPRUDENZA**  
**Cattedra di Metodologia della Scienza Giuridica**

**IDENTITÀ “SUGGESTIONATA”: QUESTIONI TEORICHE E  
PRATICHE NEL RECENTE DIBATTITO SU GOOGLE  
SUGGEST**

**RELATORE**  
**Chiar.mo Prof.**  
**Antonio Punzi**

**CANDIDATO**  
**Rosanna Celella**  
Matr. 130353

**CORRELATORE**  
**Chiar.mo Prof.**  
**Mario Esposito**

**ANNO ACCADEMICO 2014-2015**

## INDICE

<i>Introduzione</i> .....	pag. 5
---------------------------	--------

### CAPITOLO I

#### RESPONSABILITÀ DEL MOTORE DI RICERCA PER LA FUNZIONE “*AUTO-COMLETE*”

<b>1. Come funziona il completamento automatico di Google?</b> .....	pag. 9
<b>2. La normativa italiana sulla responsabilità degli <i>Internet service provider</i></b> .....	pag. 10
2.1 Il <i>trend</i> giurisprudenziale del provider attivo: ascesa e declino a margine della pronuncia della Corte d’appello di Milano.....	pag. 17
<b>3. Le avventure legali di Google. L’orientamento giurisprudenziale italiano.</b> .....	pag. 19
3.1 Google condannata e poi assolta dal Tribunale di Milano. ....	pag. 19
3.2 L’ordinanza del Tribunale di Pinerolo.....	pag. 24
<b>4. &gt;&gt;&gt;segue: L’orientamento di alcune Corti straniere</b> .....	pag. 25
4.1 Suggestioni e inserzioni nella giurisprudenza francese.....	pag. 25
4.2 Il giudice di Milano e il giudice di Parigi: un confronto.....	pag. 28
4.3 Le vicende di Google in Germania.....	pag. 30
4.4 L’algoritmo di Google sotto accusa in tutto il mondo: dall’Australia all’Asia.....	pag. 33
<b>5. Responsabilità per violazione dei diritti di proprietà intellettuale.</b> .....	pag. 36

<b>6. Europa vs USA: diritti della personalità vs libertà di espressione</b> .....	pag. 38
6.1 Google <i>suggest</i> sotto la protezione del Primo emendamento .....	pag. 38
6.2 La protezione dei dati personali: divergenze e convergenze tra Europa e Stati Uniti .....	pag. 41
6.3 Il caso Snowden .....	pag. 44

## CAPITOLO II

### VERSO IL NUOVO REGOLAMENTO EUROPEO SULLA *DATA-PROTECTION*

<b>1. Il destino di <i>Google Suggest</i> alla luce della sentenza <i>Google 46Spain</i></b> .....	pag. 46
1.1 I capisaldi della sentenza della Corte di Giustizia Europea. Il fatto. ....	pag. 47
1.2 >>>segue: Il contesto delle attività di stabilimento .....	pag. 49
1.3 >>>segue: la procedura di de-indicizzazione .....	pag. 51
1.4 >>>segue: il diritto all'oblio .....	pag. 53
<b>2. Dalla giurisprudenza della Corte europea alla legislazione del Parlamento europeo</b> .....	pag. 58
<b>3. Il futuro Regolamento europeo</b> .....	pag. 61
3.1 La proposta di Regolamento .....	pag. 62
3.2 I principali punti approvati dal Parlamento europeo .....	pag. 65
3.3 Criticità e riflessioni .....	pag. 68
<b>4. Il Regolamento europeo e la posizione delle grandi aziende di comunicazione elettronica</b> .....	pag. 71

## CAPITOLO III

### DALL'IDENTITÀ PERSONALE ALL'IDENTITÀ VIRTUALE: PROFILI GIURIDICI, FILOSOFICI E SOCIOLOGICI

<b>1. Il diritto all'identità personale</b> .....	pag. 75
1.1 L'identità personale nel tempo e nel ( <i>cyber</i> ) spazio.....	pag. 76
<b>2. L'identità nella realtà virtuale</b> .....	pag. 79
2.1 Identità personale, Identità digitale, Profilo digitale.....	pag. 80
<b>3. Il concetto filosofico di identità</b> .....	pag. 82
<i>Conclusioni</i> .....	pag. 87
<i>Bibliografia</i> .....	pag. 98

## *Introduzione*

Nel presente elaborato si cercherà di individuare le conseguenze giuridiche connesse ai servizi offerti dai nuovi mezzi di comunicazione elettronica. In particolare, ci si soffermerà sulla recente funzionalità, creata dal motore di ricerca Google per facilitare le ricerche dei suoi utenti, *Google suggest*. Si tratta, precisamente, dei suggerimenti automatici che compaiono nella stringa di ricerca Google quando l'utente inizia a digitare un termine di ricerca. In molti casi, tali suggerimenti possono causare un abbinamento di termini che si riveli offensivo e diffamatorio nei confronti di persone fisiche, enti pubblici o imprese private; non di rado possono verificarsi violazioni della proprietà intellettuale o dei diritti fondamentali della persona. Quando, poi tali associazioni di parole non sono veritiere o non sono state aggiornate, l'individuo vedrà nel web la propria identità come alterata. Inoltre, un suggerimento automatico potrebbe creare, nell'utente cui viene proposto, aspettative non corrette in merito alla reputazione e all'identità del persona, oggetto delle sue ricerche; la funzione *Google suggest* potrebbe, in altri termini, creare un'identità "suggestionata".

Nel primo capitolo saranno analizzate alcune vicende legali di Google in tutto il mondo; attraverso un *excursus* giurisprudenziale che tocca i principali Paesi, si vorrà evidenziare come la vicenda *Google suggest* sia stata affrontata e risolta nei vari tribunali, dalla giurisprudenza di Paesi molto differenti tra di loro per cultura e sistema legislativo. Partendo dall'Italia e dalla normativa italiana sulla responsabilità dell'*Internet Service Provider* si analizzeranno una serie di casi pratici che hanno interessato il nostro Paese, passando poi ad individuare la risposta data, in vicende analoga, dalle corti francese e tedesca e giungendo fino all'Australia e all'*High Court of Hong Kong*. Si è voluto porre in evidenza il fatto che le pronunce sono spesso discordanti tra di loro, in quanto alcune corti hanno ritenuto Google responsabile per diffamazione, violazione dei diritti della personalità o delle norme sul *copyright*, altre, al contrario, hanno assolto il motore di ricerca. Le principali tesi accusatorie sono incentrate sul fatto che l'algoritmo che crea le associazioni automatiche non sia del tutto automatico e neutrale, ma postuli un intervento umano. Google si difende sostenendo che gli abbinamenti di parole sono frutto di un algoritmo indipendente dalla volontà dell'uomo e dell'azienda stessa, che funziona raccogliendo le ricerche effettuate nell'ultimo periodo dalla gran

parte degli utenti. L'argomento della neutralità dell'algoritmo, tuttavia, non offre una valida difesa in tutte le giurisdizioni. Le corti statunitensi inquadrano i suggerimenti di ricerca come espressioni di libertà di manifestazione del pensiero, costituzionalmente protetti dal Primo emendamento. La validità di questa difesa è meno forte in Europa, laddove Google è spesso ritenuta responsabile di violazione di diritti della personalità ad opera della sua funzione di completamento automatico. In particolare si è approfondita la differente reazione tra Stati Uniti ed Europa, evidenziando come da un lato vi sia la tendenza a garantire libertà d'espressione e libertà d'impresa e dall'altro l'attenzione sia rivolta soprattutto alla tutela dei diritti della personalità. In nome della libertà di informazione si è sostenuto che l'algoritmo di Google opera meramente come facilitatore delle ricerche sul web. Nel campo della proprietà intellettuale, invece, la responsabilità del motore di ricerca sorge nel momento in cui le associazioni di parole inducono verso comportamenti illegittimi, ad esempio indirizzando l'utente verso siti di pirateria.

La vicenda dei suggerimenti automatici di Google, alla luce del noto caso *Google Spain*, ha forse avuto un punto di svolta. Pur riguardando i risultati di ricerca, senza dubbio la sentenza si pone in stretta connessione anche con la funzione *auto-complete* di Google e le imposizioni imposte dalla Corte di giustizia dell'Unione Europea in merito ai risultati di ricerca dovranno applicarsi anche ai suggerimenti di ricerca automatica; ciò per garantire all'interessato la rimozione di ogni collegamento ai *link* per lui diffamatori, sia attraverso ricerche correlate che attraverso suggerimenti di ricerca. Nel secondo capitolo ci riferiremo, infatti, alla giurisprudenza europea, partendo dalla sentenza del 13 maggio 2014 che si pone su una linea di continuità con altre due importanti sentenze in tema di conservazione dei dati personali e di diritto all'oblio, ossia la sentenza dell'8 aprile 2014 e del 6 ottobre 2015. Se fino ad ora si era tentato di sacrificare la *privacy* in nome della sicurezza nazionale e della libertà d'impresa, la recente linea di tendenza tenuta dalla giurisprudenza europea ha cambiato direzione: i diritti fondamentali della persona prevalgono sulle esigenze di sicurezza e di mercato. L'ultimo orientamento giurisprudenziale della Corte di giustizia dell'Unione europea confluirà senz'altro, con le dovute acconce, nel nuovo Regolamento europeo sulla protezione dei dati personali, in discussione presso le istituzioni europee dal 2012 e di vicinissima approvazione. Tale Regolamento, di cui affronteremo i punti approvati in prima lettura, le criticità e le

innovazioni e in particolare le posizioni delle grandi imprese di comunicazione elettronica, sarà destinato a sostituire tutte le normative di recepimento della Direttiva 95/96 nei vari Stati membri, compreso il nostro attuale *Codice della privacy*. Nell'ultimo capitolo ritorneremo al punto di partenza della nostra indagine, per trarre le dovute conclusioni: l'identità "suggestionata". Cosa si intende per identità e quando la stessa può dirsi "suggestionata", nella specie, da suggerimenti automatici o da altri servizi offerti dalla rete?

Il problema della conservazione della propria identità nel *cyber spazio* è oggi di rilevante importanza. L'identità personale è minata, nel *web*, dall'esistenza di identità digitali e profili digitali. Il confine tra vita reale e vita virtuale è sempre più labile in quanto la vita sociale, lavorativa e privata del singolo si esplica non solo nella realtà fisica ma anche, e ormai quasi del tutto, in quella telematica, con gli eventuali rischi connessi alla tutela dei propri dati personali, i quali, una volta immessi in rete sono destinati a rimanervi incastrati in una sorta di eterno presente, proprio perché la rete "non dimentica". Analizzando il concetto di identità personale dal punto di vista giuridico vedremo come il diritto all'identità personale ingloba in sé anche quello alla riservatezza, alla reputazione e lo stesso diritto all'oblio. Anche l'analisi dell'identità dal punto di vista filosofico, specie nell'ottica dei due filosofi Locke e Hume, ci porterà a notare come il concetto di identità sia strettamente connesso a quello di memoria: l'identità dell'individuo si forma dagli eventi non solo presenti, ma anche passati che l'hanno contraddistinto. Dunque conservare la propria identità vuol dire anche preservarla non solo da informazioni false e distorte, ma anche da eventi passati che dovrebbero essere rimossi dalla memoria collettiva. Ritorna il tema del diritto all'oblio connesso con quello di identità e con la contrapposta esigenza di tutela della libertà d'informazione e della verità storica.

Il mondo del *cyber spazio* ha bisogno di rigidi interventi normativi per poter garantire la sicurezza di chi in esso vi opera? Nel contemperamento di interessi, prevalgono i diritti della personalità o la libertà d'informazione e d'iniziativa economica? E il singolo individuo, in questo scontro continuo, in questa "*cyber-war*" tra i grandi giganti delle comunicazioni elettroniche, il legislatore europeo e i governi degli Stati più influenti nel contesto geopolitico internazionale, che ruolo occupa? A questi e ulteriori interrogativi tenteremo di rispondere nel corso della trattazione. Una constatazione è però doverosa:

noi singoli utenti della rete dobbiamo approfittare degli innumerevoli benefici che essa ci offre, dei servizi di facilitazione nel reperimento di informazioni che grandi aziende come Google ci forniscono, dobbiamo navigare nella rete senza freni e timori, ma con consapevolezza.



## CAPITOLO I

# **Responsabilità del motore di ricerca per la funzione “*auto-complete*”**

### **1. Come funziona il completamento automatico di Google?**

Durante la digitazione nella stringa di ricerca di uno o più termini di ricerca, Google è in grado di proporre delle previsioni di completamento automatico che spesso suggeriscono all'utente le informazioni desiderate. È la stessa società a spiegare come funziona Google *suggest* e come utilizzarlo. Google puntualizza nella sua “guida di ricerca” che tali previsioni costituiscono possibili termini di ricerca e non dichiarazioni riconducibili alla società o a terzi, né risposte alla ricerca eseguita. Le *query* di ricerca mostrate vengono generate automaticamente, senza l'intervento dell'uomo, da un algoritmo che funziona sulla base di fattori oggettivi, quali la frequenza con cui gli altri utenti del web hanno ricercato quella stessa parola e i contenuti delle pagine *web* indicizzate dal motore di ricerca. L'algoritmo ideato da Google rileva ed esclude automaticamente alcuni termini di ricerca per uno dei seguenti motivi: il termine di ricerca non è sufficientemente utilizzato; si tratta di un termine di ricerca troppo recente; il termine di ricerca è stato erroneamente considerato un termine che viola le norme. Non è possibile disattivare il completamento automatico perché è integrato nella Ricerca Google ed è uno degli strumenti ideati dal colosso di Mountain View per garantire agli utenti lo svolgimento di ricerche in modo facile e veloce.

La funzione di completamento automatico nasce infatti per assistere le persone con disabilità fisiche, col proposito di agevolarle nella ricerca. L'algoritmo genera suggerimenti di ricerca che gli utenti avrebbero in ogni caso ricercato, tuttavia, alcune volte, le combinazioni di parole proposte dalla funzione di riempimento automatico, pur non corrispondendo all'intento di ricerca iniziale del soggetto, possono generare nello stesso un sentimento di curiosità, spingendolo ad optare per la ricerca suggerita. In quest'ultimo caso la ricerca non viene semplicemente facilitata, bensì orientata ed in questo scenario i suggerimenti di ricerca potrebbero assumere rilevanza legale.

Il fenomeno Google *suggest* è divenuto il caso esemplare in cui libertà d'informazione e diritti della personalità entrano in conflitto nel mondo del *web*. Sorgono infatti ripercussioni in ambito legale quando l'algoritmo genera combinazioni di termini che possono avere valenza diffamatoria nei confronti di una persona fisica o giuridica oppure che possono risultare non veritiere. Può inoltre accadere che i suggerimenti di ricerca indirizzino il navigatore verso le "acque" illegali della pirateria, con ripercussioni negative nel campo della proprietà intellettuale. Molti casi tra di loro simili sono stati esaminati dalle Corti di svariati Paesi nel mondo, spesso giungendo a conclusioni differenti e contrastanti: in alcuni casi il motore di ricerca è stato condannato per diffamazione, in altri, al contrario, non è stato ritenuto responsabile.

Le differenti pronunce in merito alla responsabilità del motore di ricerca nei vari Paesi del mondo non dipendono esclusivamente dalle divergenze legali e giurisprudenziali locali, ma anche, e soprattutto, dall'ambiguità di funzionamento dell'algoritmo di Google e dalla difficoltà di verificare e dimostrare le sue implicazioni a livello legale: qual è la natura legale delle *query* di ricerca? Da chi o da cosa vengono sostanzialmente generate? Un semplice algoritmo può essere ritenuto responsabile? La funzione *auto-complete* è realmente riconducibile ad un algoritmo automatico o presuppone a monte un intervento umano? Sono queste le domande che si sono poste i giudici di quasi tutto il mondo, giungendo a delle pronunce tra loro poco o per nulla omogenee. In questo capitolo analizzeremo gli orientamenti giurisprudenziali dei vari Paesi, partendo dal quadro normativo e giurisprudenziale italiano.

## **2. La normativa italiana sulla responsabilità degli *Internet Service Provider***

La questione sulla responsabilità è un fenomeno di natura globale, tuttavia sono i singoli orientamenti giurisprudenziali a determinarla, soprattutto laddove, come in Italia, la normativa specifica risulti ambigua e lacunosa. Il d.lgs. 9 aprile 2003 n.70, di recepimento della Direttiva CE 31/2000 sul commercio elettronico, individua un sistema di responsabilità per gli ISP alternativo a quello previsto dal codice civile italiano. In caso di inapplicabilità del regime di esonero di responsabilità previsto dal

suddetto decreto, resta fermo il regime comune, il quale prevede: la responsabilità aquiliana basata su colpa e dolo ex art. 2043 c.c., la responsabilità oggettiva aggravata ex artt. 2050<sup>1</sup> e 2051<sup>2</sup> c.c. cui si ricollega la responsabilità per trattamento illecito di dati personali prevista dall'art.15<sup>3</sup> del d.lgs. 196/03<sup>4</sup> e, infine, la responsabilità civile connessa alla violazione dei diritti di proprietà intellettuale e industriale. L'esonero di responsabilità del prestatore di servizi deve considerarsi eccezionale rispetto al generale sistema di responsabilità civile d'impresa, di conseguenza i casi di esonero che rientrano nell'ambito applicativo del decreto oggetto d'analisi devono considerarsi tassativamente predeterminati dalla legge.

L'ambito soggettivo di applicazione della disciplina si riferisce a due categorie di soggetti: i cosiddetti "destinatari del servizio", ossia quei soggetti che, a scopi professionali e non, utilizzano un servizio della società dell'informazione per ricercare informazioni o renderle accessibili; il "prestatore", inteso come persona fisica o giuridica che presta un servizio della società dell'informazione.

Per quanto attiene all'ambito oggettivo di applicazione della disciplina, esso non è limitato al commercio elettronico, pur essendo quest'ultimo la più importante attività economica esercitata *online*, ma si estende anche ad una diversa attività economica, quale la fornitura dei servizi connessi alla società dell'informazione<sup>5</sup>.

Il d.lgs. 70/03 distingue tre tipi di responsabilità del gestore, in funzione del tipo di attività fornita:

- semplice trasporto di informazioni (*mere conduit*) di cui all'art.14;
- memorizzazione temporanea ed automatica di informazioni (*caching*) di cui all'art.15;
- memorizzazione di informazioni fornite dal destinatario del servizio (*hosting*) di cui all'art.16.

---

<sup>1</sup><<Chiunque cagiona danno ad altri nello svolgimento di un'attività pericolosa, per sua natura o per la natura dei mezzi adoperati, è tenuto al risarcimento, se non prova di avere adottato tutte le misure idonee ad evitare il danno>>.

<sup>2</sup>Responsabilità per danni causati da cose in custodia.

<sup>3</sup><<Chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile>>

<sup>4</sup>Codice in materia di protezione dei dati personali

<sup>5</sup>Si deve intendere, ai sensi della Direttiva CE N.34/98 modificata dalla Direttiva 48/98, <<qualsiasi servizio, prestato normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi, cioè della persona fisica o giuridica che, a scopi professionali e non, utilizza un servizio della società dell'informazione, anche per ricercare o rendere accessibili delle informazioni>>.

Condizione fondamentale per beneficiare dell'esonero è la totale estraneità del prestatore di servizi al contenuto della trasmissione, o meglio la sua passività rispetto ai contenuti immessi da terzi. Da qui si ricava la distinzione tra ISP passivo e ISP attivo e solo il primo sarà beneficiario dell'esonero di responsabilità ex d.lgs. 70/03. L'art.14 stabilisce che il *provider* che svolge attività di "*mere conduit*", ossia trasmette su una rete informazioni fornite da un destinatario del servizio o fornisce accesso alla rete, non è responsabile delle informazioni trasmesse a condizione che:

- a) non dia origine alla trasmissione;
- b) non selezioni il destinatario;
- c) non modifichi le informazioni trasmesse.

L'attività di *caching* prevista invece dall'art.15 consiste nel trasmettere su una rete le informazioni fornite da un destinatario del servizio, memorizzandole in forma automatica e temporanea, con lo scopo di rendere più efficace il successivo inoltramento delle stesse ad altri destinatari che lo richiedano. In questo caso il prestatore di servizi non è responsabile laddove:

- a) non modifichi le informazioni;
- b) agisca prontamente per rimuovere le informazioni memorizzate o per disabilitare l'accesso, non appena venga effettivamente a conoscenza del fatto che le informazioni sono state rimosse dal luogo dove si trovavano inizialmente sulla rete, o che l'accesso a tali informazioni è stato disabilitato, oppure che un'autorità giurisdizionale o amministrativa ne ha disposto la rimozione o ha ordinato di disabilitarne l'accesso.

In ultimo, l'art. 16 analizza l'attività di *hosting*, ossia di memorizzazione di informazioni fornite da un destinatario del servizio su richiesta di quest'ultimo, tramite un contratto atipico in base al quale il *provider* si obbliga nei confronti di un altro soggetto a locare uno spazio di memoria sul proprio *server* e a fornire servizi di varia natura ad esso collegati, quali ad esempio assistenza tecnica o sviluppo *software*. In tali circostanze il prestatore di servizi non è responsabile a condizione che:

- a) non sia effettivamente a conoscenza del fatto che l'attività o l'informazione è illecita (illecito penale);
- b) non sia al corrente di fatti o circostanze che rendano manifesta l'illegalità dell'attività o dell'informazione (illecito civile);

c) non appena a conoscenza di tali fatti, su comunicazione delle Autorità competenti, agisca immediatamente per rimuovere le informazioni o disabilitarne l'accesso.

L'autorità giudiziaria e amministrativa hanno una funzione di vigilanza e possono esigere, anche in via d'urgenza, che il prestatore di servizi impedisca o ponga fine alle eventuali violazioni commesse.

L'art. 17 del decreto in questione stabilisce, inoltre, che il *provider* non è assoggettato ad un obbligo generale di sorveglianza sulle informazioni che trasmette o memorizza, né ad un obbligo generale di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite. Il prestatore di servizio tuttavia è tenuto ad informare senza indugio l'autorità competente di presunte attività o informazioni illecite riguardanti il destinatario, di cui sia venuto a conoscenza. È tenuto inoltre a comunicare senza indugio alle competenti autorità, quando queste lo richiedano, informazioni che consentano l'identificazione del destinatario dei servizi, al fine di prevenire attività illecite. L'ISP passivo dunque sarà responsabile civilmente qualora non rimuova prontamente un contenuto illecito su richiesta dell'autorità giudiziaria o amministrativa avente funzione di vigilanza, o qualora non informi le predette autorità, pur essendo venuto a conoscenza del carattere illecito o pregiudizievole per un terzo del contenuto di un servizio a cui assicura l'accesso.

Sulla base dei principi qui richiamati, l'intenzione del legislatore sembrerebbe quella di voler escludere in linea di massima la responsabilità degli ISP passivi o comunque di non caricare i *provider* di una forma di responsabilità troppo gravosa. Questa, infatti, avrebbe potuto influenzare negativamente le scelte economiche e gli investimenti dei gestori di servizi, oltre che condizionarli notevolmente sulla selezione dei contenuti, all'ombra del timore che potessero rivelarsi lesivi dei diritti degli utenti. Tuttavia si riscontra un'ambiguità nella disciplina su richiamata, in quanto il principio dell'assenza dell'obbligo di sorveglianza appare limitato dall'obbligo di segnalazione all'autorità dei fatti illeciti di cui il *provider* venga a conoscenza. L'ambiguità è dettata dall'esigenza di bilanciare, da un lato gli interessi legati all'indipendenza della rete e la libertà di espressione, dall'altro la tutela dei soggetti che potrebbero essere danneggiati dagli illeciti telematici. Quindi, se per un verso si tende ad escludere la responsabilità per fatto illecito degli ISP, dall'altro verso si ha la decadenza automatica dal beneficio di esclusione di responsabilità civile in caso di conoscenza del fatto illecito e mancata

segnalazione all'autorità (art.17). Sorgono poi criticità in merito all'espressione "a conoscenza" (Tosi 2012). Quando, ai sensi del d.lgs. 70/03 il provider può dirsi "a conoscenza" di un fatto illecito? In base all'art.15 l'obbligo di rimuovere o disabilitare l'accesso alle informazioni deriva dall'essere effettivamente a conoscenza del fatto che le informazioni sono state rimosse o che l'accesso è stato disabilitato. Nell'art. 16, invece, leggiamo <<essere effettivamente a conoscenza del fatto illecito penale>> ed <<essere al corrente del fatto illecito civile>>. Quindi dalla conoscenza semplice ex art.17, si passa alla conoscenza effettiva ex art. 15 oppure all' "essere al corrente dei fatti", espressione di cui all'art. 16. Si osserva dunque un utilizzo improprio ed equivoco di livelli di conoscenza diversificati. Un'ulteriore criticità legata alla disciplina dettata dal d.lgs. 70/03 deriva dal fatto che nel corso degli anni i servizi offerti dai *provider* sono aumentati, rendendo più complessa la verifica di una perfetta corrispondenza tra attività svolta e attività descritta dagli articoli del decreto (Pirozzoli 2012). Ne è un esempio la funzione di completamento automatico di Google, poiché se il giudice del Tribunale di Pinerolo<sup>6</sup> ha qualificato tale attività come attività di *hosting*, non è giunto alle stesse conclusioni il Tribunale di Milano<sup>7</sup>, il quale ha ritenuto che tale servizio si riferisce alla speciale modalità operativa di un *software* creato dalla società, la quale sarà per ciò stesso indubbiamente responsabile delle lesioni causate agli utenti dal servizio *auto-complete*. Ne discende dunque l'applicazione di due regimi di responsabilità differenziati in capo alla società che gestisce il servizio in questione. Il d.lgs. 70/03 lascia un ampio margine di discrezionalità al giudice che dovrà valutare *case by case* il comportamento del gestore del servizio, con la conseguenza di uno scenario giuridico incerto e poco omogeneo. Nell'elaborazione giurisprudenziale più recente è emersa la necessità di individuare una nuova figura atipica, l'ISP attivo, al fine di escludere l'applicabilità del beneficio di irresponsabilità di cui al d.lgs. 70/2003. L'esigenza è maturata proprio con riguardo alle peculiari attività svolte dai motori di ricerca, primo fra tutti Google, dai social network, come Facebook e dagli aggregatori di contenuti caricati da terzi sulla rete, come YouTube. Generalmente i motori di ricerca e gli aggregatori di contenuti sono identificati come ISP passivi, tuttavia occorre verificare che in concreto si limitino a svolgere attività di *hosting* passivo e non

---

<sup>6</sup>Ordinanza del Tribunale di Pinerolo del 2 maggio 2012; cfr. cap.1, par. 3.2

<sup>7</sup>Ordinanza del Tribunale di Milano del 24 marzo 2011; cfr. cap.1, par. 3.1

svolgano invece ulteriori attività non meramente automatiche, quali ad esempio indicizzazione, selezione, organizzazione e filtraggio dei contenuti, raccolta pubblicitaria. Se con riferimento a tali ulteriori servizi è accertato anche un pur minimo grado di consapevolezza dell'operatore, tanto da renderli non meramente automatizzati, si ricade al di fuori dell'ambito di applicazione del d.lgs. 70/03. Dunque, un motore di ricerca perde il beneficio dell'irresponsabilità di cui al su citato decreto nel caso in cui, in concreto, svolga un'attività di consapevole indicizzazione ed organizzazione dei contenuti da cui tragga un utile economico (Tosi 2012). Una tale attività può essere ricondotta ad una responsabilità editoriale in senso lato. La vicenda statunitense del *Digital Millennium Copyright Act* ed altre analoghe<sup>8</sup> ci indicano che il *provider* è responsabile nel caso in cui abbia un pur minimo contributo all'editing del materiale lesivo di interessi tutelati dall'ordinamento o ne abbia consentito la pubblicazione originaria in rete mediante la predisposizione di un sito e quindi non sia più un semplice trasmittente di informazioni. Da ciò si deduce che non a tutti i *provider* può essere addebitata la responsabilità, ma solo ai cosiddetti *content provider*, ossia per l'appunto quei provider che consentono la pubblicazione elettronica in rete per la prima volta o contribuiscono alla realizzazione del sito o all'editing del materiale illecito. La figura dell'ISP attivo si pone dunque a metà tra quella del *content provider* e dell'ISP passivo. Naturalmente questa nuova figura fa sorgere problemi di non agevole soluzione e l'esigenza di valutare con prudenza i casi di esclusione dell'esonero di responsabilità. Inoltre è opportuno precisare che, mentre per far acquisire all'ISP attivo la consapevolezza del fatto illecito idonea a far escludere l'esonero della responsabilità è sufficiente una diffida stragiudiziale, nel caso dell'ISP passivo la conoscenza si acquisisce solo in seguito alla comunicazione proveniente dalle autorità competenti, in base a quanto disposto dall'art.16. Dunque, per considerare presupposto della conoscenza la diffida stragiudiziale, in luogo alla comunicazione delle autorità competenti ed escludere il beneficio dell'irresponsabilità previsto dal d.lgs. 70/03, bisogna aver preliminarmente qualificato il motore di ricerca come ISP attivo. Anche il regime normativo dell'Unione Europea è articolato in base al ruolo e alle funzioni svolte dalle diverse categorie di operatori: gli *access provider*, che sono meri fornitori d'accesso alle reti di comunicazione elettronica, esonerati dunque da qualsiasi

---

<sup>8</sup> cfr. cap.1, par. 5

responsabilità; gli *Internet Service Provider* (passivi) che svolgono attività di diffusione passiva dei contenuti (*mere conduit, caching o hosting*), in generale eleggibili ad una deroga di responsabilità; gli ISP attivi, che non hanno tardato ad emergere anche nel contesto europeo e che si differenziano dagli altri ISP perché non si limitano a svolgere una funzione di diffusione passiva dei contenuti, ma interferiscono sull'elaborazione e presentazione finale degli stessi. Tuttavia la responsabilità di questi ultimi non può definirsi *una tantum*, ma va vagliata caso per caso sulla base del grado di interferenza concretamente esercitato nell'attività dei soggetti terzi, ossia i *content provider*, i quali sono i soli direttamente responsabili delle violazioni (Caggiano 2014). La Corte di giustizia dell'Unione Europea ha rilevato che spetta al giudice del rinvio valutare se il ruolo svolto dal prestatore sia neutro, ovvero se svolga attività meramente tecniche, automatiche e passive, in mancanza di conoscenza o di controllo dei dati che memorizza. In tal caso il *provider* non può essere ritenuto responsabile per i dati che egli ha memorizzato su richiesta di un inserzionista, salvo che, essendo venuto a conoscenza dell'illiceità di tali dati o dell'attività dell'inserzionista, non abbia prontamente rimosso tali dati o disabilitato l'accesso ad essi. Dunque mentre nella sentenza *Google Spain*<sup>9</sup> la Corte ha statuito che l'attività del motore di ricerca è sicuramente qualificabile come attività di trattamento-dati, con conseguente applicazione della disciplina prevista dal d.lgs. 196/03, negli altri casi ha preferito lasciare al giudice del rinvio la qualificazione in concreto dell'attività dell'ISP.

Ricapitolando e concludendo, i gestori dei servizi in rete possono essere interessati da tre tipi di responsabilità:

- responsabilità speciale per gli *Internet Service Provider* (passivi), ossia responsabilità per colpa omissiva;
- responsabilità comune ex art. 2043 per gli *Internet Content Provider* e per gli ISP attivi, ossia responsabilità per colpa commissiva;
- responsabilità oggettiva del *content provider* o dell'ISP attivo, derivante dal trattamento illecito dei dati personali e dall'inosservanza delle misure necessarie alla sicurezza dei dati (art.15, d.lgs. 196/03).

---

<sup>9</sup>Sentenza della Corte di Giustizia dell'Unione Europea del 13 maggio 2014; cfr. cap. 2.



## **2.1. Il trend giurisprudenziale del *provider* attivo: ascesa e declino a margine della pronuncia della Corte d'appello di Milano**

Abbiamo già analizzato come il regime di responsabilità dei fornitori di *hosting* sia stato notevolmente influenzato dall'evoluzione dei servizi offerti dai *provider* che mette a rischio il mantenimento, in loro favore, del beneficio dell'esonero di responsabilità previsto dall'art. 14 della Direttiva 2000/31 e dagli artt. 16 e 17 del d.lgs. 70/03 di recepimento della direttiva nel nostro Paese. Il complesso di attività che oggi i *provider* sono in grado di offrire rischia di far perdere loro quelle caratteristiche di neutralità e passività su cui si fonda il regime sancito dalla Direttiva europea. In questo contesto è venuta affermandosi la creazione giurisprudenziale dell'*hosting provider attivo*, ossia quel fornitore di *hosting* che, pur non giungendo a configurare un *content provider*, svolge un'attività non del tutto neutra e passiva di organizzazione e gestione dei materiali immessi dagli utenti, nonché la loro utilizzazione a fini economici<sup>10</sup>.

La figura del provider attivo è stata però rifiutata di recente dalla Corte d'appello di Milano<sup>11</sup>. Il caso di specie riguardava la lesione dei diritti d'autore a danno della società RTI, in quanto era stato pubblicato sulla piattaforma YAHOO! materiale immesso da terzi, avente ad oggetto opere il cui sfruttamento era titolarità esclusiva della società attrice. Il giudice di primo grado aveva qualificato l'attività di *hosting* come non neutrale e non meramente passiva, sancendo l'esclusione del regime privilegiato di responsabilità e stabilendo l'applicazione dell'art 2043 c.c.

La Corte d'appello, invece, sembra non condividere questa impostazione, sostenendo che la responsabilità dell'*hosting provider* sussista solo nel caso in cui questi si sia reso partecipe del caricamento dei dati o quando, reso edotto dell'illiceità dei contenuti immessi da terzi, non abbia provveduto a rimuoverli. Infatti, in base al d.lgs. 70/03, l'obbligo di rimozione scatta non appena avuta notizia dell'illecito, poiché non esiste un obbligo generale e preventivo di sorveglianza sui contenuti pubblicati da terzi su una

---

<sup>10</sup> Si pensi ad esempio al ritorno finanziario ottenuto mediante lo sfruttamento pubblicitario derivante dalla presentazione dei contenuti.

<sup>11</sup> Corte di Appello di Milano, 7 gennaio 2015.

piattaforma. La responsabilità dell' *hosting provider* non implica un'attività preventiva, ma sorge a posteriori in caso di inottemperanza alla richiesta di rimozione dei contenuti illeciti. La Corte milanese ritiene che: *<<le attuali tecnologie avanzate, in mancanza di altri elementi in grado di fare intravedere una vera e propria manipolazione dei dati immessi da parte dell'hosting provider, non siano da sole in grado di determinare il mutamento della natura del servizio di hosting provider di tipo passivo (...) in servizio di hosting provider di tipo attivo>>* e inoltre i servizi forniti nel caso di specie dall'*hosting provider* *<<non sono indici rivelatori di un'attività di interferenza sui contenuti pubblicati nel sito, come tali in grado di mutare il regime di responsabilità a posteriori dell'hosting provider>>*. Ma il passaggio decisivo della pronuncia si ha quando la Corte afferma testualmente che: *<<ragionando sulla base delle argomentazioni contenute nelle decisioni delle Corti europee (...) la nozione di hosting provider attivo risulti oggi sicuramente fuorviante e sicuramente da evitare concettualmente in quanto mal si addice ai servizi di "ospitalità in rete" in cui il prestatore non interviene in alcun modo sul contenuto caricato dagli utenti, limitandosi semmai a sfruttarne commercialmente la presenza sul sito, ove il contenuto viene mostrato così come è caricato dall'utente senza alcuna ulteriore elaborazione da parte del prestatore>>*. Dunque, nell'opinione della Corte, il carattere di neutralità dell'attività dell'*hosting provider* persiste sino a che egli non intervenga direttamente sul contenuto informativo caricato sulla piattaforma da lui gestita, modificandolo e/o alterandolo. Ma in tal caso non avrebbe più senso fare ricorso alla figura dell'*hosting provider* attivo, in quanto il prestatore di servizi si è già trasformato in un *content provider* (Bugiolacchi 2015). Al momento non è dato sapere se le conclusioni della Corte milanese comporteranno il declino della figura dell' *hosting provider* attivo creata dall'opposto orientamento giurisprudenziale; tuttavia ciò che emerge è che la nozione di *provider* attivo è svincolata sia da riferimenti normativi che da indici di valutazione adoperati dalla Corte europea e presenta inconvenienti legati all'esigenza di una valutazione casistica dell'attività svolta dal fornitore di servizi di *hosting*. Sarebbe invece opportuna una revisione della Direttiva 2000/31 che aggiorni la disciplina della responsabilità degli *hosting provider* alla luce delle nuove funzionalità offerte da questi prestatori, al fine di assicurare un'armonizzazione normativa in un campo in cui l'approccio caso per caso si è rivelato insufficiente, ed allo scopo di garantire il

bilanciamento tra diritti contrapposti, in particolare, diritto d'autore e diritto alla riservatezza da un lato e libera manifestazione del pensiero e diritto all'informazione dall'altro.

### **3. Le avventure legali di Google. L'orientamento giurisprudenziale italiano.**

Il *business model* di Google è segnato dal motto che recita “tutto è lecito in Internet”. Questa visione così radicale non è certamente condivisa dai soggetti terzi che potrebbero essere lesi dalle attività poste in essere dal motore di ricerca. I servizi forniti da Google possono avere spesso implicazioni sul tema della *privacy*, del *copyright* o delle regole di mercato e della concorrenza. In questa sede ci occuperemo dei primi due ambiti, in particolare con riferimento alla funzione di completamento automatico, *Google suggest*.

Negli ultimi anni, numerose avventure legali hanno interessato il colosso californiano promuovendo spesso un'evoluzione nell'ambito legislativo che riflette la strategia di Google o, al contrario, che hanno spinto il motore di ricerca ad adattarsi alle previsioni di legge nel pieno rispetto della normativa europea. Non si può ancora ragionevolmente ipotizzare quali saranno i risvolti futuri. Sarà Google ad adattarsi sempre di più alla legge o la legge ad essere condizionata dal gigante di Mountain View?

#### **3.1. Google condannata e poi assolta dal Tribunale di Milano.**

Il Tribunale di Milano, nell'ordinanza del 24 marzo 2011 ha ritenuto Google responsabile per diffamazione e relativi danni civili per l'automatico accostamento delle parole <<truffa>> e <<truffatore>> al nome di un imprenditore italiano operante nel settore finanziario, accostamento risultante dalle ricerche nominative effettuate sul motore di ricerca, a causa della funzione di completamento automatico. L'imprenditore non lamenta a Google la mancata adozione di filtri preventivi idonei ad impedire il

verificarsi di abbinamenti di parole offensivi e lesivi di diritti della persona costituzionalmente tutelati, bensì il fatto che la società convenuta non sia intervenuta *ex post*, cioè dopo la sua segnalazione, per eliminare l'abbinamento censurato.

Il ricorrente riconduce la responsabilità del motore di ricerca a quanto previsto dagli artt. 15 e 16 del d.lgs. 70/03, in virtù dei quali l'*hosting provider* è considerato responsabile solo laddove sia effettivamente a conoscenza dell'illiceità delle informazioni fornite o ne sia venuto a conoscenza e non abbia provveduto tempestivamente alla rimozione delle stesse. In questo caso infatti, secondo l'imprenditore, Google ha ommesso l'intervento doverosamente correttivo. Google si difende evidenziando il fatto che essa si limita a fornire una piattaforma di *hosting* di per sé neutra e che può essere potenzialmente lesiva solo in virtù di contenuti illeciti eventualmente immessi da terzi e dunque non addebitabili all'azienda. Google precisa che il motore di ricerca è costituito da un software creato dall'azienda stessa, ma che agisce secondo un algoritmo matematico operante su basi esclusivamente statistiche e automatiche; non vi è dunque alcun preventivo intervento umano atto ad impedire, modificare o alterare i risultati di ricerca. Da ciò si deduce l'assenza di ogni sua responsabilità ex art.16 del d.lgs. 70/03 e, nello specifico, nessuna inottemperanza ad un obbligo di rimozione, in quanto nessun ordine dell'autorità risulta essere stato adottato nei suoi confronti. Tuttavia il giudice di *prima cure* ha accolto il ricorso cautelare, ordinando a Google di rimuovere l'associazione indebita, la quale presenta senza dubbio valenza diffamatoria e soprattutto è in grado di ingenerare nell'utente il sospetto di attività non lecite da parte dell'imprenditore e distoglierlo dal proseguire la ricerca nei suoi confronti. Google propone reclamo ritenendo che le associazioni di termini dovute alla funzione *auto-complete* non sono create dal *software* di Google, ma sono il risultato delle ricerche più popolari effettuate dagli utenti. La società reclama inoltre l'omissione da parte del giudice di primo grado di una motivata affermazione di responsabilità; non solo essa ha ampiamente dimostrato la sua natura di ISP, ma anche il ricorrente aveva espressamente riconosciuto la sua qualità di *hosting provider* ex d.lgs. 70/03, dunque non può essere considerata responsabile dei contenuti immessi in rete da terzi.

Ma cos'è realmente Google? Google è un *provider* che offre servizi di motore di ricerca. I motori di ricerca sono *database* che indicizzano i testi sulla rete ed offrono

agli utenti un accesso per la consultazione; sono dunque una banca dati più un *software*, più precisamente sono banche dati che gestiscono un catalogo delle migliori pagine selezionate dal *web*. Google, in particolare, è un enorme *database* di pagine *web* prelevate dagli *spiders* o *crawlers*<sup>12</sup> quasi sempre dal *web* e memorizzate su enormi sistemi di *storage*<sup>13</sup>. Dunque i motori di ricerca sono vere e proprie raccolte di dati, informazioni, opere ,consultabili attraverso la digitazione di “parole chiave”, che organizzano informazioni, ricavate da data-base propri o trovate in rete attraverso gli *spiders* e offerte agli utenti. Google è un *hosting provider*, ossia un soggetto che si limita ad offrire ospitalità sui propri *server*<sup>14</sup> ad un sito internet gestito da altri e dunque assoggettato al beneficio di irresponsabilità. Tuttavia è evidente che il servizio Google *suggest* funzioni attraverso il trattamento dei dati presenti sulle pagine *web* immesse da soggetti terzi, secondo il criterio dei termini di ricerca più utilizzati dagli utenti<sup>15</sup>. È dunque il meccanismo del *software* creato da Google a determinare gli abbinamenti che costituiscono previsioni possibili di ricerca e che appaiono all’utente che digita la parola chiave. Secondo il Tribunale di Milano, è la scelta a monte e l’utilizzo di tale sistema e del suo particolare meccanismo operativo a determinare, a valle, la responsabilità di Google per i risultati che il meccanismo produce, essendo irrilevante l’assenza di ogni intenzionalità lesiva da parte del *provider*. Il collegio conferma quindi la decisione del giudice di primo grado ed in particolare condivide la sua valutazione in merito al carattere diffamatorio dell’associazione al nome del ricorrente delle parole “truffa” e “truffatore” ed alla suggestione negativa che l’improprio abbinamento genera nell’utente. Non è stata condivisa la tesi di Google secondo la quale la suggestione iniziale sarebbe eliminata dal fatto che sul *web* non sia presente alcun contenuto corrispondente al suggerimento di ricerca proposto. Questo perché, in mancanza della scelta dell’utente di leggere a approfondire i contenuti della pagina, <<resta solo

---

<sup>12</sup> *Software* che analizza i contenuti di una rete o di un *database*, in genere per conto di un motore di ricerca. Operano, solitamente, acquisendo una copia testuale di tutti i documenti visitati e inserendole in un indice.

<sup>13</sup> *Software* dedicato alla memorizzazione di grandi quantità di informazioni in formato elettronico.

<sup>14</sup> Componente di elaborazione e gestione del traffico di informazioni che fornisce servizi ad altre componenti che ne fanno richiesta, attraverso la rete; si tratta di un programma che fornisce i dati richiesti da altri elaboratori (*clients*), facendo quindi da *host* per la trasmissione delle informazioni virtuali.

<sup>15</sup> L’algoritmo calcola automaticamente e con cadenze regolari il numero di volte in cui il termine è stato inserito dagli utenti nella stringa di ricerca.

*l'originaria e immediata impressione negativa ingenerata dall'abbinamento di parole>>.*

Secondo il Tribunale di Milano poi, la condotta censurabile di Google risiede nella scelta di utilizzare il suo sistema di completamento automatico per facilitare le ricerche. La Corte ha osservato che <<*si tratta di una scelta che ha chiaramente valenza commerciale ben precisa, connessa con l'evidenziata agevolazione della ricerca*>>, come se i suggerimenti di ricerca siano un'opzione unica e distinta rispetto all'insieme di tutte le altre caratteristiche del motore di ricerca; opzione di cui, quindi, Google potrebbe anche fare a meno in quanto lo scopo di lucro della società è preponderante rispetto all'agevolazione offerta agli utenti e una modifica o soppressione della funzione *auto-complete* non comprimerebbe la libertà degli stessi di accedere alle ricerche offerte dal motore di ricerca. In realtà ci sono molte caratteristiche che, nel loro insieme, differenziano e migliorano un motore di ricerca rispetto ad un altro. Risultati non aggiornati o fuori-tema dovuti ad un problema di attualità o pertinenza sono sintomi di un motore che funziona in modo discreto e non ottimale. La ragione dell'esistenza dei motori di ricerca sta nell'assistere gli utenti nella ricerca e scoperta di informazioni nel vastissimo *world wide web* (www). Durante gli anni Google ha proposto sempre più servizi per promuovere la scoperta di informazioni sul *web*. Il completamento automatico, lanciato nel 2004, è solo uno degli strumenti realizzati da Google per agevolare il reperimento rapido ed efficiente delle informazioni. L'affermazione del Tribunale in base alla quale tale funzionalità risulti essere distinta ed opzionale e in grado di arricchire Google diversamente dagli altri strumenti di ricerca messi a punto dall'azienda, sembra non reggere. La Corte ha anche aggiunto che Google *suggest* perde la sua neutralità quando un algoritmo produce abbinamenti impropri di termini. Tuttavia questi abbinamenti sembrerebbero rappresentare quello che più di frequente gli utenti scrivono nelle loro ricerche relative, nel caso di specie, all'imprenditore. Se sono abbinamenti offensivi e inappropriati, ciò postula un problema di reputazione più ampio e solo minimamente accentuato dalla funzione *auto-complete* di Google. Detto in altre parole, ci sarà un motivo di fondo per cui le ricerche condotte dalla maggior parte dei navigatori nel *web* portino a tali associazioni improprie di parole. Nel caso in questione, qualora l'imprenditore abbia realmente assunto un comportamento discutibile, che molti sembrano sospettare sulla base delle loro ricerche, la decisione della Corte favorisce tale

condotta, ostacolando gli utenti nel loro processo di scoperta dell'informazione. La *mission* di un motore di ricerca è quella di facilitare l'accesso alle informazioni, ma la Corte attraverso questa pronuncia sembra impedire il suo richiamato obiettivo. Qui, come in altri casi che analizzeremo, il problema di fondo è un bilanciamento tra diritti della personalità, quali la reputazione e la libertà di informazione.

Nell'ordinanza del 23 marzo 2013, il Tribunale di Milano ha decisamente cambiato rotta. A depositare denuncia contro Google è stata questa volta il presidente di due associazioni *no profit*, dopo aver rivelato che il motore di ricerca collegava il proprio nome e quello delle sue fondazioni ai termini “truffa”, “truffatore”, “setta”, “plagio”.

Il Tribunale di Milano, questa volta, non ha accolto la richiesta e ha negato la responsabilità di Google. Ci troviamo davanti a due casi molto simili, ma con sentenze decisamente antitetiche. Non può affermarsi, secondo quanto avanzato invece dai ricorrenti, la qualità di Google di *content provider*, in quanto le funzioni *auto-complete* e ricerche correlate rappresentano funzionalità del motore di ricerca. Il giudice ha chiarito che: << *I termini visualizzati dagli utenti sulla stringa di ricerca attraverso la funzionalità Autocomplete, ovvero in fondo alla pagina di ricerca nella sezione Ricerche Correlate, non costituiscono un archivio, né sono strutturati, organizzati o influenzati da Google che, tramite un software automatico, si limita ad analizzarne la popolarità e a rilasciarli sulla base di un algoritmo (...) trattasi di servizi della cd. attività di caching svolta da Google al fine di facilitare, a loro richiesta, l'accesso ad altri destinatari di informazioni fornite da destinatari del servizio, senza che il prestatore del servizio, nella specie Google, sia responsabile del contenuto di tali informazioni a norma dell'art. 15 del d.lgs. 70/03*>>. Inoltre le associazioni di cui i ricorrenti si dolgono non costituiscono frasi di senso compiuto, né una manifestazione di pensiero da parte di Google, ma esclusivamente il risultato delle ricerche più popolari effettuate dagli utenti o la visualizzazione dei termini ricorrenti nelle pagine web incluse tra i risultati di ricerca di una data *query*. Sono dunque degli strumenti resi disponibili agli utenti come “aiuto” alla ricerca. Mentre nel 2011 il Tribunale riteneva che, sebbene il risultato dell'auto-completamento non dipenda direttamente da Google, la sua visualizzazione avviene in forza di un algoritmo creato dalla stessa azienda e ciò è

sufficiente ad addebitare la responsabilità all'azienda, nella più recente pronuncia, il Tribunale esclude tale responsabilità, sostenendo che:

*<<l'accostamento di termini in una stringa o un profilo di ricerca non costituisce un'affermazione bensì un suggerimento>>.*

### **3.2 L'ordinanza del Tribunale di Pinerolo**

L'ordinanza del Tribunale del Pinerolo del 2 maggio 2012 ha indicato un nuovo percorso nell'articolato scenario giuridico relativo alla responsabilità degli *hosting provider*. La vicenda riguarda un imprenditore piemontese il quale verifica che la funzione *auto-complete* suggerisce di associare alla sua identità i termini "arrestato" e "indagato". Data l'infondatezza e la mancata veridicità dei suggerimenti, l'imprenditore diffida Google a rimuovere tale associazione, ritenendola gravemente diffamatoria. Il ricorrente ritiene che l'associazione integri gli estremi del reato di diffamazione e che sussista in capo a Google una responsabilità omissiva colposa per aver creato il meccanismo automatico e, in ogni caso, per non aver accolto la diffida stragiudiziale.

Il Tribunale esclude il reato di diffamazione, in quanto ritiene che il servizio di completamento automatico offerto da Google funzioni in modo oggettivo e neutrale, sulla base dei contenuti immessi dagli utenti nel *box* delle ricerche. L'associazione di termini lamentata dal ricorrente non significa altro se non che un certo numero di utenti ha, in tempi recenti, interrogato il motore di ricerca per sapere se il soggetto fosse stato indagato oppure arrestato. Il ruolo della resistente è quello di ISP soggetto alla disciplina di cui al d.lgs. 70/03, con conseguente esclusione di responsabilità. Inoltre, nessuna responsabilità di carattere omissiva può riscontrarsi a suo carico, considerando che non esiste un obbligo generale di sorveglianza dell'ISP sulle informazioni trasmesse o memorizzate, così come non esiste un obbligo di rimozione a seguito di una richiesta stragiudiziale degli interessati, ma solo a seguito di un ordine dall'autorità giudiziaria o amministrativa di vigilanza. La Corte aggiunge che *<<la mera associazione dei termini in una stringa di ricerca non è un'affermazione, dovendo piuttosto essere paragonata ad una domanda>>*. La domanda se taluno sia indagato o arrestato non è di per sé lesiva della reputazione, ma può diventare tale solo se si tratta di una domanda retorica o



maliziosamente posta da chi sappia che la risposta sia negativa e voglia tuttavia insinuare che il soggetto sia implicato in fatti penalmente rilevanti. Il contesto in esame, però, esclude che si tratti di una domanda retorica o di una maliziosa insinuazione, anche perché persino gli utenti di Internet meno informati riescono a sciogliere facilmente ogni equivoco, verificando che le ricerche effettuate con quella combinazione di termini non producono alcun risultato<sup>16</sup>. È dunque escluso sotto il profilo oggettivo il reato di diffamazione e anche sotto il profilo soggettivo, in quanto non è possibile attribuire alcuna responsabilità agli utenti che abbiano digitato nelle loro ricerche su Google le parole in questione, accostandole al nome del ricorrente, non essendo forniti elementi dimostrativi che possano provare il loro comportamento doloso in grado di integrare il reato di diffamazione. Né, d'altro canto, si può individuare una responsabilità in capo all'ISP, avendo svolto un'attività di mera diffusione della notizia, ossia un'attività di hosting in riferimento alla quale il decreto di recepimento della direttiva sul commercio elettronico esclude ogni responsabilità, a meno che l'informazione trasmessa e ospitata sia illecita e il *provider* sia consapevole di tale illiceità.

## **4. L'orientamento di alcune Corti straniere**

### **4.1. Suggestioni e inserzioni nella giurisprudenza francese**

A partire dal 2008 Google offre anche in Francia la funzionalità *suggest*. Una delle prime pronunce della Corte d'appello di Parigi è quella riguardante la società *Lyonnaise de Garantie*<sup>17</sup>, al cui nome il servizio Google *suggest* associava la parola “*escroc*” (truffatore). La società attrice chiede la rimozione dell'associazione diffamatoria dalla pagina Google in Francia, Belgio, Regno Unito, Spagna, Italia e Canada; chiede, inoltre, il risarcimento dei danni subiti e la pubblicazione della sentenza

---

<sup>16</sup>Si noti che il Tribunale di Milano, nel 2011, non aveva accettato una simile argomentazione addotta in quel caso da Google nelle sue memorie difensive.

<sup>17</sup>Cour d'appel de Paris Pôle 2, chambre 7 Arrêt du 14 décembre 2011

sulla *homepage* di Google e su alcuni quotidiani nazionali francesi. Google eccepisce il funzionamento tecnico e automatico del sistema che, dunque, escluderebbe il dolo nella selezione dei termini da accostare alle parole ricercate, e solleva l'inapplicabilità della legge francese ad una società stabilita negli Stati Uniti. Tuttavia i giudici hanno ritenuto che la legge applicabile fosse quella francese, poiché gli effetti dell'azione dannosa si sono prodotti in Francia, ed hanno affermato che non possa essere invocato l'art.10 della Convenzione europea in materia di libertà di manifestazione del pensiero, poiché i commenti recanti accuse alla società attrice erano per lo più anonimi.<sup>18</sup> Inoltre non è possibile appellarsi alla natura automatica del servizio; infatti, considerando che il motore di ricerca può limitare l'accesso a pornografia ed espressioni razziali, è evidente che sia in grado di intervenire anche nei confronti di associazioni di parole diffamatorie o ingiuriose. Da ciò si evince <<la possibilité d'un contrôle humain sur la fonctionnalité>>. Le conclusioni della Corte che portano a rilevare la responsabilità del motore di ricerca si fondano essenzialmente sulla qualificazione del servizio Google *suggest* come un servizio editoriale, piuttosto che come servizio reso da un *provider* tramite la rete Internet. Tuttavia in questa decisione, come in un'altra riguardo un uomo accusato di corruzione minorile, l'orientamento successivo della giurisprudenza francese ha mutato opinione. Inizialmente in questi due casi la motivazione dei giudici di prima istanza è pressappoco la medesima: secondo i giudici francesi di *prima cure* la società che gestisce il motore di ricerca non è in grado di dimostrare che le parole suggerite rappresentino l'esito di un mero calcolo statistico basato su precedenti ricerche effettuate con gli stessi termini, pertanto il *provider* ne è responsabile. Successivamente, al contrario, la *Cour de Cassation* non ha accolto l'accusa mossa nei confronti di Google, ritenendo che le combinazioni di parole generate dalla funzione *auto-complete* non costituiscano un'espressione di pensiero o un ragionamento, ma metodi tecnici per facilitare la ricerca. Ciò significa che tali combinazioni di parole sono prive di alcun significato e non implicano l'intenzione del motore di ricerca di unire una parola all'altra; di conseguenza nessuna accusa di diffamazione può essere mossa nei confronti della società convenuta. Nel caso "*Lyonnaise de garantie*", la *Cassation* ha concluso che l'automatica e istantanea comparsa di parole chiavi nella stringa di ricerca

---

<sup>18</sup><<Figurent parmi les textes des commentaires émanant d'internautes qui mettent de manière anonyme en cause la société Lyonnaise de Gestion sans justificatif ou pièce démonstrative de leurs points de vue>>.

è priva di ogni significato intrinseco e costituisce un mero strumento di ricerca per gli utenti di internet. Alle stesse conclusioni la *Cassation* è giunta con riferimento all'altro caso su menzionato. Questa volta il ricorrente è un soggetto privato accusato di essere coinvolto in una vicenda di corruzione di un minore. Nel digitare il suo nome nella stringa di ricerca di Google, la funzione di completamente automatico suggeriva parole come “*viol*” (violenza), “*condamné*” (condannato) e “*sataniste*” (satanista). L'uomo ingiunge Google a rimuovere tali suggerimenti diffamatori e il suo reclamo, accolto in primo grado, è rigettato in appello. La *Cour de Cassation* conferma la decisione della Corte d'Appello, ritenendo che l'elemento soggettivo del reato di diffamazione debba essere collegato alla “funzionalità” dei suggerimenti automatici. Infatti, sebbene le espressioni denunciate dal ricorrente siano diffamatorie in senso letterale, al fine di associare ad esse l'elemento dell'intenzionalità, occorre considerare la loro funzionalità, ossia quella di facilitare l'accesso ai siti. In altre parole, bisogna considerare contesto e funzionalità dell'accostamento dei termini e non soffermarsi solo al significato letterale. La Corte, infatti, descrive una precisa distinzione tra “senso letterale” e “funzionalità” di uno strumento il cui solo proposito è quello di facilitare la ricerca e l'accesso ai siti web. Con riferimento a questo tipo di funzionalità, infatti, il significato delle associazioni di termini può essere rilevato solo dopo che la ricerca è stata effettuata e non nel momento precedente, ossia quello in cui l'utente inizia la sua ricerca ed è posto innanzi ad eventuali suggerimenti automatici proposti dal motore di ricerca (Stavroula - Borghi 2015). Di conseguenza nessuna violazione di diritti della personalità può essere addebitata ad un servizio che prevede questa funzionalità. Non c'è dunque nessuna aspettativa di credibilità dei suggerimenti che il motore di ricerca possa ingenerare negli utenti. Una simile aspettativa invece sarà l'elemento alla base delle argomentazioni a sostegno della valenza diffamatoria dei suggerimenti di ricerca, su cui si fonderà, come vedremo in seguito, la corte tedesca.<sup>19</sup>

In una meno recente sentenza del Tribunale de Commerce di Parigi, risalente al 7 maggio 2009, la società “*Direct Energie*” lamentava l'associazione del suo nome con il termine “*arnaque*” (truffa). La Corte accoglieva la richiesta della società attrice e ordinava alla convenuta di rimuovere la parola offensiva dai suggerimenti di ricerca collegati alla società *Direct Energie*. Le argomentazioni che Google ha addotto in sua

---

<sup>19</sup>Cfr. cap. I, par. 4.3

difesa non ci sono del tutto nuove: Google *suggest* è una funzione del motore di ricerca statistica, automatica e oggettiva, di conseguenza l'azienda non può essere considerata responsabile, poiché non c'è un suo intervento diretto sulla schermata dei suggerimenti. In più, Google sollevava ragioni difensive basate sulla libertà di parola e di espressione e sul diritto di informazione: i risultati suggeriti dalla funzione auto-complete sono ritenuti legittimi e utili per l'intera *community* degli utenti di Internet ed essi riflettono in modo oggettivo le ricerche più frequenti degli utenti del *web*. La giurisprudenza francese in più casi non ha condiviso le argomentazioni difensive di Google basate sulla libertà di espressione di cui all'art. 10<sup>20</sup> della Convenzione europea dei diritti dell'uomo e delle libertà fondamentali, ritenendo che la libertà di espressione sia un diritto esclusivo della persona e, in ragione di ciò, non può essere invocata per proteggere una funzione automatica applicata ad un motore di ricerca. Tuttavia, il fatto che la legge applicabile alle sole persone non possa essere applicata ai contenuti generati da una macchina, non lascia esenti da responsabilità civile i proprietari di tale macchina. La lettura della Corte sembra da questo punto di vista abbastanza superficiale, in quanto non ha considerato il diritto di ricevere informazioni come costitutivo della libertà di espressione, oltre al diritto di diffondere informazioni. Una diversa ed opposta concezione di libertà di espressione del pensiero intesa sia come diritto di informare che diritto ad essere informati è quella statunitense, come vedremo in seguito.<sup>21</sup>

## 4.2. Il giudice di Milano e il giudice di Parigi: un confronto

Dopo aver analizzato posizioni della giurisprudenza sia italiana che francese discordanti tra loro in merito alla responsabilità del motore di ricerca, passiamo a comparare la *ratio* alla base di due sentenze che sono giunte alla stessa soluzione, ma attraverso un percorso motivazionale evidentemente divergente. Si tratta di due casi precedentemente analizzati, l'ordinanza del Tribunale di Milano del 2011 e la decisione della Corte d'Appello di Parigi del dicembre dello stesso anno. Entrambi i casi hanno ad oggetto il funzionamento del servizio Google *suggest*, in entrambi i casi il collegio giudicante

---

<sup>20</sup>L'incipit dell'art. 10 recita infatti: <<Toute personne a droit à la liberté d'expression>>.

<sup>21</sup>Cfr. cap. 1, par. 6

conclude con la responsabilità di Google per diffamazione. Inoltre, entrambi i giudici convergono sull'applicazione della legge del luogo in cui si è prodotta l'offesa, rispettivamente quella italiana e quella francese. La differenza sostanziale tra le due pronunce riguarda il campo di gioco entro cui accertare le eventuali responsabilità del servizio offerto da Google (Pollicino Oreste). Il Tribunale di Milano considera la Direttiva europea sul commercio elettronico e il d.lgs. 70/03 di recepimento della stessa e giunge alla conclusione di dover escludere il beneficio dell'esonero di responsabilità in capo a Google, in quanto il decreto sopra citato riguarda esclusivamente i prestatori di servizi che pongono in essere un'attività meramente tecnica, automatica e passiva. La modalità operativa del servizio Google *suggest*, invece, secondo il parere del Tribunale, non rende tale servizio neutro e passivo, per cui le conseguenze negative del servizio in questione non possono che essere addebitate alla società che lo fornisce. Abbiamo già discusso abbastanza riguardo i pro e i contro di questa decisione che lascia spazio a perplessità e interrogativi, tuttavia dubbi mai tanto grandi quanto quelli che emergono dinanzi alla decisione del giudice francese. L'iter argomentativo e motivazionale della Corte d'Appello francese, a differenza di quello italiano, non prevede riferimenti né alla Direttiva europea, né alla normativa francese di recepimento, né tantomeno all'eventuale, per quanto astratta, differenza tra ISP attivo e passivo. Fortunatamente, poi, il giudice di Milano aveva quantomeno confermato l'inesistenza di un obbligo di sorveglianza preventivo in capo al service provider; al contrario, il giudice francese non fa nessun riferimento all'inesigibilità di un controllo *ex ante*. Egli, in sostanza, costruisce tutta la sua motivazione su un assunto di base alquanto poco condivisibile, ossia l'equiparazione del servizio Google *suggest* ad un servizio editoriale.<sup>22</sup> Si tratta di un'affermazione non condivisibile alla luce del nuovo orientamento della nostra Corte di Cassazione che ha affermato l'inapplicabilità delle disposizioni ex art. 57 c.p. al direttore di un giornale web per i commenti dei lettori presenti nella propria piattaforma, pur trattandosi, anche in questo caso, di attività editoriale, sebbene svolta sulla rete. La giurisprudenza francese, invece, ha applicato la disciplina prevista per la stampa ai

---

<sup>22</sup> La giurisprudenza inglese ha ritenuto che per la qualifica di "editore" debbano ricorrere due condizioni: 1) che il soggetto abbia un'intenzione alla pubblicazione dei contenuti e non rivesta meramente il ruolo di intermediario passivo; 2) che il soggetto abbia l'attuale ed effettiva conoscenza del contenuto della pubblicazione, ossia, in caso di diffamazione, conosca o avrebbe potuto conoscere, utilizzando la ragionevole diligenza, il potenziale contenuto diffamatorio della pubblicazione (*McLeod v St. Aubyn* [1899] AC 549).

servizi forniti da un ISP, il quale non ha nessun obbligo di sorveglianza. L'orientamento così fuorviante del giudice di Parigi potrebbe comprendersi ed essere almeno minimamente giustificato dal tentativo di far emergere la prevalenza di diritti della personalità costituzionalmente tutelati e la libertà di espressione ex art. 10 della Convenzione Europea dei Diritti dell'Uomo; infatti in un passaggio della pronuncia, il giudice afferma che non qualsiasi espressione del pensiero ricade sotto la tutela dell'art.10 e nel caso di specie non vi ricadranno i messaggi offensivi anonimi e ingiustificati. Molte volte però può capitare che, al fine di tutelare in maniera effettiva i diritti fondamentali dell'uomo, si rischia di fare un uso eccessivo dello strumento della censura, che pure lede una libertà costituzionalmente tutelata. Anche in questo caso il problema che si pone è un'esigenza di bilanciamento tra interessi in gioco meritevoli, almeno in teoria, di uguale protezione. In questo caso, è giusto ritenere che una modifica della funzione auto-complete di Google non comprimerebbe la libertà degli utenti di accedere alle ricerche offerte da motore di ricerca, tuttavia è pur vero che l'eliminazione del servizio renderebbe meno efficace ed immediato lo svolgimento di ricerche sul *web*. Dunque, l'esigenza di protezione di beni meritevoli di tutela, quali la reputazione, l'onore, l'identità, il diritto all'oblio o la proprietà intellettuale, non può ingenerare il rischio di subordinare eccessivamente la libertà di espressione a tali diritti fondamentali della persona umana. Inoltre c'è da dire, che nel bilanciamento tra valori contrapposti e meritevoli di tutela, non c'è solo la tanto celebrata libertà di espressione, ma entra in scena un'altra libertà, sempre costituzionalmente tutelata, di non poco conto, ossia la libertà di iniziativa economica e d'impresa. Non si può negare che tali pronunce contro Google, comportano una compressione dei servizi che la stessa offre e della libertà di agire e di gestire la sua attività di business che si svolge interamente sul *web*; il suo *business model* non può essere compromesso solo perché i suoi vettori portanti sono il *cyber-spazio*, gli utenti del *web* e le informazioni, i dati e i servizi connessi al *web*.

### 4.3. Le vicende di Google in Germania

Anche la giurisprudenza tedesca ha mutato spesso parere riguardo Google e la sua innocenza o colpevolezza. Partendo dalla decisione del 2013 della Suprema Corte Federale tedesca<sup>23</sup>, si nota che il cuore della decisione si basa sulla convinzione che la responsabilità di Google per diffamazione derivi dalla suggestione negativa che eventuali associazioni di parole diffamatorie possano ingenerare negli utenti del *web* che ne prendano visione. Nel caso di specie, il ricorrente, proprietario di una società di cosmetici registrata a suo nome, scopre che il proprio nome è associato con i termini “frode” e “*scientology*”. La Corte tedesca accoglie il reclamo e considera Google responsabile per non aver rimosso le false associazioni non appena ricevuta la notifica dal ricorrente. Secondo la Corte, infatti, la funzione *auto-complete* crea un’aspettativa nei confronti degli utilizzatori di Internet, in quanto le associazioni di parole hanno un significato informativo; indipendentemente dal fatto che ci siano o meno dei risultati di ricerca che confermino l’associazione, gli utenti di Internet saranno portati a ritenere che le associazioni sono informate a contenuti reali indicizzati da Google, saranno cioè letteralmente “suggestionati” e condizionati da tali suggerimenti di ricerca. Sulla base di questa argomentazione, la Suprema Corte tedesca ritiene che le previsioni generate dall’algoritmo siano informazioni personali dell’ISP e non informazioni acquisite dai beneficiari del servizio e ad essi riconducibili. Inoltre, secondo la Corte tedesca, Google ha l’onere di reagire e attivarsi non appena apprenda di star fornendo informazioni in conflitto con i diritti della personalità. Tuttavia è specificato che il motore di ricerca non ha un obbligo generale di attivarsi in caso di violazioni commesse dall’algoritmo, ma il dovere sussiste quando ne sia venuto a conoscenza, anche tramite una comunicazione del diretto interessato. È bene precisare che il caso appena descritto, oggetto di revisione dalla Corte Suprema, era stato esaminato in modo differente dalla Corte Regionale di Cologne<sup>24</sup>, la quale aveva stabilito che i suggerimenti forniti dalla funzione *auto-complete* non costituivano un’affermazione piena da parte del motore di ricerca e quindi aveva negato la violazione di diritti della personalità e la responsabilità del *provider*, rigettando il reclamo. La decisione della Suprema Corte ovviamente ha sancito

---

<sup>23</sup>BGH Case VI ZR 269/12, del maggio 2013

<sup>24</sup>Oberlandesgericht Köln, 15 U 199/11, del 10 maggio 2012

l'orientamento dominante in materia, tuttavia la sentenza della Corte di Cologne si è mostrata in linea con le decisioni di altre corti tedesche, prima fra tutte quella concernente il famoso caso di Bettina Wulff, la *first lady*, moglie dell'allora presidente tedesco. Digitando il nome della signora Wulff, i principali suggerimenti di ricerca sono "Bettina Wulff *escort*" o l'equivalente tedesco di prostituta. Alcuni *rumors* sul presunto passato della *first lady* giravano discretamente all'interno della *élite* politica, ma secondo la donna, i suggerimenti automatici diffamatori del motore di ricerca ne avevano ampliato la diffusione. Per tale motivo agisce per vie legali ritenendo che il motore di ricerca abbia perpetrato le voci negative sul suo conto e i danni alla sua reputazione e alla sua immagine, ad ogni modo eccessivi e non compatibili neppure con la sua condizione di personaggio pubblico. Google si difende sostenendo che non è il motore di ricerca a suggerire i termini in modo diretto, ma questi sono il risultato di ricerche precedentemente effettuate dagli utenti con una certa frequenza; quindi le espressioni più comunemente ricercate diventano le "*top suggestions*". È certamente noto che Google ha steso una sorta di "*black-list*" contenente alcuni termini in riferimento ai quali la funzione di completamento automatico non opera (pornografia, violenza, odio razziale, condivisione di file illegali) ed esiste anche una lista specifica per ogni Paese che impone a Google di rimuovere i riferimenti a termini che sono considerati "fuori-legge" in quel determinato Paese (ad esempio in Germania si parla di divieto di negazionismo<sup>25</sup> in merito all'Olocausto); tuttavia Google precisa che il suo algoritmo non può applicare questo controllo al di fuori di tali aree determinate. Secondo questa linea di pensiero, dunque, il motore di ricerca non può essere considerato responsabile. La Corte è del parere che, fin quando i termini suggeriti non sono contemplati nel loro contesto globale, ad esempio insieme agli effettivi risultati di ricerca, questi non posseggono un significato specifico facilmente apprezzabile dagli utenti e, quindi, nessun diritto della personalità appare violato. Di conseguenza, solo il contenuto specifico dei risultati di ricerca attribuisce ai suggerimenti di ricerca un possibile significato diffamatorio; diversamente, quando tali suggerimenti operano in un contesto differente, costituito da una connessione anticipata tra soli termini, non

---

<sup>25</sup> Fenomeno culturale, politico e giuridico che si manifesta in comportamenti e discorsi che hanno in comune la negazione della verità di fatti storici percepiti dai più come massima ingiustizia e pertanto oggetto di processi di elaborazione scientifica e/o giudiziaria di responsabilità.  
Cfr. Luther, Joerg <<L'antinegazionismo nell'esperienza giuridica tedesca e comparata>>



collegati a nessun reale risultato di ricerca, essi assumono un significato irrilevante e non determinano alcuna responsabilità in capo al *provider*. In un simile contesto operano le associazioni di termini del caso di specie, per cui il reclamo della signora Wulff è stato rigettato dalla Corte.

#### **4.4. L'algoritmo di Google sotto accusa in tutto il mondo: dall'Australia all'Asia.**

Un semplice algoritmo sta costando a Google migliaia di dollari per adempiere ai risarcimenti dei danni per diffamazione.

In Australia il motore di ricerca è condannato a risarcire un soggetto ritenutosi diffamato dal servizio Google *suggest*. In particolare il ricorrente lamenta il fatto che svolgendo una ricerca su Google il proprio nome sia associato a foto di persone legate al crimine. Il tribunale ha ritenuto l'associazione diffamatoria perché inesatta ed ha accolto il ricorso. Si precisa che il ricorrente ha preliminarmente avvisato Google dell'associazione diffamatoria, richiedendone la rimozione, ma la società è rimasta indifferente dinanzi al reclamo. Questa particolare circostanza ha giustificato la condanna risarcitoria. Il tribunale, infatti, non ha condannato l'algoritmo in sé, attribuendo con ciò una responsabilità oggettiva al motore di ricerca, ma piuttosto è stata incriminata la condotta omissiva della società, ossia il non essersi attivata per eliminare l'associazione impropria, sebbene segnalata dall'interessato. Nei tribunali di tutto il mondo, si va delineando una figura di responsabilità autonoma per gli intermediari di servizi sulla rete. Si esclude invece una responsabilità oggettiva, ossia addebitata in assenza di dolo o colpa, considerata inappropriata per la natura degli intermediari a causa dell'enorme mole di dati gestiti e a causa dell'impossibilità di un meccanismo di controllo su questi allo stato attuale della tecnica. Si cerca, dunque, di inquadrare la questione nell'ambito della responsabilità omissiva, ossia quella conseguente alla mancata pronta attivazione a rimuovere l'illecito, una volta ricevuta la segnalazione dall'interessato.<sup>26</sup>

---

<sup>26</sup> Si consideri che l'orientamento italiano propende per una richiesta proveniente dalle autorità competenti e non dal soggetto leso.

Spostandoci nel continente europeo, è doveroso accennare al curioso caso di un hotel irlandese, che ha visto comparire sul motore di ricerca, accanto al proprio brand, la parole “*receivership*” (fallimento) e che è stato tempestato dalle telefonate dei clienti preoccupati di non aver più modo di soggiornare nelle costose *suite* prenotate con largo anticipo. Il servizio Google *suggest* ha causato all’hotel in questione, oltre ai danni di reputazione, anche danni economici, in quanto molti clienti che avevano programmato cerimonie in anticipo non erano più disposti a pagare il deposito, credendo che l’hotel stesse per fallire. L’azienda ha quindi fatto causa a Google, ma quest’ultima si è limitata a discolarsi dichiarando che la finalità della funzione *auto-complete* è quella di facilitare gli utenti nella ricerca e precisando che non è il motore di ricerca a selezionare manualmente i termini, ma si tratta di chiavi di ricerca digitate in precedenza da un alto numero di utenti. Tuttavia Google, soccombente, è stata costretta, anche in questo caso, ad intervenire per modificare manualmente i risultati previsti dalla funzione di completamento automatico.

Nel Regno Unito, la vicenda oggetto d’esame, non riguarda propriamente i suggerimenti di ricerca forniti da Google, bensì la visualizzazione di *snippets*<sup>27</sup> offensivi associati alla ricerca del *Metropolitan International Schools Limited*. La *High Court Queen’s Bench Division* qualifica in modo alternativo l’attività svolta dal motore di ricerca. Ritiene, infatti, che un motore di ricerca non è propriamente un *hosting*, ma un diverso tipo di intermediario che svolge una mera attività di facilitatore, in quanto l’indicizzazione dei risultati non presuppone alcun intervento umano, poiché si realizza tramite l’agire degli *spider*. Google, dunque, non opera certamente come un editore, non avendo nessun controllo sui termini di ricerca inseriti dagli utenti e non potendo operare una scelta sui contenuti forniti dalla rete.

Focalizziamo ora l’attenzione sul Sud America, il cui orientamento si avvicina maggiormente al pensiero europeo, anziché a quello statunitense. In Argentina una comunità ebraica ha ottenuto un’ingiunzione che ha imposto a Google l’indicizzazione di alcuni siti ritenuti antisemiti e il blocco della funzione *suggest* di alcuni termini considerati discriminatori. Alla ricerca del termine *judío* era associato il suggerimento “*avaro*”, “*tacaño*”, “*usurero*”, e alla ricerca del termine *holocausto* veniva suggerito il

---

<sup>27</sup> Estratti di testo visualizzati sotto il titolo di una pagina nei risultati di ricerca, che descrivono sommariamente i contenuti della pagina.

termine “*mentira*”, ossia menzogna. Restando in tema di rapporto tra Google e le religioni, alcuni si sono divertiti a verificare un caso interessante: digitando nella stringa di ricerca di Google “*Christianity is*” la funzione *suggest* suggerisce “*Christianity is not a religion*” e “*Christianity is a lie*” ed altre espressioni simili. Lo stesso accade per altre tra le maggiori religioni nel mondo (“*Hinduism is false*”, “*Protestantism is heresy* etc.) eccetto l’Islam, a cui sono associate espressioni positive, come “*Islam is a religion of peace*”. Google si giustifica dicendo che la differenza non è intenzionale, ma il risultato di un errore informatico. Alcune riviste, invece, suggeriscono che “qualcuno” abbia indotto Google a rimuovere i termini offensivi. Entrambe le ipotesi sembrano plausibili, meno lo è la teoria secondo cui Google avrebbe timore di offendere i musulmani. Non è una novità assoluta per Google censurare parte dei contenuti del suo archivio; si pensi che ha già dovuto rimuovere alcuni siti che criticavano l’Islam da *Google News* sul presupposto che non si trattavano di siti di informazione. Tuttavia è sufficiente svolgere alcune ricerche per scagionare Google da ogni accusa cospiratoria: se digitiamo “*Islam will*” o “*Islam must*”, Google ci suggerisce “*be destroyed*” ed altre espressioni simili, con una valenza non proprio positiva. Dunque sembrerebbe che chiunque stia provando ad eliminare i termini di ricerca che potrebbero offendere i musulmani, non stia facendo un buon lavoro (Richmond 2010).

Tornando ad indagare sulla responsabilità di Google per diffamazione, ci spostiamo adesso all’estremo opposto dell’emisfero. Ad Hong Kong un ricco cittadino accusa Google di diffamazione perché ricercando il suo nome, Albert Yeung Sau-shing, Google *suggest* suggeriva il termine “*triad*”, una nota organizzazione criminale di Hong Kong. *L’High Court of Hong Kong* ha disatteso la difesa di Google basata sulla presunta non responsabilità del motore di ricerca per i suggerimenti *auto-complete* e sul fatto che la corte in questione non abbia giurisdizione sulla materia; di conseguenza Big G. è per l’ennesima volta costretta a risarcire i danni e a rimuovere i suggerimenti di ricerca diffamatori.

Da questa rapida panoramica si deduce che le accuse di diffamazione mosse contro il gigante del web sono molteplici. C’è chi lamenta una mancanza di controllo da parte di Google sull’ottimizzazione delle SERP<sup>28</sup> che non combacia con la *mission* dichiarata

---

<sup>28</sup> “*Search engine results page*” ( Pagina dei risultati del motore di ricerca)

dall'azienda, ossia offrire ricerche veritiere, precise ed attendibili. Molti esperti SEO<sup>29</sup> hanno messo in guardia le aziende, suggerendo loro di controllare con cadenza regolare il proprio brand nei risultati di ricerca di Google, al fine di assicurarsi che non vi siano associazioni con termini negativi o di comparire in posizioni troppo basse nei risultati di ricerca. Tuttavia è opportuno precisare che non sempre i fatti di diffamazione che interessano Google sono realmente non veritieri e inesistenti; anzi molto spesso le ricerche effettuate dagli utenti non costituiscono semplici curiosità, ma hanno un fondamento di verità. Chi ritiene Google responsabile è inoltre convinto che nel procedimento di auto-completamento sia coinvolto qualche elemento umano, considerando che i risultati cambiano a seconda della posizione geografica e di altre circostanze. Tuttavia Google continua a difendersi adducendo che la funzione auto-complete offre risultati basati su quello che la gente cerca e che raccoglie dati in modo automatico. Ma è chiaro che solo Google conosce come opera realmente la sua funzione e fino a quando non si comprendono i meccanismi tecnici che la caratterizzano non si può presumere di attribuire all'operato di una funzione matematica rilevanza legale.

## **5. Responsabilità per violazione dei diritti di proprietà intellettuale.**

I servizi innovativi proposti dal gigante Google sono spesso accusati di violare non solo i diritti della personalità, ma anche i diritti di proprietà intellettuale. Nel 2010 il *Syndicat National de l'Edition Phonographique (SNEP)*<sup>30</sup> dà inizio ad un procedimento contro Google, in quanto i suggerimenti di ricerca indirizzavano gli utenti verso siti *torrent* (“*Torrent*”, “*Megaupload*”, o “*Rapidshare*”) quando questi digitavano il nome di artisti o gruppi musicali nella barra di ricerca di Google. Sia la Corte di prima Istanza che la Corte d'Appello hanno ritenuto che tali associazioni di parole automatiche non rendessero Google responsabile per attività poste in essere dagli utenti di Internet; così non hanno accolto il reclamo di SNEP volto a far censurare tali induzioni alla pirateria,

---

<sup>29</sup> “*Search Engine Optimization*” (ottimizzazione: nel linguaggio di internet si intendono tutte quelle attività volte ad ottenere la migliore rilevazione, analisi e lettura del sito web da parte dei motori di ricerca attraverso i loro spider al fine di migliorare o mantenere un elevato posizionamento nelle pagine di risposta alle interrogazioni degli utenti del web.

<sup>30</sup> Principale organizzazione francese che protegge l'industria musicale francese.

accentuate dalla funzione auto-complete. Entrambi i collegi giudicanti hanno ritenuto che i siti su menzionati non fossero illegali di per sé, sebbene potrebbero essere utilizzati per violare il *copyright*, qualora si scaricassero ad esempio canzoni illegalmente e senza il consenso dei diretti interessati. Sulla questione si è pronunciata la *Cour de Cassation*, la quale ha ritenuto che la funzione di completamento automatico di Google, allo stato dei fatti, orienta sistematicamente gli utenti del web verso siti illegali e la soppressione di suggerimenti di questo tipo renderebbe la ricerca di tali siti più difficile. L'algoritmo che genera i suggerimenti ha la potenzialità di indirizzare gli utenti verso ricerche particolari ed ha anche la capacità di indurli verso comportamenti illeciti. Sebbene non totalmente effettive, le misure richieste da SNEP, ossia l'ordine di rimozione di tali termini dalla funzione *auto-complete*, sono in grado di prevenire o eliminare tali violazioni, senza compromettere l'efficienza del motore di ricerca. La Corte di Cassazione francese, in conclusione, ha ritenuto che, laddove le associazioni di parole automatiche orientino i navigatori verso siti che potrebbero indurre ad infrangere le leggi sul *copyright* o potrebbero suscitare altri comportamenti illeciti, il motore di ricerca sarebbe da ritenersi responsabile.

Confrontando la vicenda Google con quella che ha interessato una nota azienda di commercio elettronico, troviamo che le associazioni di parole non solo causerebbero comportamenti illeciti, ma esse stesse rappresenterebbero una violazione del diritto di proprietà intellettuale. La questione è stata discussa nel Regno Unito e il caso riguarda il proprietario del marchio "LUSH", produttore di cosmetici, il quale accusa Amazon di utilizzare il proprio marchio per indirizzare i consumatori verso prodotti concorrenti: appena il consumatore inizia la sua ricerca digitando il termine "lush" nella barra di ricerca di Amazon, compare un menù di suggerimenti di vari prodotti simili o equivalenti, in altre parole, concorrenti con quelli venduti dall'azienda ricorrente. Per il giudice si tratta di utilizzo illecito del marchio del ricorrente che colpisce il corretto funzionamento del mercato, avendo la potenzialità di confondere il consumatore medio. In questi due casi, i suggerimenti di ricerca non sono considerati nel loro significato meramente linguistico e letterale come nelle vicende che coinvolgevano i diritti della personalità. Le vicende sulla proprietà intellettuale ci insegnano che, anche quando le associazioni di parole conservano il loro carattere strumentale di facilitatore di ricerca, potrebbero assumere rilevanza legale quando, nei casi di specie, esse facilitano il

ritrovamento di informazioni che, diversamente, rimarrebbero oscure, o potrebbero confondere i consumatori. In questo caso, la “mera” facilitazione, argomento di difesa che aveva in altri casi indotto le corti a discolpare il motore di ricerca, produrrebbe l’effetto contrario, configurando una responsabilità solidale per violazione delle leggi sul *copyright* e sul mercato.

## 6. Europa vs USA: diritti della personalità vs libertà di espressione

### 6.1. Google *suggest* sotto la protezione del Primo emendamento

Negli USA il caso Google *suggest* è trattato da un punto di vista completamente differente. I suggerimenti di ricerca sono considerati opinioni costituzionalmente protette dal principio di libertà di parola e opinione (*freedom of speech*), ossia dal Primo emendamento<sup>31</sup>. Negli Stati Uniti, le opinioni che si presentano come “dichiarazioni su questioni di interesse pubblico”<sup>32</sup> sono protette sia nel caso in cui riguardino un personaggio pubblico che nel caso in cui si riferiscano ad un soggetto privato, sebbene in quest’ultima circostanza lo scudo costituzionale sia più vulnerabile. Nello specifico, devono ricorrere tre condizioni affinché una dichiarazione possa ricevere tutela costituzionale: (i) deve trattarsi di una manifestazione di pensiero/opinione; (ii) deve riguardare una questione di interesse pubblico; (iii) non deve essere manifestamente falsa. Le Corti statunitensi hanno gradualmente espanso la nozione di “manifestazione di pensiero” fino a comprendere qualsiasi rappresentazione di informazioni o di fatti, anche resa tramite fonti elettroniche. Conformemente a tale linea di pensiero, la giurisprudenza statunitense sostiene che le decisioni basate su un algoritmo, e più in generale i risultati di un procedimento interamente automatico, sono tutelati dal Primo emendamento, fintanto che l’algoritmo o il processo automatico interagiscano e

---

<sup>31</sup> Primo emendamento della Costituzione degli Stati Uniti d’America: « *Il Congresso non promulgherà leggi per il riconoscimento ufficiale di una religione, o che ne proibiscano la libera professione, o che limitino la libertà di parola, o di stampa; o il diritto delle persone di riunirsi pacificamente in assemblea, e di fare petizioni al governo per la riparazione dei torti.* »

<sup>32</sup> <<Statements on matters of public concern>>.

comunicano un messaggio ad un pubblico. La tesi in base alla quale i risultati di ricerca sono opinioni protette dalla Costituzione statunitense è stata inizialmente utilizzata come argomento di difesa dalle accuse rivolte a Google, riguardanti pratiche scorrette o comportamenti anticoncorrenziali, quali appunto l'esclusione dei siti dai risultati di ricerca o un'indicizzazione degli stessi a sfavore dei concorrenti. In un Libro Bianco<sup>33</sup>, commissionato da Google nel 2012, è stato sostenuto che il motore di ricerca opera nello stesso modo delle imprese di *mass-media*, le quali hanno il diritto di effettuare una legittima valutazione editoriale su ciò che gli utenti trovano interessante e prezioso. Una tale valutazione comprende la decisione circa quali informazioni includere e quali escludere dai risultati di ricerca e quali siano i risultati da rendere prioritari. Dal loro punto di vista, il fatto che le scelte siano implementate da un algoritmo, non riduce la protezione offerta dal Primo emendamento, in quanto l'algoritmo stesso è elaborato da una persona umana e quindi racchiude in sé una valutazione editoriale umana<sup>34</sup>. Anche se gli utenti si aspetterebbero che Google presentasse i risultati di ricerca sulla base di un algoritmo neutrale, l'azienda non ha mai rinunciato al suo diritto di selezionare quali informazioni presentare e come presentarle.

Quest'approccio è stato adottato anche dalle decisioni delle corti, in riferimento ai reclami circa la rimozione o la de-indicizzazione di alcuni siti dai risultati di ricerca.

Nel caso *Search King*<sup>35</sup>, la richiesta riguarda la pregiudizievole e intenzionale de-indicizzazione di alcuni siti dai risultati di ricerca di Google. Il ricorrente stava guadagnando dalla vendita di spazi pubblicitari su siti altamente indicizzati da Google, il quale ha, per ciò stesso, ammesso l'intenzionale declassamento di tali siti tra i risultati di ricerca più bassi, in quanto le azioni del ricorrente minacciavano l'integrità del sistema. La corte ha accolto la difesa di Google, in base alla quale il sistema rappresenta una manifestazione di opinione protetta dal Primo emendamento, ed ogni azione

---

<sup>33</sup> White Paper: Eugene Volokh and Donald M Falk, <<*First Amendment Protection for Search Engine Results*>>, 20 April 2012.

<sup>34</sup> Si noti come l'intervento umano e, connesso ad esso, l'equiparazione del motore di ricerca ad un editore sono negli USA utilizzati come argomenti di difesa, utili a far valere la copertura costituzionale dettata dal Primo emendamento. In Europa invece le corti hanno spesso utilizzato l'intervento umano e la presunta attività editoriale del motore di ricerca come elemento di accusa volto a sostenere l'addebito di responsabilità nei confronti di Google.

<sup>35</sup> *Search King, Inc. v Google Technology, Inc.*, Inc No 02-1457, 2003 (WD Oklahoma, 27 May 2003).

finalizzata in modo cosciente ed intenzionale a modificare l'indicizzazione dei siti è legittima espressione della libertà di opinione. La stessa questione si è presentata in un altro caso che aveva coinvolto più aziende del mondo delle comunicazioni elettroniche<sup>36</sup>. La causa riguarda due siti di cui, uno esponeva reati di frode perpetrati da vari ufficiali del North Carolina e l'altro descriveva atrocità commesse dal governo cinese. La corte non ha accolto il reclamo, ritenendo che i convenuti avessero legittimamente preso una "decisione editoriale", esercitando, di conseguenza, il diritto costituzionalmente tutelato di scegliere quali informazioni mostrare tra i risultati di ricerca e quali escludere. Secondo la giurisprudenza nordamericana, quindi, attraverso i risultati di ricerca, il motore esprime una propria opinione in merito alla quale informazione possa rivelarsi rilevante per gli utenti durante una specifica ricerca sul *web*; allo stesso modo, la funzione *auto-complete* esprime un'ulteriore opinione del motore di ricerca in merito a cosa valga la pena ricercare nel corso di una ricerca, a partire da specifiche parole-chiave. Si tratta in entrambi i casi di atti di libertà di espressione, entrambi costituzionalmente rilevanti. Tuttavia, secondo alcuni, una prima criticità può riguardare il fatto che potrebbe risultare problematico qualificare l'indicizzazione dei risultati di ricerca o i suggerimenti automatici di ricerca come una "manifestazione di pensiero". Sebbene l'orientamento giurisprudenziale abbia esteso la nozione di "*speech*", includendovi anche comunicazioni non verbali, come il linguaggio simbolico o il linguaggio commerciale, la qualificazione dei risultati di un puro algoritmo come "opinioni" resta problematica. In secondo luogo, l'analogia tra il motore di ricerca e un *media publisher* non sembrerebbe a molti del tutto appropriata. Ciò che caratterizza una rivista o un'emittente radiotelevisiva non è tanto il godere della libertà di selezionare cosa pubblicare e come pubblicarlo, ma soprattutto l'approvare le informazioni rese note al pubblico. L'editore "fa proprie" le informazioni che rende pubbliche, assunto non valido per quanto riguarda i motori di ricerca. Non c'è un lavoro di controllo e approvazione da parte di Google sulle informazioni contenute nei *website*, lo stesso vale anche con riferimento ai suggerimenti di ricerca. È interessante notare che in Europa, alcune corti, hanno rigettato i reclami contro Google proprio perché le associazioni di parole suggerite non potevano considerarsi espressione di pensiero o

---

<sup>36</sup>Langdon v Google, Yahoo! and Microsoft Corp., 474 F Supp 2d 622 (D Del 2007).



opinione e quindi non potevano avere un significato diffamatorio di rilevanza legale. Ciò che costituisce un possibile motivo di difesa per la legge statunitense, sarebbe stato invece un motivo di responsabilità del motore di ricerca per il diritto europeo.

## **6.2. La protezione dei dati personali: divergenze e convergenze tra Europa e Stati Uniti**

Sono molteplici le divergenze tra vecchio e nuovo continente nell'ambito della regolamentazione sulla protezione dei dati personali. In Europa l'idea di *privacy* si ricollega al concetto di dignità e onore, di conseguenza, la tutela giuridica comporta l'esigenza di proteggere il soggetto dalla circolazione di informazioni personali in grado di incidere sulla sua immagine sociale. Negli USA invece l'idea di *privacy* è incentrata sulla tutela dello spazio vitale dell'individuo, circoscritto dalla sua persona e proprietà, rispetto alle intrusioni da parte dello Stato. Sono concetti di *privacy* molto differenti: da un lato abbiamo il controllo sulla propria rappresentazione sociale, dall'altro la libertà da intrusioni pubbliche nella propria sfera privata (Sartor- Cunha). Conseguentemente, avranno diverso rilievo i valori e gli interessi suscettibili di opporsi alla *privacy*. Negli USA vi è la predominanza assoluta della libertà di espressione che limita fortemente il diritto alla riservatezza sulla pubblicazione d'informazioni personali attraverso i mezzi di comunicazione, incluso Internet; i soli limiti sono la proprietà intellettuale e le immagini di nudità. La preminenza della "*freedom of speech*" preclude, nel diritto nordamericano, ogni spazio per il diritto all'oblio. Infatti, a differenza dell'Europa, in cui vi è il riconoscimento del diritto all'oblio rispetto a informazioni pregiudizievoli per l'interessato e non più attuali, negli Stati Uniti non vi è alcun limite alla pubblicazione di informazioni vere su eventi passati. In realtà, il fatto che notizie vere siano pregiudizievoli per la reputazione di un soggetto non esclude la liceità della loro pubblicazione. Nel contesto statunitense, anche la libertà d'iniziativa economica viene spesso ad acquistare preminenza rispetto alla *privacy*. Infatti, la profilazione<sup>37</sup> e la cessione di profili di consumatori, il riuso di dati personali per scopi ulteriori e diversi

---

<sup>37</sup> Insieme di attività di raccolta ed elaborazione dati inerenti agli utenti di servizi per suddividere l'utenza in gruppi di comportamento.

da quelli che ne hanno determinato la raccolta, sono ritenuti comportamenti leciti, indipendentemente dal consenso dell'interessato.

Le due culture giuridiche differiscono anche nell'attitudine rispetto al rischio derivante dall'innovazione tecnologica. Per questo motivo negli USA abbiamo l'idea di un'innovazione libera e non subordinata a richieste e autorizzazioni, in Europa si temono la pericolosità ed illiceità dell'innovazione, che va quindi subordinata all'intervento di controllo delle autorità competenti. In particolare, negli ordinamenti europei, è considerato illegittimo ogni trattamento di dati personali che non sia previsto dal Garante o espressamente consentito dall'interessato. Ciò diventa problematico nella nuova era, segnata dai cosiddetti *big data*<sup>38</sup> e dalla possibilità di elaborare dati personali in modi nuovi e complessi, per scopi legittimi, ma non originariamente previsti e consentiti. Stiamo parlando della raccolta automatica di enormi quantità di dati, per svariate finalità di utilità economica, scientifica, sociale, non prevedibili al momento della raccolta.

I grandi protagonisti dell'economia digitale si trovano proprio negli Stati Uniti e traggono enorme profitto dalla raccolta e dall'elaborazione dei dati personali, esercitando tra l'altro una grande capacità di *lobbying*<sup>39</sup> nei confronti del legislatore statunitense. Il legislatore europeo, invece, sente l'esigenza di limitare il grande potere delle imprese statunitensi e di tutelare i consumatori, ma anche le stesse imprese europee; dunque la restrizione della libertà d'impresa in nome del diritto alla riservatezza assume connotazioni protezionistiche.

Un'altra divergenza tra le due realtà giuridiche oggetto del nostro confronto sta nella subordinazione della *privacy* alla preponderante importanza della sicurezza pubblica nazionale. Gli Stati Uniti, infatti, essendo una superpotenza militare, soggetta a particolari rischi e minacce, soprattutto dopo l'attentato dell'11 settembre 2001, tendono a dare maggior importanza alle esigenze geopolitiche e di sicurezza nazionale. Il fatto che detengano strumenti per il controllo globale delle comunicazioni e che nel loro territorio risiedano i principali attori della rete, permette loro di effettuare una raccolta di informazioni globale, così come emerso anche dalle rivelazioni di Edward

---

<sup>38</sup>Si parla di *big data* quando sia ha un *dataset* talmente grande da richiedere strumenti non convenzionali per estrapolare e gestire informazioni in tempi ragionevoli.

<sup>39</sup>Pressione politica.

Snowden<sup>40</sup>. Ciò non vuol dire che la raccolta massiccia di informazioni così come avviene negli USA possa essere giustificata, tuttavia non è avvertita in modo così rigido ed indignato come accade in Europa, ma con maggior comprensione e flessibilità, giacché le predominanti esigenze di sicurezza e controllo rendono meno sconvolgente l'impiego di mezzi di sorveglianza. Dopo l'attentato alle Torri Gemelle, gli Stati Uniti hanno adottato due provvedimenti restrittivi dei diritti dei cittadini: il *Patriot Act*, che autorizza agenzie ed enti governativi ad avere libero accesso a banche-dati pubbliche e private, nonché a tabulati telefonici, email, file finanziari e medici; l'*Aviation and Transportation Security Act*, in base al quale tutte le compagnie aeree che volano verso gli USA devono fornire i dati dei propri passeggeri. Anche molti governi europei hanno cominciato a cedere alla convinzione che il diritto alla riservatezza possa essere sacrificato in nome della lotta contro il terrorismo e la criminalità organizzata e lo scambio di dati personali tra le autorità di polizia dei diversi Stati membri è la prova di questa cooperazione internazionale. Tuttavia, recentemente, è stato sostenuto in un parere del Gruppo di Lavoro per la protezione dei dati personali, nell'articolo 29 che <<*i provvedimenti contro il terrorismo non devono compromettere gli standard per la protezione dei diritti fondamentali che caratterizzano le società democratiche*>>.

In conclusione, alla preminenza assoluta della libertà di espressione nel sistema giuridico statunitense si contrappone il rilievo della protezione dei dati in Europa; alla fiducia nella libertà economica e nel progresso tecnologico tipiche della cultura statunitense, si oppongono gli atteggiamenti più sospettosi degli europei. All'interesse degli utenti ad avere accesso alla massima quantità di informazioni veritiere e affidabili, all'interesse opposto di chi carica informazioni in rete ad avere il più ampio numero possibile di lettori, e per finire all'interesse delle imprese di Internet a fornire la massima quantità di informazioni ai propri utenti ed evitare i costi connessi all'esercizio di una funzione di controllo e di censura, troviamo contrapposto l'interesse dell'individuo a rimuovere informazioni personali per sé pregiudizievoli. Dietro questo apparente scenario di difesa di interessi, diritti e libertà costituzionalmente tutelati dai rispettivi ordinamenti, si nascondono senza ombra di dubbio anche ragioni economiche non meno rilevanti. Gli Stati Uniti sono interessati a mantenere la superiorità delle proprie imprese e l'influenza sulla rete; gli europei vogliono invece limitare tale superiorità e promuovere le attività

---

<sup>40</sup>Cfr. par. 6.3.

proprie. Tra i giganti statunitensi del *web*, Google occupa sicuramente il posto principale e negli ultimi tempi le preoccupazioni legate ad un cattivo utilizzo ed eccessiva commercializzazione dei dati personali hanno ingenerato una vera e propria “*Googlephobia*” che il recente caso Snowden ha rivestito di connotati politici, oltre che economici.

### 6.3 Il caso Snowden

I principali fornitori di servizi di rete e ISP sono localizzati negli USA e la preminenza economica delle imprese statunitensi è tale che esse sono in grado di determinare la regolazione di Internet in modo conforme ai propri interessi. Tali imprese possono essere indotte o costrette a collaborare con il governo statunitense, fornendo dati e strumenti per operazioni di sorveglianza sul terrorismo, ma anche per indagini giudiziarie, spionaggio politico e militare, e addirittura spionaggio industriale. D’altro canto bisogna ricordare che è stato lo stesso governo statunitense a promuovere lo sviluppo di Internet quale area di libertà e di progresso, incentivando la libertà di iniziativa economica, l’innovazione tecnologica, la libertà di espressione, nonché il dialogo politico e culturale. Le rivelazioni dell’ex consulente della NSA<sup>41</sup> sull’esistenza di programmi di sorveglianza di massa hanno evidenziato il carattere “oscuro” del predominio statunitense sulla rete. Il fatto che la *governance* di Internet spetti agli Stati Uniti, che le imprese americane profittino di Internet in modo sproporzionato e in più che i servizi di sicurezza statunitensi abbiano accesso privilegiato a tutte le informazioni che transitano sulla rete, ha fatto emergere l’esigenza di rivedere il sistema di *governance* e passare ad un nuovo quadro internazionale. In Europa, specie in Germania, Francia e Spagna è stata evidente la reazione indignata a seguito delle rivelazioni sul monitoraggio di massa effettuato dalla NSA. Una reazione di stupore e di sdegno da molti ritenuta ipocrita, considerando che le operazioni di sorveglianza erano state compiute con il sostegno delle agenzie di *intelligence* locali. Lo stesso Snowden,

---

<sup>41</sup> *National Security Agency*: organismo governativo degli Stati Uniti d’America che, insieme alla CIA e all’FBI, si occupa della sicurezza nazionale.

infatti, ha rivelato che alcuni Paesi europei, tra cui Regno Unito e Francia, avevano agito di concerto con la NSA e condiviso con gli USA enormi quantità di dati.

In ogni caso, anche queste rivelazioni hanno contribuito ad allontanare ulteriormente il quadro europeo di regolamentazione della *data-protection* da quello statunitense.

Sembra indubbio che anche in seguito alla decisione della CGUE sul noto caso *Google Spain*, il divario sia aumentato ancora di più, a spese, in particolare, del diritto di informazione dei cittadini europei. In particolare, i *link* a dati “da dimenticare” saranno inaccessibili agli utenti europei, rimanendo invece a disposizione degli statunitensi; ma di questo ci occuperemo approfonditamente nel prossimo capitolo.

## CAPITOLO II

### **Verso il nuovo regolamento europeo sulla *data-protection***

#### **1. Il destino di *Google Suggest* alla luce della sentenza *Google Spain***

Sebbene *Google Spain* sia una decisione che riguarda i risultati di ricerca, la sua connessione con i suggerimenti della funzione *auto-complete* è molto forte. Se, infatti, i motori di ricerca hanno l'obbligo di controllare i dati personali che semplicemente appaiono inclusi tra le pagine *web*, essi dovranno *a fortiori* controllare le informazioni personali suggerite e presentate agli utenti quando inseriscono un termine di ricerca. Quando un utente digita il nome di una persona nella barra di ricerca, il dato viene processato dall'algoritmo, che lo combina con altre informazioni e mostra una lista di suggerimenti di ricerca che potrebbero far scoprire altre informazioni personali riguardanti l'interessato. Quindi, sembra ragionevole concludere che le imposizioni imposte dalla Corte di Giustizia dell'Unione Europea in merito ai risultati di ricerca debbano estendersi ai suggerimenti di ricerca. Supponiamo infatti che il soggetto interessato ottenga la rimozione di *link* pregiudizievole dalla lista dei risultati di ricerca; le informazioni non appariranno più tra i risultati di ricerca, tuttavia la funzione *auto-complete* potrebbe facilitare gli utenti nel rintracciarle attraverso ricerche alternative, utilizzando i suggerimenti di ricerca proposti da detta funzione. L'esercizio del diritto all'oblio comporta per l'interessato la definitiva rottura e separazione tra le ricerche aventi ad oggetto la sua identità e i link che conducono ad informazioni lesive della sua reputazione; in virtù di ciò, l'osservanza di quanto previsto dalla Corte europea dovrebbe interessare ogni sistema o procedura tecnica che faciliti la ricostruzione di tali *link* diffamatori. La decisione sul caso *Google Spain* si estende, dunque, anche ai suggerimenti di ricerca automatici. I motori di ricerca rivestono un ruolo decisivo nella diffusione di informazioni riguardo una persona. Il modo in cui queste informazioni sono organizzate, aggregate e presentate dal motore di ricerca, ad esempio attraverso i risultati di ricerca oppure attraverso i suggerimenti di ricerca, possono porre l'utente

nelle condizioni di stabilire un profilo più o meno dettagliato del soggetto interessato. Secondo la Corte di Giustizia dell'Unione Europea, i fattori da considerare nell'esame del caso devono includere la natura dell'informazione, il grado di sensibilità dei dati e l'interesse pubblico all'ottenimento di quella informazione, un interesse che dipende dal ruolo ricoperto dall'interessato nella vita pubblica. Il bilanciamento tra interesse pubblico e privato è uno degli argomenti basilari della questione. Nel caso precedentemente analizzato riguardo Bettina Wulff, moglie dell'ex Presidente tedesco, il ruolo di personaggio pubblico rivestito dalla donna aveva escluso l'accoglimento del suo reclamo. Il criterio di bilanciamento tra interessi pubblici e privati è stato descritto dalla Corte Europea dei Diritti dell'Uomo nel caso *von Hannover v Germany*<sup>42</sup> in cui è stabilito che può essere invocata la libertà di espressione e quindi l'interesse del pubblico alla scoperta delle informazioni private riguardanti la vita di un personaggio pubblico, solo laddove tale interesse non sia meramente volto al soddisfacimento di una propria curiosità personale. Di conseguenza dovrà essere presa in considerazione non tanto la notorietà del soggetto interessato, quanto piuttosto la natura dell'informazione in questione.

### **1.1. I capisaldi della sentenza della Corte di Giustizia Europea. Il fatto.**

Il fatto oggetto della celebre statuizione della CGUE riguarda la controversia tra Google Spain e Google Inc. contro un cittadino spagnolo, il quale ha chiesto all' *Agencia Española de Protección de Datos (AEPD)* la rimozione dai motori di ricerca di alcuni suoi dati personali. Infatti, digitando il suo nome tramite "Google search", il motore di ricerca restituiva come risultati di ricerca alcuni *link* verso pagine di un quotidiano risalenti al 1998. Tali pagine annunciavano una vendita all'asta di immobili organizzata a seguito di un pignoramento effettuato per la riscossione coattiva di crediti previdenziali nei confronti dell'interessato. Il ricorrente ha richiesto la rimozione dei suoi dati sia dal quotidiano spagnolo che da *Google search*. Il Garante per la Privacy

---

<sup>42</sup> Von Hannover v Germany II Case Nos 40660/08 and 60641/08 (ECtHR, 7 February 2012).

spagnolo ha respinto il ricorso diretto al quotidiano in quanto la pubblicazione delle informazioni in questione era assolutamente legittima, considerando che aveva avuto luogo su ordine del Ministero del Lavoro e degli Affari sociali e aveva lo scopo di rendere pubblica la vendita, al fine di avere il maggior numero di partecipanti all'asta.

Il Garante ha accolto il reclamo contro Google considerando l'attività del motore di ricerca come un'attività di trattamento di dati, della quale Google è responsabile. Tale decisione è stata impugnata da Google dinanzi all' *Audiencia Nacional de España*, la quale ha sospeso il procedimento, rinviando pregiudizialmente alcuni punti della questione alla Corte di Giustizia dell'Unione Europea. La Corte europea ha analizzato l'attività del motore di ricerca ritenendo che questi: dapprima esplora Internet alla ricerca di informazioni ivi pubblicate; in seguito i dati così reperiti vengono raccolti, estratti, registrati, organizzati attraverso programmi di indicizzazione e conservati nei *server*; infine tali dati vengono messi a disposizione degli utenti tramite elenchi di risultati forniti a seguito delle loro ricerche. La Corte ha rilevato che tale attività di organizzazione e aggregazione delle informazioni, svolta dai motori di ricerca al fine di facilitare ai loro utenti l'accesso a queste informazioni, può avere come effetto che *<<tali utenti, quando la loro ricerca viene effettuata a partire dal nome di una persona fisica, ottengono attraverso l'elenco dei risultati, una visione complessiva strutturata delle informazioni relative a questa persona reperibili su Internet, che consente loro di stabilire un profilo più o meno dettagliato di quest'ultima>>*. Un siffatto trattamento di dati potrebbe *<<incidere significativamente sui diritti fondamentali al rispetto della vita privata e alla protezione dei dati personali>>*. La Corte, quindi, ha qualificato tali operazioni del motore di ricerca come "trattamento" ai sensi della Direttiva 95/46, facendo di conseguenza sorgere in capo a Google gli obblighi di cui alla suddetta direttiva, ovvero, *in primis*, il riconoscimento all'interessato di ottenere dal responsabile del trattamento la rettifica, la cancellazione o il congelamento dei dati.

Tuttavia, la soppressione dei *link* dall'elenco dei risultati di ricerca potrebbe avere ripercussioni sul legittimo interesse degli utenti di Internet all'accesso a tali informazioni; occorre dunque trovare un giusto equilibrio tra tale interesse e i diritti fondamentali della persona di cui agli artt. 7 e 8 della Carta di Nizza. Tale equilibrio potrebbe dipendere *<<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>>, fermo restando che i diritti fondamentali, in linea di principio, prevalgono, <<non soltanto sull'interesse economico del gestore del motore di ricerca, ma anche sull'interesse di tale pubblico a trovare l'informazione suddetta (...). Tuttavia, così non sarebbe qualora risultasse, per ragioni particolari, come il ruolo ricoperto da tale persona nella vita pubblica, che l'ingerenza nei suoi diritti fondamentali è giustificata dall'interesse preponderante del pubblico suddetto ad avere accesso (...) all'informazione di cui trattasi>>.*

In conclusione, la Corte, in relazione al procedimento sottoposto al suo esame, ha affermato che: *<<tenuto conto del carattere sensibile delle informazioni contenute in tali annunci per la vita privata di detta persona, nonché del fatto che la loro pubblicazione iniziale era stata effettuata 16 anni prima, la persona interessata vanta un diritto a che tali informazioni non siano più collegate al suo nome attraverso un elenco siffatto. Pertanto, dal momento che nella fattispecie non sembrano sussistere ragioni particolari giustificanti un interesse preponderante del pubblico (...) - aspetto questo che spetta però al giudice del rinvio verificare -, la persona interessata può esigere (...) la soppressione dei link suddetti da tale elenco di risultati>>.*

## **1.2 >>>segue: il contesto delle attività di stabilimento**

È importante identificare lo stabilimento di un'impresa responsabile del trattamento di dati personali al fine dell'individuazione delle norme nazionali di attuazione della Direttiva 95/46 sulla tutela dei dati personali. Le attività del Gruppo Google sono svolte in parte, dalla società madre che opera in un Paese extraeuropeo, ossia in California (USA) e che indicizza e archivia le ricerche sul *web* ed in parte dalle filiali localizzate nei vari Stati membri dell'Unione che offrono l'interfaccia del servizio di ricerca agli utenti di uno Stato membro e gestiscono l'attività pubblicitaria tramite una serie di *link* sponsorizzati dalle imprese. Il principio del diritto europeo di cui all'art. 49 del TFUE stabilisce che le persone fisiche che esercitano attività autonome e le persone giuridiche che operano in uno Stato membro possono esercitare un'attività economica in un altro Stato membro stabilmente e prestare così servizi transfrontalieri pur conservando il loro

stabilimento nel Paese d'origine. L'interpretazione data dalla Corte di giustizia europea nella sentenza in esame parte dall'analisi dell'organizzazione dei servizi offerti da Google. La Corte nota che la società madre indicizza i siti *web* a livello globale e raccoglie informazioni per poi memorizzarle su *server* di cui resta ignota l'ubicazione. Parallelamente, Google svolge anche attività di comunicazione pubblicitaria tramite le proprie filiali che si occupano della gestione degli spazi pubblicitari. Le due finalità di ricerca e pubblicità del motore sono da considerarsi inscindibili e ciò vale anche per le relative attività realizzate nel "contesto delle attività di stabilimento" delle filiali nazionali del Gruppo Google. Un trattamento di dati personali viene effettuato nel contesto delle attività di stabilimento del responsabile di tale trattamento nel territorio di uno Stato membro, qualora il gestore di un motore di ricerca apra in uno Stato membro una succursale o una filiale destinata alla promozione e alla vendita degli spazi pubblicitari proposti dal motore di ricerca e la cui attività è diretta agli abitanti dello Stato membro. Non è determinante stabilire se concretamente le singole filiali concorrano all'indicizzazione, che può essere effettuata anche al di fuori dell'Unione. Infatti, le filiali nazionali sono da considerarsi responsabili del trattamento dei dati in virtù della loro mera partecipazione all'attività di comunicazione commerciale. Secondo la Corte europea, quindi, lo stabilimento in uno Stato membro di un'impresa stabilita al di fuori dell'Unione gioca un ruolo determinante per l'identificazione della normativa applicabile, che sarà quella dello Stato membro in questione (e quindi la normativa europea) se è implicato un servizio di vendita pubblicitaria rivolto agli abitanti di tale Stato. Per quanto riguarda le possibili influenze della sentenza *Google Spain* sul futuro Regolamento europeo, ormai di prossima adozione, il Consiglio e il Parlamento europeo sembrano intenzionati a riaffermare il criterio delle attività svolte all'interno dello stabilimento del responsabile del trattamento nell'Unione. Tuttavia, il nuovo Regolamento renderà uniforme la disciplina in materia nei vari Paesi del continente. Dunque non si porrà più la questione relativa all'applicazione della legge nazionale dei singoli Stati membri, ma il problema principale riguarderà l'applicabilità del nuovo regolamento ai responsabili di trattamento non stabiliti all'interno dell'Unione Europea. Infatti nella proposta di Regolamento della Commissione troviamo l'introduzione di un ulteriore criterio di applicazione all'art. 3, par.2. L'art. 3 della proposta della Commissione recita infatti:

<< 1. Il presente regolamento si applica al trattamento dei dati personali effettuato nell'ambito delle attività di uno stabilimento di un responsabile del trattamento nell'Unione. 2. Il presente regolamento si applica al trattamento dei dati personali di residenti nell'Unione effettuato da un responsabile del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano: a) l'offerta di beni o la prestazione di servizi ai suddetti residenti nell'Unione, oppure b) il controllo del loro comportamento>>.

### **1.3 >>>segue: la procedura di de-indicizzazione**

Nella sentenza *Google Spain* non compare esattamente la locuzione di “diritto all’oblio” in quanto il vero oggetto della sentenza è il diritto all’oscuramento di determinati risultati di ricerca associati al proprio nome dalla funzione *Google search*. La Corte riconosce a qualsivoglia interessato il diritto di presentare al gestore del motore di ricerca un’istanza volta ad ottenere l’esclusione dai risultati di ricerca collegati al suo nome di determinate informazioni presenti in rete e riguardanti la sua sfera privata. Se il gestore dovesse disattendere l’istanza, l’interessato potrà rivolgersi all’autorità di controllo nazionale in materia di *privacy* o, in alternativa, all’autorità giudiziaria. La Corte, qualificando l’attività del *search engine* come trattamento dati, ha posto le basi per l’applicabilità della direttiva 95/46 CE a tale attività, prevedendo la possibilità per l’interessato di proporre un’istanza e, in caso di mancato accoglimento, di rivolgersi al Garante o all’autorità giudiziaria. Oggetto dell’istanza, come abbiamo detto, sarà il diritto alla dissociazione del proprio nome da un dato risultato di ricerca. Non quindi il diritto alla cancellazione dell’informazione dalla rete, bensì alla dissociazione di una specifica pagina da una peculiare *query* di ricerca, ossia il nome dell’interessato. Non si tratta più, o almeno non esclusivamente, di diritto alla dimenticanza di sé, ma di diritto al semplice ridimensionamento della propria visibilità telematica. Il dato personale oggetto d’istanza di de-indicizzazione non verrà rimosso dal *web*, ma semplicemente sottratto ad una modalità di reperimento semplice ed istantanea; l’utente interessato a quella specifica informazione potrebbe effettuare ulteriori ricerche, visitando direttamente le pagine e gli archivi dei quotidiani; dunque l’informazione continuerà ad

essere accessibile, ma attraverso una più difficoltosa navigazione. La criticità maggiore di un simile meccanismo è rappresentata dal forte pregiudizio alla libertà di espressione. Infatti l'istanza sarà vagliata ed accolta o rigettata in base alle sole valutazioni dell'interessato e del motore di ricerca, tenendo quindi conto principalmente degli interessi di queste due figure (diritti della personalità da un lato, libertà d'impresa dall'altro). Sarebbe forse stato opportuno introdurre una valutazione *ex ante* del Garante, a tutela dell'interesse pubblico alla libertà di espressione e di informazione, invece di prevedere l'intervento dell'autorità amministrativa solo in seguito al non accoglimento dell'istanza da parte del *search engine*. Il soggetto chiamato a valutare l'istanza è il motore di ricerca, il quale difficilmente anteporrà l'interesse collettivo al proprio interesse economico. Per il motore di ricerca sarà economicamente più efficiente accontentare tutti i segnalanti, piuttosto che valutare analiticamente i presupposti di ogni singola istanza. Ciò potrebbe spingere i gestori dei motori di ricerca ad optare sempre per la soluzione meno rischiosa, a prescindere dalla sussistenza o meno di un reale diritto all'oblio e al mancato interesse pubblico che giustifichi la permanenza dell'informazione sulla rete. Oppure, al contrario, i motori di ricerca potrebbero rigettare la maggior parte delle istanze, al fine di oberare le autorità garanti nazionali e dimostrare l'inefficacia di una siffatta tutela.

Si presenta poi un ulteriore problema: le misure conseguenti all'omologazione alla sentenza *Google Spain* si applicheranno solo ai motori di ricerca stabiliti in Europa e ciò potrebbe determinare un vantaggio competitivo per gli operatori extra-europei (ad esempio Baidu in Cina o Yandex in Russia) che indicizzeranno un numero maggiore di informazioni e, essendo accessibili anche dall'Europa, potrebbero attrarre gli utenti dei loro *competitor*.

Per finire, l'ultimo aspetto critico riguarda il fatto che l'interessato è sì titolare di un diritto assoluto alla cancellazione del dato personale, ma non di un diritto all'indicizzazione dei contenuti, che non è riconosciuto a livello normativo. Di conseguenza, qualora il motore di ricerca non ottemperi, non potrà essere chiamato a risarcire un danno da mancata indicizzazione. Non è dunque sufficiente la mancata rimozione del risultato di ricerca per aversi risarcimento, ma l'interessato dovrà dimostrare di aver subito un danno dalla permanenza del collegamento ipertestuale.

Google sembra stia tentando di adeguarsi alle previsioni della sentenza *Google Spain*: annuncia di essersi dotata di un *team* di esperti tecnici e legali che esamineranno le istanze provenienti dai cittadini europei; ha messo a disposizione degli utenti sul *web* i moduli precompilati<sup>43</sup> per proporre istanza; ha ideato strumenti disponibili per esercitare una qualche forma di controllo sui dati pubblicati. Con riguardo a quest'ultimo punto, il motore di ricerca ha messo a disposizione degli utenti delle apposite sezioni, *Google Webmaster Tools*, per segnalare link a pagine non più esistenti, modificate o non aggiornate. In assenza di segnalazioni, infatti, il motore di ricerca potrebbe impiegare mesi prima di accorgersi che una data pagina sia stata modificata o addirittura rimossa. Abbiamo poi altre tecniche di de-indicizzazione *ex post* o di prevenzione dell'indicizzazione, che tuttavia rimangono per il momento abbastanza rudimentali. Tra queste, il *Robots Exclusion Protocol* (REP), una convenzione grazie alla quale la visibilità dei contenuti di un sito tra i risultati di ricerca è modulabile dal gestore tramite compilazione di un *file* di tipo testuale (*robots.txt*). Tuttavia non è detto che i motori di ricerca rispettino pienamente il REP, in quanto non esiste nessun obbligo di attenersi ad esso. Infine, effetti inibitori dell'indicizzazione automatica si ottengono proteggendo le pagine *web* con l'utilizzo dei *Captcha*, volti a discriminare tra utenti umani e programmi automatici di raccolta dati, attraverso un'applicazione informatica. In ogni caso, ad avviso del Garante, in seguito al caso *Google Spain*, l'azienda è tenuta a dotarsi di una *policy* di data *deletion*, cioè di cancellazione dei dati su richiesta degli utenti, e di una *policy* di data *retention* che tenga conto del rispetto del principio di finalità del trattamento.

#### **1.4. >>>segue: il diritto all'oblio**

La questione al centro del rinvio pregiudiziale, nel caso *Google Spain*, consiste essenzialmente nello stabilire se il diritto dell'Unione Europea conferisca agli individui il diritto di ottenere la rimozione dei propri dati, laddove le finalità per le quali si sta

---

<sup>43</sup>In tali moduli l'interessato dovrà indicare: a) normativa nazionale di riferimento; b)nome che ha condotto alla visualizzazione dei risultati di ricerca indesiderati; c)nome del richiedente; d) email; e) URL dei risultati di cui si richiede la rimozione; f)motivazione sintetica; g)copia documento d'identità; h)dichiarazione di esattezza e conformità delle dichiarazioni riportate; i) firma e data.

svolgendo il trattamento siano state soddisfatte o siano venute meno. In tale contesto, si incontra quella declinazione del diritto alla protezione dei dati personali che è nota come “diritto all’oblio”<sup>44</sup> e che la proposta di Regolamento adottata dalla Commissione sembra voler cristallizzare in una norma *ad hoc*. Questione dibattuta, al di là della futura approvazione del Regolamento, è se un siffatto diritto possa dirsi esistente e le corti siano chiamate a garantirne la tutela, sebbene non abbia per ora un esplicito riconoscimento normativo. La Corte europea, nella sentenza *Google Spain*, ha tentato di ravvisare il fondamento normativo di tale diritto nella Carta di Nizza. Partendo dalle questioni che pone l’Avvocato Generale<sup>45</sup>, notiamo che egli si chiede proprio se l’art. 7<sup>46</sup> della Carta di Nizza, in combinato disposto con le norme della direttiva 95/46 che attribuiscono agli interessati il diritto di ottenere la cancellazione o il blocco dei dati e il diritto di opporsi al trattamento<sup>47</sup>, possa offrire un fondamento giuridico al diritto all’oblio. L’Avvocato ritiene che se i gestori dei motori di ricerca in Internet fossero gravati della rimozione dei risultati segnalati dagli utenti, senza una previa consultazione o richiesta del gestore delle pagine *web* interessate, si assisterebbe ad una non adeguata ponderazione degli interessi in merito, nel caso di specie libertà di espressione e tutela della sfera privata dell’individuo. Inoltre, nessun generalizzato diritto all’oblio potrebbe desumersi dalle disposizioni della direttiva, neppure se lette in combinato disposto con l’art. 7. Tuttavia, la Corte di Giustizia ha stravolto il ragionamento dell’Avvocato Generale, ritenendo che gli interessati abbiano il diritto di ottenere dal motore di ricerca l’eliminazione di risultati di ricerca che rechino collegamenti a contenuti indesiderati o non più attuali e che il fondamento giuridico di tale diritto si individua proprio negli artt. 7 e 8<sup>48</sup> della Carta dei Diritti Fondamentali

---

<sup>44</sup> Si ricordi che la sentenza non parla esplicitamente di diritto all’oblio ma di diritto alla cancellazione di determinati *link* dai risultati di ricerca. Il riferimento al diritto all’oblio si ricava in maniera indiretta.

<sup>45</sup> Cfr. Conclusioni dell’Avvocato Generale Niilo Jääskinen nella causa C-131/12.

<sup>46</sup> 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>>.

<sup>47</sup> Rispettivamente art. 12, lett. b) e art. 14, lett. a).

dell'Unione Europea e dalle previsioni già richiamate, contenute nella direttiva 95/46. Secondo i giudici, l'obbligo di valutazione e attuazione delle richieste degli utenti deriva dalla qualifica di titolari del trattamento di dati personali che i motori di ricerca rivestirebbero nell'atto di indicizzare i contenuti delle pagine *web* dei siti sorgente. Ciò che maggiormente interessa è la scarsissima rilevanza attribuita dalla Corte alla libertà d'informazione, nella sua declinazione attiva e passiva, vale a dire al diritto dei titolari di siti, si pensi ad esempio ad un giornale *online* il cui interesse è quello di vedere circolare le proprie informazioni in modo ampio attraverso i motori di ricerca, e al diritto degli utenti di reperire agevolmente una notizia e di accedere all'informazione. Sono questi diritti che risultano sacrificati, in nome di una preminente tutela che la Corte riserva alla protezione dei dati personali. Il bilanciamento condotto dalla Corte è apparso eccessivamente orientato a favore dei diritti consacrati dagli artt. 7 e 8 (rispetto della vita privata e protezione dei dati personali) e a danno dei diritti e delle libertà ex artt. 11 e 16 della stessa Carta (libertà di espressione e di informazione e libertà d'impresa). La questione risulta ancora più seria e problematica, laddove la Corte omette di dettare criteri specifici ai quali i motori di ricerca dovranno attenersi per operare il bilanciamento degli interessi in gioco; la valutazione che il *search engine* è chiamato a compiere, a fronte di una richiesta di rimozione, resta sprovvista di precise indicazioni che avrebbero invece potuto garantire un rapporto più ponderato tra protezione dei dati personali e diritto all'informazione. Sorprende il fatto che la Corte, in tutta la sentenza, non abbia mai fatto riferimento all'art. 11, mentre dovrebbe essere principalmente quello il termine di paragone con cui confrontare il diritto dell'interessato alla cancellazione e non il fatto che Google abbia lucrato sull'attività di trattamento dati. Che Google sia considerata una società americana che gestisce il suo servizio Google *search* per fini economici e commerciali è un fatto del tutto irrilevante nell'operazione di bilanciamento. È la finalità, o meglio l'utilità del trattamento in sé del

---

<sup>48</sup> 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 è soggetto al controllo di un'autorità indipendente>>.

dato personale a determinare l'accoglimento o il rigetto dell'istanza dell'interessato, non le motivazioni imprenditoriali o filantropiche di chi opera il trattamento.

Il diritto all'oblio, la cui affermazione in molti ravvisano nella sentenza del 13 maggio 2014, rappresenta il diritto dell'individuo ad essere dimenticato soprattutto riferendosi ad una notizia che, già resa pubblica, è destinata a finire nel dimenticatoio, a causa del decorso del tempo. Il diritto all'oblio viene concepito come manifestazione del diritto alla riservatezza e del diritto all'identità personale. Per quanto attiene al primo profilo, si ritiene che, una volta venuto meno l'interesse alla conoscenza del fatto, il diritto alla riservatezza tuteli il soggetto dalla curiosità pubblica. Tuttavia il diritto all'oblio, pur essendo attinente alla sfera della riservatezza, si distingue nettamente dal diritto alla riservatezza, in quanto ha ad oggetto informazioni già uscite dalla sfera privata dell'interessato e delle quali si vuole impedire una nuova circolazione. Il connotato essenziale del diritto all'oblio è il fattore tempo: decorso un notevole intervallo temporale, si ritiene giustificata la pretesa del soggetto a riappropriarsi di notizie che lo riguardano, che un tempo sono state note, ma sulle quali è in seguito caduto l'oblio. C'è un ulteriore dato che si aggiunge al fattore tempo ed è l'inesistenza di un'utilità sociale alla rievocazione di tali notizie.

Con riferimento al secondo profilo, invece, il diritto all'oblio salvaguarda la proiezione sociale dell'identità personale, ossia tutela il soggetto dalla divulgazione di notizie potenzialmente lesive, non più attuali e il cui trattamento potrebbe risultare ingiustificato e suscettibile di ostacolare il soggetto nell'esplicazione e nel godimento della propria personalità.

Per determinare se esiste o meno il diritto all'oblio occorre verificare la sussistenza di un interesse pubblico alla conoscenza dei fatti oggetto della nuova pubblicazione. L'antigiuridicità della condotta lesiva della altrui reputazione deve essere ponderata sull'interesse generale alla conoscenza del fatto, o meglio sull'attitudine della notizia a contribuire alla formazione dell'opinione pubblica, in modo che ognuno possa fare liberamente le sue scelte, sulla base di un'ampia conoscenza. La giurisprudenza ha ritenuto che l'interesse pubblico, anche se persistente o rinnovato, debba in ogni caso contemperarsi con la legittima aspettativa dell'interessato ad essere dimenticato dall'opinione pubblica e dalla memoria collettiva. Il fatto che una data notizia sia stata legittimamente resa pubblica in un'epoca anteriore e in un contesto differente, non ne



legittima la sua riproposizione in un'epoca posteriore e in un contesto del tutto differente. Dunque, la tematica del diritto all'oblio deve essere valutata alla luce del parametro dell'interesse pubblico, il quale, a sua volta, deve possedere il requisito dell'attualità: laddove la notizia manchi di attualità, questa non potrà soddisfare alcuna utilità sociale e quindi non potrà legittimamente contrapporsi al diritto all'oblio dell'interessato. L'attualità, poi, non tanto viene richiesta rispetto al fatto, quanto piuttosto rispetto all'interesse pubblico della notizia; infatti, notizie anche molto datate, o per la loro eccezionalità o per l'efferatezza dei delitti cui attengono, necessitano di essere sempre ricordate.

Il diritto all'oblio è diventato un tema ancora più centrale nelle corti, soprattutto in seguito all'avvento di Internet, che ha stravolto la logica dei mezzi di comunicazione di massa tradizionali. Internet, a differenza degli archivi, è dotato di una memoria illimitata; inoltre, sulla rete, le informazioni non sono catalogate e organizzate, ma poste tutte sullo stesso livello, per cui ne risultano appiattite e decontestualizzate. Da qui si comprende come la diffusione di informazioni riguardo un medesimo soggetto sulla rete risulti cumulativa ed immediata e suscettibile di ledere diritti e interessi legittimi del soggetto, soprattutto quando si tratta di fatti ormai risalenti nel tempo. Per questo, la giurisprudenza sta cercando di tutelare i casi di informazioni diffuse via Internet, tenendo conto della natura del mezzo che consente alle informazioni di "galleggiare" in una sorta di eterno presente, prive di contestualizzazione e rendendo gli utenti incapaci di valutare la realtà e l'eventuale evoluzione dei fatti. Innanzitutto è quindi necessario l'aggiornamento costante delle informazioni presenti sulla rete, al fine di andare al passo con possibili evoluzioni dei fatti; in secondo luogo, è necessario il riconoscimento in capo al soggetto del diritto all'oblio. La sentenza che abbiamo ampiamente analizzato rappresenta per molti il riconoscimento a livello europeo del diritto all'oblio e ha introdotto anche un'ulteriore novità, ossia che le richieste di cancellazione dei propri dati personali possano essere dirette anche solo al gestore del motore di ricerca, cui è richiesto non un controllo preventivo, bensì un intervento *a posteriori* e su iniziativa dell'interessato. Tuttavia l'esigenza di dare una solida tutela anche al contrapposto diritto di informazione sembra non trovare cittadinanza nella celebre sentenza; allo stesso tempo si pone l'esigenza di dare al diritto all'oblio un riconoscimento normativo e di individuare specifici criteri di bilanciamento, essendo l'approccio *case by case*

proposto dalla Corte di non semplice attuazione e non corrispondente ai principi di certezza ed uniformità del diritto.

## **2. Dalla giurisprudenza della Corte di giustizia europea alla legislazione del Parlamento europeo**

La recente giurisprudenza della Corte di Giustizia in materia di protezione di dati personali influenzerà senza ombra di dubbio il Regolamento europeo di prossima approvazione. In particolare ci riferiamo alle pronunce della Grande Sezione, tra le quali ne spiccano tre di importanza decisiva. Oltre alla già ampiamente analizzata sentenza *Google Spain*, è opportuno accennare alla sentenza dell'8 aprile 2014 sulla cosiddetta *data retention* ed alla recentissima sentenza del 6 ottobre 2015. Sono sentenze che hanno segnato un rafforzamento del diritto alla riservatezza e alla protezione dei dati personali, a danno però di altri importanti interessi.

Nella sentenza sulla *data retention* la Corte ha invalidato la Direttiva 2006/64, in quanto ritenuta non compatibile con i limiti imposti dal principio di proporzionalità, alla luce degli artt. 7, 8 e 52 della Carta di Nizza. Dunque la Direttiva 2006/64 sulla *data retention* è stata ritenuta contraria ad alcuni diritti fondamentali, quali i già richiamati diritti ex artt. 7 e 8, e al principio di proporzionalità ex art. 52 par. 1<sup>49</sup>. La direttiva in questione richiedeva l'applicazione degli obblighi di conservazione di tutti i dati di traffico connessi a qualsiasi mezzo comunicativo, con la finalità di accertamento e prevenzione dei reati. Questi obblighi, dunque, riguardavano l'archiviazione di dati relativi, in modo generalizzato, a tutti gli utenti e a tutti i mezzi di comunicazione elettronica, quindi anche i dati riguardanti persone nemmeno indirettamente coinvolte o collegate a procedimenti penali o reati gravi. Inoltre, la Direttiva non prevedeva nessuna

---

<sup>49</sup> <<Eventuali limitazioni all'esercizio dei diritti e delle libertà riconosciuti dalla presente Carta devono essere previste dalla legge e rispettare il contenuto essenziale di detti diritti e libertà. Nel rispetto del principio di proporzionalità, possono essere apportate limitazioni solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui. >>

eccezione, con la conseguenza che veniva applicata anche a quei soggetti le cui comunicazioni erano protette, in base al diritto nazionale, dal segreto professionale. La Direttiva non prevedeva neppure alcun limite oggettivo per l'accesso ai dati da parte delle autorità nazionali competenti e per il successivo utilizzo ai fini di prevenzione e accertamento di reati che fossero di una gravità tale da giustificare una restrizione dei diritti di cui agli artt. 7 e 8 della Carta. Al contrario, essa faceva riferimento, in modo generale, a "gravi reati", in base a come erano "definiti negli Stati membri" e non prevedeva che l'accesso ai dati avvenisse dopo l'esame di un giudice o di un'autorità amministrativa indipendente che potesse limitare l'accesso e l'utilizzo di tali dati ai soli casi di assoluta necessità. Le criticità della Direttiva consisterebbero soprattutto nella difficoltà di individuazione dei "gravi reati" e nella mancata definizione di presupposti oggettivi che possano giustificare la *data retention*. L'epocale sentenza della Corte si scontra con la complessità dell'attuale società dell'informazione, governata dalla rivoluzione informatica e dall'evoluzione tecnologica, che hanno trasformato i dati e le informazioni in beni immateriali di inestimabile valore. Tuttavia, nell'attuale assetto socio-economico l'utilizzo degli strumenti tecnologici a nostra disposizione può risultare indispensabile per accertare o prevenire gravi reati lesivi di altrettanti importanti beni giuridici. Gli stessi Stati membri hanno affermato che la conservazione dei dati è in alcuni casi indispensabile per prevenire e contrastare la criminalità, compresa la protezione delle vittime e l'assoluzione degli imputati innocenti. Nella delicata operazione di bilanciamento, il diritto all'oblio viene quindi ad essere ponderato anche rispetto ad un altro interesse generale, ossia quello relativo all'accertamento e alla prevenzione di gravi reati. I principi espressi dalla Corte di Giustizia in quest'ultimo caso e nel caso *Google Spain*, devono essere letti congiuntamente, nel tentativo di elaborare dei criteri di bilanciamento e di definire i possibili limiti al diritto dell'interessato di ottenere la cancellazione delle informazioni che lo riguardano.

Un'altra importante sentenza della Corte è quella dello scorso ottobre, in cui è stata dichiarata invalida la decisione della Commissione europea attestante che gli Stati Uniti garantiscono un adeguato livello di protezione dei dati personali trasferiti. La Direttiva europea sul trattamento dei dati personali dispone che il trasferimento di tali dati verso un Paese terzo può avere luogo solo se nel Paese terzo si garantisca un adeguato livello

di protezione. Il caso di specie riguarda un cittadino che utilizza Facebook ed i cui dati, in quanto utente registrato del *social network*, sono trasferiti dalla filiale irlandese di Facebook, su *server* situati negli USA, dove sono oggetto di trattamento. Il ricorrente ha presentato denuncia all'autorità irlandese di controllo ritenendo che, alla luce delle rivelazioni fatte nel 2013 da Snowden, il diritto statunitense non offra una tutela adeguata contro la sorveglianza delle autorità pubbliche sui dati trasferiti in tale Paese. L'autorità irlandese, tuttavia, ha respinto la denuncia, segnalando che la Commissione, nella decisione del 26 luglio 2002, ha ritenuto che gli Stati Uniti garantiscano un livello adeguato di protezione dei dati personali trasferiti. La *High Court of Ireland*, investita della causa, si è rivolta alla Corte di giustizia europea, la quale ha considerato che anche quando esiste una decisione della Commissione, le autorità nazionali di controllo, investite di una domanda, devono poter esaminare in piena indipendenza se il trasferimento dei dati personali verso un Paese terzo rispetti i requisiti stabiliti dalla Direttiva<sup>50</sup>.

Ciò che ci interessa di questa sentenza è il fatto oggetto di giudizio, in quanto manifesta le evidenti divergenze tra il trattamento dei dati personali in Europa e negli Stati Uniti, soprattutto in seguito alle rivelazioni dell'ufficiale NSA. La questione concernente i rapporti USA/UE rappresenta un'altra sfida che il futuro Regolamento sarà chiamato a risolvere.

Dal caso *Google Spain* è possibile indagare le implicazioni della pronuncia sugli scenari futuri e sembra opportuno collocare la decisione in un più ampio contesto che comprenda anche le altre due sentenze appena analizzate. Ciò che emerge è un'ondata inversa rispetto all'orientamento che ha caratterizzato l'ultimo decennio. Le estese raccolte di dati, gli obblighi di conservazione dei dati nel tempo, nonché i poteri di indagine e di accesso in capo alle autorità pubbliche, hanno creato un contesto in cui i cittadini hanno perso la percezione del confine tra la raccolta dei propri dati per finalità commerciale e il loro riutilizzo per finalità di controllo e monitoraggio sociale. A questa strategia hanno partecipato anche le imprese private, ai cui ricchi data-base i governi

---

<sup>50</sup> Nello specifico, la Corte ha ritenuto che una decisione adottata dalla Commissione <<non osta a che un'autorità di controllo di uno Stato membro (...) esamini la domanda di una persona relativa alla protezione dei suoi diritti e delle sue libertà con riguardo al trattamento dei dati personali che la riguardano, i quali sono stati trasferiti da uno Stato membro verso tale paese terzo, qualora tale persona faccia valere che il diritto e la prassi in vigore in quest'ultimo non garantiscono un livello di protezione adeguato>>.

potevano accedere all'insaputa degli interessati e della collettività generale. Ecco come l'interesse del singolo ad ottenere la cancellazione dei propri dati si pone in un'ottica più ampia, rivelandosi come interesse generale della popolazione che reagisce all'eccessiva raccolta di dati personali.

Il nuovo Regolamento europeo sarà in particolare chiamato a concentrarsi sul diritto all'oblio e sui temi connessi, emersi dalle recenti pronunce della Corte di Giustizia dell'Unione Europea. Si tratta di profili controversi per via delle evidenti implicazioni e ricadute sui modelli di *business* adottati da alcune imprese, tra le maggiori operanti nel mercato digitale. Sembrerebbe dunque che siano i modelli di *business* a doversi adeguare al rispetto dei diritti fondamentali e non viceversa. Un difficile contemperamento di interessi di cui attendiamo di conoscerne la precisa regolamentazione.

### **3. Il futuro Regolamento europeo**

La Corte Di Giustizia Europea, chiamata a pronunciarsi su temi alla base della moderna società digitale, quali l'efficacia temporale delle norme in materia di protezione dei dati personali, il ruolo rivestito dai motori di ricerca nel trattamento delle informazioni ed il difficile rapporto tra diritto di accesso alle informazioni e diritto all'oblio nella realtà digitale, ha dimostrato di voler dare alla sua decisione una valenza politica e le carenze, soprattutto in merito al diritto all'oblio, evidenziano l'esigenza di un fermo intervento normativo. Due sono gli aspetti fondamentali della sentenza precedentemente analizzata a costituire, anche, i punti centrali della proposta di Regolamento comunitario<sup>51</sup> in materia di tutela dei dati personali, ormai entrata nella fase finale del proprio *iter*.

Il nuovo Regolamento europeo consentirà l'aggiornamento e l'armonizzazione della disciplina sulla protezione dei dati personali e, considerando che si tratta di una fonte regolamentare, sarà applicabile a tutti gli Stati membri in maniera uniforme.

---

<sup>51</sup> Proposal for a regulation of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final, Brussels, 25/01/2012.

### 3.1. La proposta di Regolamento

La direttiva 95/46/CE, pietra angolare nell'impianto della vigente normativa europea in materia di protezione dei dati personali, è stata adottata nel 1995 con due obiettivi: salvaguardare il diritto fondamentale alla protezione dei dati e garantire la libera circolazione dei dati personali tra gli Stati membri. Il Consiglio europeo ha invitato la Commissione a valutare il funzionamento degli strumenti giuridici dell'Unione in materia di protezione dei dati e a presentare, se necessario, nuove iniziative legislative. La Commissione ha sottolineato la necessità di assicurare l'applicazione sistematica del diritto fondamentale alla protezione dei dati personali nel contesto di tutte le politiche europee. Il piano d'azione della Commissione ha evidenziato che: *<<in una società globalizzata, caratterizzata da un rapido progresso tecnologico in cui lo scambio d'informazioni non conosce confini, è quanto mai importante garantire il rispetto della vita privata. L'Unione deve assicurare l'applicazione sistematica del diritto fondamentale alla protezione dei dati. Occorre rafforzare la posizione dell'UE in relazione alla protezione dei dati personali in tutte le politiche europee, anche nel contrastare e prevenire la criminalità e nelle relazioni internazionali>>*. La Commissione, dunque, è giunta alla conclusione che l'Unione europea ha bisogno di una politica più completa e coerente rispetto al diritto fondamentale alla protezione dei dati personali.

L'evoluzione tecnologica e delle modalità di raccolta e trattamento dei dati, nonché le divergenze tra i vari Stati membri nell'attuazione della direttiva del 1995 sui dati personali, hanno fatto emergere un'esigenza di riforma, della quale il nuovo Regolamento europeo è espressione. Tale Regolamento, di vicinissima approvazione e attuazione, abrogherà la Direttiva 95/46 in materia di protezione dei dati personali e sostituirà anche il "Codice della privacy" che ha recepito, nel nostro ordinamento, la Direttiva in questione. Sono stati delineati alcuni profili che necessitano di regolamentazione e che il Codice della privacy, risalente a più di un decennio fa, non avrebbe mai potuto considerare, in quanto all'epoca tali ambiti erano ancora sconosciuti.

Il primo punto riguarda l'affermarsi di una normativa che vada di pari passo con l'evoluzione tecnologica, considerando che l'avanzare della tecnologia ha reso obsolete

alcune modalità di raccolta, trattamento e utilizzo dei dati, richiedendone la sostituzione con altre di nuova generazione. La seconda questione, ma non meno importante, è quella che riguarda la tutela del diritto all'oblio e le inevitabili ripercussioni sulla libertà di espressione e il diritto di cronaca, di cui abbiamo già ampiamente discusso. Il bilanciamento che di volta in volta si deve raggiungere non può essere discrezionale, ma deve basarsi su precisi criteri predeterminati, quali ad esempio l'assenza di interesse pubblico all'acquisizione della notizia e la non attualità della stessa. Appare evidente il motivo per cui proprio sull'art. 17 della proposta di Regolamento, che riguarda il diritto alla cancellazione dei dati personali, originariamente rubricato "*right to be forgotten*", si siano concentrate le principali critiche e le *lobby* abbiano esercitato una forte azione di contrasto. Tuttavia, la proposta di Regolamento prevede specifiche limitazioni al diritto all'oblio e alla cancellazione dei dati, fornendo una base giuridica per il bilanciamento fra contrapposte esigenze. L'art. 21, infatti, dispone che l'Unione o gli Stati membri possono limitare la portata di tale diritto qualora ciò costituisca una misura necessaria e proporzionata volta a salvaguardare: *a)* la pubblica sicurezza; *b)* le attività volte a prevenire, indagare, accertare e perseguire reati; *c)* altri interessi pubblici dell'Unione o di uno Stato membro, in particolare un rilevante interesse economico o finanziario dell'Unione o di uno Stato membro, anche in materia monetaria, di bilancio e tributaria, e la stabilità e l'integrità del mercato; *d)* le attività volte a prevenire, indagare, accertare e perseguire violazioni della deontologia delle professioni regolamentate; *e)* una funzione di controllo, d'ispezione o di regolamentazione connessa, anche occasionalmente, all'esercizio di pubblici poteri nei casi di cui alle lett. *a)*, *b)*, *c)*, e *d)*, *f)* la tutela dell'interessato o dei diritti e delle libertà altrui. La questione più delicata riguarda l'individuazione del soggetto deputato ad operare il bilanciamento fra le diverse esigenze: tutela della riservatezza da un lato e, dall'altro, esigenze di giustizia penale, tutela della sicurezza pubblica o della libertà di espressione. L'art. 12 della proposta di regolamento fa incombere sul responsabile del trattamento l'obbligo di stabilire le procedure per l'esercizio dei diritti dell'interessato, fra i quali l'obbligo di informazione a tale soggetto, tempestivamente e, comunque, entro un mese qualora sia stata intrapresa un'azione. Se il responsabile rifiuta di ottemperare alla richiesta dell'interessato, deve informarlo dei motivi e delle possibilità di proporre reclamo all'autorità di controllo o anche ricorso giurisdizionale. È noto che nella maggior parte

dei casi il fornitore di servizi è un soggetto privato che esercita le libertà connesse all'esercizio di impresa. Egli dovrebbe dimostrare, in caso di rifiuto, non solo che i suoi legittimi interessi possono prevalere sull'interesse o sui diritti e sulle libertà fondamentali dell'interessato, ma anche che la richiesta non possa essere accolta per una delle esigenze ex art.17. La proposta di regolamento, tuttavia, prevede, all'art. 79, specifiche sanzioni amministrative nel caso in cui il responsabile non rispetti il diritto all'oblio o alla cancellazione, ometta di predisporre meccanismi che garantiscano il rispetto dei termini o non prenda tutte le misure necessarie per informare i terzi della richiesta dell'interessato di cancellare tutti i link verso i dati personali. Il legislatore europeo dovrà poi fare i conti col fenomeno sempre più attuale e moderno dei Big Data<sup>52</sup>, che consentono di ottenere profilazioni dettagliate lesive del diritto alla riservatezza degli interessati, le cui abitudini e i cui comportamenti saranno carpiri per diverse finalità, come quella di influenzare le loro scelte. Inoltre, grazie alle nuove tecniche di re-identificazione, le loro potenzialità non si esplicano solo nei confronti di dati idonei ad identificare una persona, ma anche con riferimento a dati anonimi. Per non parlare poi della diffusione dei *social network*, cui sono connessi rischi per la *privacy* ampiamente noti a tutti. Il Garante europeo ha, infatti, più volte sottolineato l'importanza di sensibilizzare gli utenti sull'utilizzo dei *social network*, poiché non esiste una separazione netta tra vita reale e vita digitale e spesso ciò che accade su Facebook si ripercuote sulla reputazione, sull'identità e sulle relazioni personali e non virtuali del soggetto<sup>53</sup>. Inoltre i dati, una volta immessi, sfuggono dal controllo dell'interessato ed è quasi sempre impossibile ottenerne una cancellazione definitiva, in quanto rimarranno comunque conservati nei *server* dell'azienda che offre il servizio. I dati immessi in un *social network*, possono allo stesso modo essere trattati per finalità commerciali, di *marketing* e profilazione e ai rischi di violazione della *privacy* si aggiungono le ipotesi di furto d'identità o di risalimento a *password* o credenziali dell'utente. Ci spostiamo in questo caso nel vasto ambito della criminalità informatica di cui il *cyber* spazio, connotato da vastità e mancanza di regole e di controllo, costituisce terreno fertile. A questo complesso panorama va ad aggiungersi un ulteriore fattore di non scarsa rilevanza, ossia il fatto che le regole previste per la protezione dei

---

<sup>52</sup> Cfr. nota 38

<sup>53</sup> Cfr. cap. 4



dati personali in Europa non sono uguali a quelle vigenti in altri Paesi. In Europa il diritto alla protezione dei dati personali è sancito come diritto fondamentale dell'individuo, dunque il rispetto della sfera di riservatezza del soggetto è avvertito in modo stringente rispetto a quanto accade in altri Stati. Sorge, pertanto, un notevole problema nel momento in cui la sede principale del titolare del trattamento risulti situata in Stati che non prevedono una disciplina altrettanto garantista. Il Regolamento, allora, conterrà una clausola in virtù della quale si ovvierà all'applicazione di due normative differenti, stabilendo un'unica disciplina cui dovrà sottostare qualsiasi soggetto che offra i propri servizi ai cittadini dell'Unione Europea, anche se stabilito nel territorio di un Paese terzo. Sarà inoltre introdotta una nuova figura, ossia quella del *Data Protection Officer* (Responsabile della protezione dei dati personali), il quale avrà il compito di informare, sorvegliare e controllare gli adempimenti che la normativa impone e la corretta osservanza delle disposizioni della stessa.

### **3.2. I principali punti approvati dal Parlamento europeo**

La proposta di Regolamento è stata presentata il 25 gennaio 2012 ed il Parlamento si è espresso su di essa in prima lettura il 12 marzo 2014<sup>54</sup>. Il Parlamento europeo ha adottato, con 621 voti a favore, una risoluzione legislativa riguardo la proposta di Regolamento in materia di protezione dei dati personali e di libero spostamento di tali dati (*General Data Protection Regulation*). Analizziamo brevemente le posizioni del Parlamento in prima lettura riguardo i principali temi contenuti nella proposta.

- Campo di applicazione territoriale: il Regolamento si applica indipendentemente dal luogo in cui il trattamento dei dati si svolge, a nulla rilevando se l'operazione ha luogo nell'Unione o al di fuori dell'Unione. Esso, dunque, si applica sempre in caso di trattamento di dati personali riguardanti un soggetto dell'Unione, anche laddove il responsabile del trattamento non sia stabilito in uno degli Stati membri.

---

<sup>54</sup> 2012/0011 (COD)- 12/03/2014 Text adopted by Parliament, 1st reading.

- Principi generali concernenti l'attività di trattamento dei dati: il trattamento deve conformarsi ai principi di correttezza, liceità e trasparenza; deve essere prevista una limitazione delle finalità di trattamento (i dati non possono essere utilizzati e trattati per finalità plurime e/o indeterminate); è necessaria inoltre la minimizzazione dei dati (i dati devono essere trattati nei limiti di necessità e indispensabilità) e la precisione; deve essere garantita l'integrità e protezione dei dati personali da trattamenti illeciti e non autorizzati, da perdita accidentale degli stessi o, ancora, da distruzione o danneggiamento, attraverso tecniche appropriate e misure di sicurezza; infine vige il principio di responsabilità di chi si occupa del trattamento.
- Condizioni del consenso: l'interessato deve essere informato sull'esistenza dell'operazione di trattamento e sulle finalità della stessa; deve essere inoltre informato sul periodo di tempo in cui i suoi dati saranno oggetto di trattamento, in base alla specifica finalità e se i dati saranno trasferiti a terze persone o a Stati terzi. Il Parlamento conferma che il responsabile del trattamento ha l'onere di provare che il soggetto abbia prestato il consenso all'operazione di trattamento. Previsioni sul consenso dell'interessato che violano anche solo parzialmente il Regolamento sono completamente vietate. Ritirare il consenso deve essere semplice, così come è semplice darlo. L'interessato deve essere informato se, ritirando il proprio consenso, avrà come conseguenza l'interruzione della fornitura del servizio o del rapporto obbligatorio con il responsabile del trattamento. Il consenso deve essere limitato alle finalità del trattamento dichiarate e non è più valido quando la finalità di trattamento dei dati originariamente dichiarata cessa di esistere o se il periodo di trattamento dei dati personali è eccessivamente lungo e non proporzionato rispetto alle finalità per cui i dati sono stati originariamente raccolti.
- Casi di divieto di trattamento: è vietato il trattamento di dati personali riguardanti razza, origini etniche, opinioni politiche, credo filosofico o religioso, orientamento sessuale, appartenenza sindacale e attività sindacali; è proibito, inoltre, il trattamento di dati genetici o concernenti la salute o la vita sessuale, sanzioni amministrative, sentenze, reati, condanne o misure di sicurezza.
- Diritti dell'interessato: l'interessato deve poter ottenere chiare e semplici

informazioni riguardanti il trattamento dei propri dati. È, inoltre, titolare di una serie di diritti sui propri dati personali; diritto di accesso, rettifica e cancellazione degli stessi; diritto di acquisire i dati; diritto di opporsi alla profilazione; diritto di presentare reclamo all'autorità competente e di agire per via legale; diritto al risarcimento dei danni risultanti da un'illecita operazione di trattamento.

- Diritto alla cancellazione dei dati: gli Stati membri hanno l'obbligo di garantire che l'interessato ottenga la cancellazione dei link che conducono ai propri dati personali, laddove intervenga un ordine di rimozione da parte di un'autorità giudiziaria o di regolamentazione, oppure laddove i dati siano stati trattati con modalità non lecite.
- Profilazione: il Parlamento ha chiarito che ogni persona ha il diritto di opporsi alla profilazione e l'interessato deve essere informato in modo chiaro ed evidente di tale diritto. La profilazione che ha l'effetto di discriminare gli individui per ragioni di razza, etnia, credo politico, filosofico o religioso, orientamento sessuale è assolutamente vietata.
- Trasferimento o divulgazione di dati non autorizzati dalla legge dell'Unione: un nuovo articolo prevede che nessuna sentenza di una corte o tribunale e nessuna decisione di un'autorità amministrativa di un Paese terzo, che richieda al responsabile del trattamento di rivelare dati personali, possa essere riconosciuta o eseguita senza pregiudizio per gli accordi internazionali.
- Sanzioni amministrative: a chiunque non osservi le disposizioni previste dal Regolamento, l'autorità di controllo deve imporre una sanzione amministrativa.

Il Regolamento dovrebbe essere approvato nei prossimi mesi. Diversi Stati membri hanno opinioni contrastanti in merito ad esso: alcuni vogliono raggiungere presto un accordo (ad esempio, Francia, Italia e Spagna), altri sono completamente contrari (come Danimarca, Svezia e Regno Unito), mentre un terzo gruppo sta nel mezzo e rimane neutrale. La posizione assunta dalla Germania sarà fondamentale per decidere quella dell'intero Consiglio. Attualmente la discussione è ancora in corso e si sta svolgendo un negoziato informale tra Commissione, Parlamento e Consiglio che dovrebbe portare al raggiungimento di un compromesso e all'adozione di un testo comune sotto la presidenza lussemburghese.

### 3.3.Criticità e riflessioni

Anche il nuovo Regolamento ormai da alcuni anni all'esame delle istituzioni europee, sembra non essere destinato a risolvere tutti i problemi. Pur essendo stato modificato il titolo dell'art. 17 da "diritto all'oblio" in "diritto alla cancellazione dei dati personali" e pur considerando che la tutela garantita è certamente ampliata rispetto alla precedente Direttiva, tuttavia si continua a non distinguere adeguatamente tra la natura dei dati personali raccolti e postati in rete sui siti sorgente che li contengono e li trattano per finalità specifiche, e la natura dei dati personali trattati da motori di ricerca e da questi indicizzati. I dati personali indicizzati dai motori di ricerca o diffusi secondo le modalità proprie dei *social network* sono oggetto di una tipologia di trattamento differenziato e creano problemi nuovi e diversi da quelli tradizionali. In questo senso, anche la normativa del Regolamento europeo, pur attenta, per quanto possibile, a calare la tutela dei dati personali nel nuovo contesto del *web*, resta abbastanza insoddisfacente. Per far sì che il Regolamento non nasca già superato dall'evoluzione dei *social*, dovrebbe essere chiaro a tutti che non si possono applicare le medesime regole a tutti i trattamenti di dati, come se ci trovassimo di fronte a medesime tipologie di trattamento, e che le distinzioni che il Regolamento introduce nel rivisitato art. 17 non sono sufficienti. Inoltre sarebbe opportuno rendere il Regolamento più flessibile ed aperto ad auspicabili attività regolatorie internazionali. Il rischio, infatti, è che il Regolamento nasca troppo dominato dall'idea di una fortificazione chiusa, con pochi e limitati ponti levatoi, eretta a difesa di una sola regione, l'Europa, in un mondo sempre più globalizzato (F. Pizzetti). Il diritto alla protezione dei dati personali è stato preso talmente sul serio da trascurare le conseguenze negative che un approccio così "dato-centrico", seppur comprensibilmente dettato dallo scandalo mondiale seguito alle rivelazioni sulle intercettazioni da parte della NSA, rischia di avere sul delicato equilibrio alla base del *web*. Oltre alla già più volte ricordata esigenza di tutelare la libertà di espressione che rischia di essere soverchiata da un <<*digital right to privacy*>> preso troppo sul serio (O. Pollicino), c'è il rischio che si attivi un processo di ipereuropeizzazione. Infatti, la legge applicabile qualora l'interessato sia un cittadino europeo sarà il Regolamento europeo. In questo modo si viene a costruire una fortezza continentale posta a presidio dei dati personali dei residenti in Europa, ma che resta ancorata alla sola Europa, non garantendo effettività della tutela a livello extra-europeo: i dati personali di cui si ottiene

la rimozione in base alla normativa europea continueranno ad essere visibili al di fuori dell'Unione. Un'ulteriore criticità del futuro Regolamento è legata al fatto che esso si riferisce a tutti i tipi di dati, mentre si dovrebbe assicurare che la regolamentazione sull'utilizzo dei dati sia proporzionale alla sensibilità degli stessi e rifiutare un approccio unico alla protezione dei dati. La definizione data dal Regolamento distingue tra "dati personali" ordinari e "categorie speciali di dati personali" sensibili, prevedendo regole più severe per il trattamento di questi ultimi. Lo stesso principio dovrebbe valere anche al contrario, si dovrebbe cioè facilitare il trattamento di quei dati personali meno sensibili che non permettono di identificare un individuo. A tal fine, il Regolamento generale sulla protezione dei dati dovrebbe adottare un approccio al trattamento dei dati personali basato sul rischio, concentrando l'esame e l'applicazione delle previsioni del Regolamento solo sul trattamento di dati che espone l'interessato a un rischio significativo e prevedendo regole chiare e diversificate nel caso di trattamento di dati personali meno sensibili, come era stato proposto inizialmente dal Parlamento europeo. A questo scopo, il Regolamento potrebbe prevedere incentivi sia per la pseudonimizzazione<sup>55</sup> dei dati personali sia per il trattamento di dati pseudonimizzati. Si potrebbe, infatti, promuovere la minimizzazione dei dati incentivando la pseudonimizzazione e altre tecniche che rafforzano la tutela della privacy, concedendo un trattamento privilegiato al trattamento dei dati che non permettono di identificare direttamente i singoli individui. I dati personali sottoposti alla pseudonimizzazione non permettono l'identificazione diretta di una persona fisica senza l'utilizzo di informazioni aggiuntive e forniscono ulteriori garanzie ai soggetti interessati; pertanto, il trattamento di dati pseudonimizzati è molto più riguardoso nei confronti della privacy rispetto al trattamento dei dati personali ordinari. Al contempo, un trattamento di questo genere rappresenta un tassello fondamentale dell'odierno ecosistema pubblicitario digitale, in quanto permette alle aziende di personalizzare l'esperienza degli utenti in una maniera rispettosa della vita privata. Questa personalizzazione è uno strumento fondamentale per proporre offerte online che siano d'interesse per l'utente, per attrarre nuovi clienti, differenziare i servizi e mantenere la capacità di essere competitivi sul mercato. Sarebbe possibile anche collegare la pseudonimizzazione dei dati personali a un fondamento

---

<sup>55</sup> L'uso di uno pseudonimo permette di sostituire l'insieme dei dati identificativi con un appellativo neutro (lo pseudonimo, appunto), in modo che sia resa molto difficile l'identificazione del soggetto interessato.

giuridico per il trattamento, come per esempio il legittimo interesse del responsabile del trattamento. Il Regolamento, inoltre, potrebbe assicurare la possibilità di continuare a concedere il proprio consenso in maniera flessibile, a seconda del contesto in cui questo viene dato, e rifiutare un sistema di consenso rigido che non si adatti alle circostanze di un'interazione. L'attuale modello di "consenso inequivocabile" richiede un'espressione chiara e certa del consenso per mezzo di qualsiasi metodo adeguato e prevede requisiti più rigidi in talune circostanze, come nel caso di trattamento di dati personali sensibili. Tale meccanismo permette al consenso di adattarsi con flessibilità a varie circostanze, concedendo ai singoli individui la possibilità di acconsentire al trattamento dei propri dati nella maniera più appropriata. Pertanto, l'attuale modello del "consenso inequivocabile" dovrebbe essere confermato anche nel futuro Regolamento. L'idea del Parlamento europeo di richiedere il consenso esplicito, senza flessibilità alcuna rispetto alla modalità di espressione dello stesso, è adeguata solo nel caso del trattamento di dati ad alto rischio. Inoltre, trattare i dati più sensibili esattamente allo stesso modo dei dati non sensibili non accrescerebbe il livello di protezione degli utenti. Gli utenti verrebbero infatti bombardati dalle richieste di consenso e, potenzialmente, potrebbero sviluppare l'abitudine di dare il proprio consenso a prescindere, il che configurerebbe un caso di consenso esplicito, ma non significativo. Molte aziende europee non hanno un rapporto diretto con i consumatori e, di conseguenza, non possono richiederne il consenso. Si dovrebbe quindi continuare a permettere il trattamento dei dati personali a fini commerciali non basato sul consenso, sulla base del legittimo interesse del responsabile del trattamento. Il Regolamento non dovrebbe essere discriminatorio nei confronti dei modelli di business B2B<sup>56</sup>. Nel quadro attuale, le aziende che non hanno un rapporto diretto con il soggetto interessato e che quindi non possono ottenerne il consenso, godono comunque del diritto al trattamento dei dati personali se hanno un legittimo interesse a farlo e se l'interesse del soggetto titolare dei dati personali non è prevalente. È necessario assicurare che il Regolamento faccia riferimento agli interessi commerciali, quale il marketing, come interesse legittimo, come già avviene nell'attuale quadro giuridico sulla protezione dei dati e come è stato proposto dal Consiglio. Al

---

<sup>56</sup> Modello Business to Business: espressione utilizzata per descrivere le transazioni commerciali elettroniche tra imprese, in opposizione a quelle che intercorrono tra impresa e consumatore (B2C) o impresa e Governo (B2G). Generalmente ci si riferisce a quelle transazioni che vengono effettuate in una catena di valore industriale, prima che il prodotto finito venga venduto al consumatore.

contempo, la proposta del Parlamento europeo di subordinare l'utilizzo di questa base giuridica per il trattamento alle ragionevoli aspettative del soggetto interessato sulla base della relazione con il responsabile del trattamento deve essere rigettata in quanto priverebbe le aziende che operano in modalità B2B di qualsiasi strumento per continuare a trattare i dati in maniera legale. Il Regolamento dovrebbe, inoltre, evitare sistemi di profilazione eccessivamente restrittivi, concentrandosi sulla tutela degli utenti da una profilazione che produca effetti giuridici o effetti nocivi per l'individuo e permettendo, invece, la profilazione non lesiva e portatrice di potenziali benefici.

Il Regolamento ha lo scopo di tutelare gli interessi, i diritti e le libertà fondamentali delle persone fisiche e non deve trasformarsi in uno strumento che proibisca le tecnologie che rafforzano la tutela della privacy o i metodi innovativi per il trattamento dei dati.

#### **4. Il Regolamento europeo e la posizione delle grandi aziende di comunicazione elettronica**

La proposta della Commissione per un Regolamento Generale sulla Protezione dei Dati Personali ha suscitato ampie discussioni tra l'Unione da un lato e le imprese di Internet e il governo statunitense dall'altro. Alcuni aspetti del Regolamento rispondono alle esigenze delle imprese globali di Internet: la sostituzione di un'unica normativa europea alle diverse discipline nazionali oggi esistenti; l'indicazione di un'unica autorità per la protezione dei dati quale soggetto competente per tutte le questioni concernenti un certo titolare, ossia quella dove è stabilito il titolare stesso; la creazione di un organo di appello per assicurare la coerenza tra le decisioni nazionali; l'esplicita estensione delle immunità dei *provider* anche alle violazioni della protezione dei dati. Adottando il modello tipicamente statunitense dell'autoregolamentazione, il Parlamento europeo ha introdotto nella bozza predisposta dalla Commissione il sigillo europeo per la protezione dei dati, rilasciato dalle autorità di protezione dei dati per garantire che il titolare o il responsabile è in conformità al Regolamento. Il sigillo limita la responsabilità amministrativa dei gestori, e consente loro di trasferire dati all'estero senza dover ottenere volta per volta l'autorizzazione delle autorità di protezione dei dati.

Altri aspetti del regolamento, invece, hanno incontrato l'opposizione delle imprese e del governo statunitensi, come la potenziale applicabilità della normativa europea a ogni trattamento che coinvolga interessati situati in Europa, anche quando il sito che esegue il trattamento non abbia specifica destinazione europea. Il tema più controverso è stato però quello del diritto all'oblio; infatti gli osservatori statunitensi hanno immediatamente identificato il conflitto con la libertà di espressione e di informazione. Secondo l'opinione prevalente negli Stati Uniti, l'affermazione di un diritto dell'interessato alla rimozione delle informazioni che lo riguardano metterebbe a rischio le libertà altrui, e in particolare le libertà di esprimere opinioni su terzi, di comunicare informazioni, e di accedere alle stesse. Le potenzialità censorie di tale diritto erano addirittura assimilate agli interventi su Internet attuati da regimi oppressivi, come la Cina e alcuni governi del Medio Oriente, e si affermava che la disciplina del "diritto ad essere dimenticati", imponendo a Google di rispondere alle richieste di rimozione, avrebbe trasformato Google stessa in un riluttante «censore capo per l'Unione europea<sup>57</sup>». Il Parlamento, eliminando il riferimento a un «*right to be forgotten*», sostituito dal richiamo al diritto alla cancellazione (*erasure*), avrebbe introdotto altresì tra le condizioni per la cancellazione la presenza di una decisione «*final and absolute*» di una «*court or regulatory authority*», suggerendo forse come il giudizio di illegittimità, presupposto per la cancellazione, dovrebbe essere affidato ad autorità pubbliche competenti, piuttosto che agli intermediari. Questo apparente avvicinamento tra posizioni europee e statunitensi sulla rimozione di informazioni da Internet è stato però interrotto dalla decisione della Corte di Giustizia sul caso *Google-Spain*, che conferisce all'interessato il diritto rimozione di *link* a notizie legittimamente pubblicate e distribuite in rete, esercitabile direttamente nei confronti dei motori di ricerca. Questi sono ritenuti responsabili per l'accessibilità di tali notizie, ogni qualvolta la *privacy*, nel corso del tempo, sia divenuta prevalente rispetto alla libertà di espressione, essendo diminuito l'interesse pubblico alla conoscenza delle stesse notizie. Il Regolamento sembra essere stato pensato proprio per garantire la centralità della protezione dei dati personali e per sfuggire alle pressioni lobbistiche delle grandi aziende che operano nel settore. La finalità, seppur nobile, di protezione dei diritti della personalità cela

---

<sup>57</sup> J.Rosen, *The right to be forgotten* (2012). *Stanford Law Review Online*, pp. 64:88-92.



probabilmente l'intento di contrastare chi trae profitto dalla raccolta e dal trattamento dei dati personali. Forse per comprendere le motivazioni per cui le grandi aziende delle comunicazioni elettroniche si oppongono a un così rigido e dato-centrico Regolamento, dovremmo abbandonare le paure orwelliane di monitoraggio sociale e la fanatica visione di un *Big Google* nelle vesti di *Big Brother*. Forse queste grandi aziende sono solo dei semplici intermediari che forniscono notizie e informazioni a chi le richieda, siano essi utenti, governi, servizi di sicurezza. Il problema di fondo non è contrastare l'attività di aziende che si qualifica come legittima attività d'impresa con finalità economiche e commerciali altrettanto legittime, ma il potere di chi sfrutta tale attività per finalità sicuramente non commerciali.

## CAPITOLO III

### **Dall'identità personale all'identità virtuale: profili giuridici, filosofici e sociologici.**

Il diritto alla protezione dei dati personali va collocato nell'ambito dei diritti della personalità. Si tratta di una categoria aperta di diritti caratterizzati dall'essere assoluti, indisponibili ed imprescrittibili, suscettibili di ampliamento normativo e giurisprudenziale. La giurisprudenza creatrice, in questa materia, si è data molto da fare, muovendo dall'elaborazione del diritto alla riservatezza fino al diritto all'identità personale. Il diritto alla protezione dei dati, a differenza del diritto all'identità personale, è un diritto al controllo sui dati, non sull'immagine sociale; dunque consiste in un controllo positivo, non in senso negativo, ossia come diritto di escludere. Il fondamento costituzionale del diritto alla protezione dei dati personali e degli altri diritti della personalità è dato dall'art. 2 della Costituzione, clausola generale ed aperta di tutela del libero ed integrale svolgimento della persona umana<sup>58</sup>. Il diritto alla protezione dei dati personali e i diritti della personalità ad esso limitrofi, quali il diritto all'identità personale, il diritto alla riservatezza, il diritto alla reputazione, il diritto all'immagine e il diritto al nome, sono tutti finalizzati alla tutela di un unico bene giuridico: l'identità. Essa viene vista nelle sue molteplici forme ed espressioni e può riguardare le informazioni concernenti un soggetto, la sua immagine sociale, la sua immagine sulla stampa e attraverso i *mass media*, la sua immagine fisica, il suo nome. Il bene giuridico complessivamente tutelato è unicamente quello dell'identità, declinata nei suoi molteplici aspetti e forme. Oggi, un ulteriore elemento di complessità è aggiunto dalla possibilità concessa all'individuo di esplicitare la sua personalità e la sua identità anche attraverso i mezzi digitali e di assumere, nel mondo virtuale, molteplici identità. Ci sono casi in cui il soggetto crea personalmente e consapevolmente una propria identità sulla rete, altri casi in cui, all'insaputa dell'interessato, è la rete stessa ad attribuirgli

---

<sup>58</sup> Cass., 22.6.1985, n. 3769.

un'identità, attraverso meccanismi matematici o tecniche di profilazione, che molto spesso è distorta da quella reale.

## 1. Il diritto all'identità personale

La prima legge italiana in materia di protezione dei dati personali è stata la l. n. 675/1996. Essendosi succedute nell'arco di circa sette anni numerose modifiche, il D. Lgs. n. 196/2003 è nato con lo scopo di riordinare la materia, ed è invalso l'uso di chiamarlo comunemente "Codice della *privacy*"<sup>59</sup>. L'espressione non è del tutto corretta, in quanto il codice è piuttosto una legge sull'utilizzo delle informazioni, riservate o meno, che detta norme di natura essenzialmente procedurale. I principi generali li troviamo riassunti nei primi due articoli: l'art. 1<sup>60</sup>, che sancisce il diritto alla protezione dei dati personali e l'art. 2<sup>61</sup>, che fa riferimento ad altri diritti considerati di fondamentale importanza, tra cui il diritto all'identità personale. Quest'ultima disposizione, in particolare, evidenzia che i diritti della personalità trattati dal codice sono almeno tre: il diritto alla protezione dei dati personali, il diritto alla riservatezza, il diritto all'identità personale.

Una storica sentenza della pretura di Roma<sup>62</sup> ha definito il diritto all'identità personale come il diritto a <<*non vedersi travisare la propria personalità individuale*>>, mentre la Cassazione<sup>63</sup> l'ha definito come <<*l'interesse del soggetto, ritenuto generalmente meritevole di tutela giuridica, ad essere rappresentato, nella vita di relazione, con la sua vera identità, così come questa nella realtà sociale, generale o particolare, è conosciuta o poteva essere riconosciuta con l'esplicazione dei criteri della normale*

---

<sup>59</sup> Si ricordi che attualmente il quadro normativo europeo è in corso di modifica, essendo stata presentata al Parlamento europeo, il 25.01.2014, la proposta di Regolamento generale sulla protezione dei dati personali.

<sup>60</sup> << *Chiunque ha diritto alla protezione dei dati personali che lo riguardano* >>

<sup>61</sup> << *Il presente testo unico, di seguito denominato "codice", garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.* >>

<sup>62</sup> Pret. Roma, 6.05.1974.

<sup>63</sup> Cass., 22.6.1985, n. 3769.

*diligenza e della buona fede oggettiva* >>. Si tratta, sostanzialmente, dell'interesse a non vedere, all'esterno, alterato o offuscato il proprio patrimonio intellettuale, sociale, politico, religioso, ideologico o professionale. Il bene giuridico protetto dal diritto all'identità personale è, dunque, la proiezione sociale della propria identità. Non è l'immagine che il soggetto ha di sé (verità personale), ma neppure l'insieme delle informazioni oggettivamente riferibili ad esso (verità storica); è l'immagine socialmente mediata e oggettivata del soggetto stesso.

### **1.1. L'identità personale nel tempo e nel (*cyber*) spazio**

Un soggetto viene identificato dal suo nome, dalle immagini che gli altri hanno di lui, dal giudizio degli altri e dalle informazioni che lo riguardano; tutti questi elementi concorrono a formare il concetto di identità. Mentre risulta evidente che il nome sia un elemento di carattere oggettivo e le opinioni altrui siano elementi soggettivi, le informazioni, o meglio i dati personali che riguardano il soggetto, possono essere sia informazioni di carattere oggettivo che opinioni. L'immagine mediata e oggettivata di un soggetto è quindi frutto di un processo ricostruttivo che, a partire sia da fatti oggettivi che da opinioni, approda ad una sintesi obiettiva. Infatti, la nostra identità può variare in base allo sguardo di chi ci osserva: per noi stessi siamo ciò che siamo, ma per qualcun altro, per il pubblico, per la società potremmo apparire diversi, in quanto i soggetti esterni possono avere una diversa percezione della nostra identità. Fatti salvi, dunque, alcuni elementi di natura oggettiva, l'identità è sintesi, è mediazione. Essa però non è una sintesi statica, ma può mutare col tempo. In questa situazione di conflitto, tra verità storica ed identità attuale, nasce il diritto all'oblio. Il diritto all'identità personale è il diritto ad esercitare una forma di controllo sulla propria immagine sociale, che può giungere sino a pretendere che alcuni eventi siano dimenticati. Il diritto all'identità personale, riscontrando uno dei suoi limiti nel diritto di cronaca, assume nuovi connotati e richiede nuove esigenze di tutela su Internet. Non si parla più di ripubblicazione, in quanto la rete, per sua stessa natura, difficilmente dimentica. Infatti, non è diffusa la pratica di cancellare informazioni dai siti, né tale operazione di cancellazione può dirsi facilmente effettuabile. Si costituisce così sulla rete un archivio storico di dimensioni

globali. C'è poi da ribadire che sulla rete le informazioni sono tutte poste sul medesimo livello, appiattite, prive di contestualizzazione e spesso prive di fonti che consentano di attribuire ad esse un peso. Fondamentale, invece, nella costruzione del diritto all'identità personale, è la contestualizzazione, cioè collegare le vicende in un quadro completo di tutti gli elementi essenziali. Il Garante<sup>64</sup> è intervenuto in materia e, con riferimento alla pubblicazione *online* degli archivi storici dei giornali, ha ritenuto legittima la messa a disposizione per la consultazione di informazioni personali attraverso il sito dell'editore, precisando però che la pagina web contenente i dati personali deve essere sottratta all'indicizzazione dei motori di ricerca.

Nel contesto delineato si inserisce una decisione della Corte di Cassazione<sup>65</sup> che costituisce un punto di riferimento importante, in quanto non è solo una decisione sul tema dell'oblio o della protezione dei dati personali, ma anche sul diritto all'identità personale e sulla contestualizzazione dell'informazione su Internet. Il fatto oggetto della sentenza riguarda un politico imputato di corruzione nel 1993. La notizia, correttamente riportata dai quotidiani dell'epoca, non era tuttavia stata aggiornata in seguito alla assoluzione dell'uomo. Infatti, effettuando una ricerca, risultava la notizia dell'imputazione, ma non quella della successiva assoluzione. Dunque, il soggetto ha richiesto l'oscuramento dei dati contenuti nell'archivio storico del quotidiano *online*. La sua domanda è stata, però, respinta sia dall'Autorità Garante per la protezione dei dati personali che dal Tribunale di Milano sulla base di due argomenti: il bilanciamento tra diritto all'informazione e diritto alla protezione dei dati personali e il fatto che non si tratta di una ripubblicazione della notizia, per cui non è configurabile il diritto all'oblio, il quale si ha solo in caso, appunto, di ripubblicazione. L'Autorità Garante per la protezione dei dati personali ha ritenuto che: se l'informazione, che costituisce una notizia di cronaca, è correttamente pubblicata, nell'osservanza del codice deontologico dei giornalisti, non vi è alcuna lesione del diritto alla protezione dei dati personali, dal momento che va operato un bilanciamento di interessi; se poi la notizia è inserita nell'archivio storico di un giornale, il trattamento dei dati contenuti in tale archivio è effettuato per finalità storiche, compatibile con le finalità di trattamento per ragioni di cronaca.

---

<sup>64</sup> Garante: decisioni 11.12.2008 e 19.12.2008

<sup>65</sup> Cass., 5.4.2012, n.5525.

L'iter logico seguito dalla Corte di Cassazione è, invece, estremamente innovativo e allo stesso tempo lineare. L'articolo del 1993, recante la notizia dell'imputazione non poteva, ovviamente, contenere la notizia del proscioglimento verificatosi successivamente. Inoltre, la pubblicazione della notizia era stata correttamente effettuata, nel pieno e legittimo diritto di cronaca; altrettanto legittima deve ritenersi la pubblicazione dell'archivio *online*, effettuata per finalità storica ed espressione di una modalità di esercizio nel tempo del diritto di cronaca. Tuttavia, appare manifesta la lesione nei confronti dell'interessato, il quale trova la sua immagine attuale travisata e ancorata ad un'informazione datata e solo parzialmente vera: *<<La notizia, originariamente completa e vera, diviene non aggiornata, risultando quindi parziale e non esatta, e pertanto sostanzialmente non vera>>*. Dunque, in questo caso, il diritto alla protezione dei dati personali va interpretato in modo strettamente connesso con il concetto di identità personale e quindi come diritto a *<<non vedersi travisare la propria personalità individuale>>*<sup>66</sup>. Nel caso di specie si profilava, dunque, un travisamento dell'immagine sociale del soggetto e di conseguenza una lesione del diritto all'identità personale.

Nel caso appena analizzato, la questione non verte sul diritto ad essere dimenticati, bensì sul diritto alla cancellazione o quanto meno alla contestualizzazione dell'informazione. Come afferma la Corte, una verità non aggiornata non è una verità. Occorre provvedere all'integrazione ed all'aggiornamento delle notizie *<<con modalità tecniche non modificative dell'originale >>*<sup>67</sup>. La giurisprudenza, tuttavia, lascia alla tecnica le modalità operative attraverso cui attuare il principio della contestualizzazione. Occorre configurare un sistema tecnico idoneo a segnalare la sussistenza di un seguito e l'evolversi della notizia. La decisione della Corte di Cassazione risulta essere fortemente innovativa, poiché sposta l'attenzione dall'oblio alla contestualizzazione; tuttavia lascia aperte molte sfide. Innanzitutto l'individuazione delle modalità tecniche in grado di dare piena attuazione alla decisione, e inoltre l'esigenza di ridefinire di volta in volta il diritto all'identità personale in base al caso concreto, non avendo l'identità un carattere assoluto, ma esigendo sempre un'opera di sintesi ed elaborazione. Inoltre, è opportuno precisare che gli archivi storici debbano rimanere intatti ma la notizia che

---

<sup>66</sup>Pret. Roma, 6.05.1974

<sup>67</sup>Cass., 22.06.1985, n.3769

produca una lesione al diritto all'identità personale, verificata caso per caso la lesione, deve essere corroborata dall'informazione che ne assicuri l'attualità, la completezza e la contestualizzazione.

## **2. L'identità nella realtà virtuale**

Nel mondo delle nuove tecnologie dell'informazione e della comunicazione, l'identità diventa il frutto di una costruzione continua e incessante, dai contorni labili e sfumati. La vastissima diffusione di raccolte di dati personali sempre più settoriali, per svariate finalità, produce una frantumazione dell'identità, dislocando i soggetti in luoghi diversificati. Un po' come l'idea hegeliana di "Io" assoluto che si frantuma nei vari "Io" relativi, con la differenza che non si parla più del rapporto tra mondo delle idee e mondo reale, ma di relazione tra mondo reale e mondo virtuale. L'unità delle persone viene spezzata e al suo posto troviamo tante piccole persone elettroniche, contrassegnate da profili specifici, tanti quanti sono gli interessi del mercato. L'individuo si ritrova così nel *cyber spazio* ad avere molteplici identità, a lui spesso sconosciute e che non si conformano perfettamente alla sua identità personale. Oltre ai profili dell'individuo creati per scopi di mercato, l'identità dell'individuo può essere ricavata dal collegamento tra dati e informazioni presenti in maniera disparata e casuale nel *web*, venendosi a creare profili identitari che spesso sfuggono oltre che al diretto interessato, anche alle stesse dinamiche del *web*. Di queste circostanze sono gli individui a pagarne le spese, soprattutto quando il *web* "suggerisce" e associa loro informazioni e identità non vere e crea suggestione nei navigatori che potrebbero lasciarsi condizionare dall'identità suggerita dal *web*. Molte volte sono gli stessi individui a ricercare nel mondo virtuale ciò che non trovano in quello reale. Assistiamo, nell'epoca del digitale, ad una sorta di "ellenismo" moderno che porta gli individui ad evadere dalla realtà, non per rinchiudersi in se stessi, nel proprio "Io", ma per rintanarsi nel porto apparentemente sicuro del *web*, dove tutto sembra evanescente e onirico, per rifugiarsi cioè nel proprio "Io" virtuale. L'uomo vive spesso nell'epoca attuale una condizione di inautenticità e insoddisfazione e ricerca nel *web* nuovi stimoli, nuove opportunità, nuove identità. Il mondo virtuale può essere anche tutto questo: può dare gli stimoli giusti ed essere fonte

di vantaggio e progresso per l'individuo, a patto che questi lo utilizzi con criterio e consapevolezza. Il *web* è un grande strumento di conoscenza e di sviluppo messo dalla tecnica nelle mani dell'umanità; tuttavia, questo “fuoco di Prometeo” rischia di appiccare irrimediabili incendi, qualora l'individuo non ne sappia fare un corretto utilizzo.

## **2.1. Identità personale, Identità digitale, Profilo digitale**

Lo sviluppo del *web* ha generato una rappresentazione digitale degli utenti che si discosta dalla rappresentazione basata sull'identità apparente dell'individuo e sui suoi comportamenti pubblici. Da qui la distinzione tra identità personale e identità virtuale. Ogni individuo riesce ad esercitare un certo grado di controllo sulla propria identità personale, influenzando la percezione che gli altri hanno di sé, ma non della propria identità digitale, la quale viene spesso creata automaticamente, attraverso l'elaborazione di profili digitali ricavati in base ai dati forniti dagli stessi individui o comunque raccolti in rete, o basati su algoritmi costruiti da enti pubblici o aziende private. Tuttavia tale profilo è pur sempre espressione della personalità individuale e per questo è destinato ad essere utilizzato su delega, ma oggi questa delega viene il più delle volte negata. I gestori di motori di ricerca o di *social network* e gli altri *provider*, infatti, possono acquisire dati personali legalmente, grazie ai contratti di accesso ai servizi cui l'utente accede; ci sono anche ipotesi di acquisizione di dati in maniera illegale, ma giustificata da altre esigenze, come il caso delle agenzie di *intelligence* che possono decidere autonomamente di acquisire dati su individui sospettati di atti terroristici.

L'identità personale è costruita in modo consapevole dal soggetto stesso ed è la proiezione sociale della personalità dell'individuo. Tuttavia, come abbiamo precedentemente detto, anche l'identità personale può avere aspetto multiforme a seconda dalla prospettiva da cui si guarda l'individuo cui tale identità appartiene. Lo stesso termine “persona” deriva dal latino e significa “maschera”; riprendendo il concetto pirandelliano potremmo quindi ritenere che l'individuo assume una pluralità di identità personali, una valida per se stesso, altre diverse, valide per gli altri. Una delle definizioni più note di persona proviene dal filosofo Locke: <<*un essere pensante*



*dotato di intelligenza, di ragione e di riflessione, è capace di considerarsi in se stesso come la medesima realtà, in differenti luoghi e tempi>>*. Dei rilievi giuridici dell'identità personale abbiamo già ampiamente discusso, resta da considerare invece l'identità digitale. L'espressione non ricorre in alcuna disposizione normativa vigente, tuttavia è ormai entrata a far parte, negli ultimi decenni, del vocabolario del giurista e viene comunemente declinata in due accezioni distinte. In una prima e più generale accezione, l'espressione "identità digitale" viene utilizzata come sinonimo di "identità in rete" o "identità virtuale" ed impiegata dal punto di vista giuridico per distinguere tra "corpo fisico" e "corpo elettronico" o per riferirsi alla possibilità di assumere diverse identità sulla rete. In un'accezione più ristretta, invece, l'espressione "identità digitale" è impiegata per designare l'insieme delle informazioni e risorse concesse da un sistema informatico ad un particolare utilizzatore. L'autenticazione può essere effettuata tramite *password*, impronte digitali, riconoscimento vocale o del volto, tessere magnetiche etc. A questa seconda accezione fa riferimento la questione di rilevanza giuridica e penale legata al furto d'identità<sup>68</sup>. L'identità digitale, dunque, si riferisce ad un individuo reale, e per questo si distingue dal profilo digitale, riferito invece ad un individuo potenziale e costruito automaticamente attraverso dati e correlazioni algoritmiche tra essi. Il profilo digitale è il risultato di processi automatici in cui i dati relativi all'individuo vengono prelevati da grandi *database* e sottoposti a processi che impiegano algoritmi per trovare correlazione tra vari dati personali riferiti ad uno stesso soggetto. Un profilo può essere connesso ad un individuo anche successivamente alla sua creazione; la connessione avviene quando l'individuo viene riconosciuto come possessore di una o più caratteristiche appartenenti al profilo. La profilazione può avvenire per scopo commerciale o ad opera dei servizi segreti. Le attività della NSA sono state ampiamente documentate dai giornalisti del *New York Times*, Laura Poitras e James Risen, che si sono ampiamente basati sulle rivelazioni di Edward Snowden. La NSA avrebbe acquisito milioni di immagini facciali ricavate da comunicazioni intercettate in tutto il mondo. Tali immagini, ottenute tramite un software, da e-mail, messaggi, social network e altre fonti di comunicazioni verrebbero associate ai dati ricavati dalle intercettazioni di comunicazioni private, ottenendo così un'accurata profilazione di

---

<sup>68</sup> Condotta criminale volta ad ottenere indebitamente denaro o vantaggi fingendosi un'altra persona. Esistono almeno tre tipologie di furto d'identità: furto dell'identità finanziaria, furto criminale d'identità, clonazione d'identità.

milioni di cittadini. Ciò che ha riscosso particolare allarme sociale è il fatto che nel mirino della NSA, per caso o per errore, siano finiti anche molti comuni cittadini e non solo persone sospette; basterebbe infatti esprimere interesse sul *web* verso strumenti per la protezione della *privacy* per diventare un *target* NSA. Per quanto attiene alla profilazione commerciale ci riferiamo invece alle aziende che costruiscono e vendono i profili dei consumatori, acquisendo dati anagrafici del soggetto, sui gusti, interessi ed abitudini comportamentali. Anche in questo caso, per trasformare l'utente in un preciso target commerciale, occorre mettere in relazione i dati personali acquisiti *online*, sottoponendoli ad algoritmi specifici. Le tecniche di profilazione senza dubbio incutono stupore e destano sospetto e timore nei confronti della macchina della rete che sembra operare alle nostre spalle, a nostra insaputa, col suo "grande occhio" fisso su di noi. E poi ci siamo noi individui, smarriti, spersonalizzati e frammentati in mille identità confuse in un mondo dai confini labili, sospeso tra realtà e virtualità. Uno scenario apocalittico e destabilizzante, forse frutto di ignoranza, intesa come mancata consapevolezza.

Viviamo in un mondo globalizzato e digitalizzato in cui tutto dipende ormai dalla rete. In questo mondo la maggior parte di noi si sente perso e ha bisogno di conservare la propria identità, l'ancora che consente di navigare nell'oceano della globalizzazione. Ma l'identità non si conserva evitando di gettarci nell'infinito mare del *web*, né tentando di arginare questo mare con regole inflessibili o rigidi controlli. L'identità è una prerogativa dell'essere umano e spetta a lui solo conservarla, anche nei meandri del cyber-spazio. La consapevolezza è la parola-chiave.

### **3. Il concetto filosofico di Identità**

Quello di identità è un concetto complesso ed uno dei più sfuggenti e difficilmente definibili in modo univoco, in quanto, come afferma Claude Lévi Strauss: <<*In effetti il tema dell'identità si situa al punto di confluenza non di due semplicemente ma di più strade insieme. Interessa praticamente tutte le discipline*<sup>69</sup>>>. Se ne occupano la sociologia, l'antropologia, la logica, la psicologia, il diritto; nonché le scienze in senso

---

<sup>69</sup> Claude L.S., *L'identità*, pag.11, Sellerio editore, Palermo 1980.

stretto come biologia e medicina, allorquando intervengono nella discussione sulle componenti e sulle strutture fisiologiche e patologiche dell'identità degli individui. In ogni caso questo concetto così ampio e variegato trova la sua prima formulazione in filosofia, in ambito speculativo. È in filosofia che per la prima volta viene introdotta la nozione di identità nella sua duplice fondamentale accezione; inizialmente come unicità, unitarietà e distinzione da qualsiasi altra cosa; successivamente, e molto più tardi, come identità personale, collettiva e sociale. Il primo oggetto, quello teoretico, nasce ed è caratteristico dei primordi della filosofia e dei suoi successivi sviluppi<sup>70</sup> il secondo invece, non teoretico ma pratico, è frutto e patrimonio essenzialmente della filosofia moderna<sup>71</sup>. È quest'ultimo aspetto che interessa il tema in oggetto e desta notevole interesse ai nostri fini che riguardano essenzialmente l'identità personale. Tralasciamo perciò il primo aspetto, quello teoretico, riguardante soprattutto il rapporto identità-diversità e che ha rappresentato uno dei problemi permanenti della filosofia teoretica, ad iniziare quantomeno da Parmenide, il primo ad affermare che la realtà poteva essere compresa e spiegata ricorrendo ad un principio unico presente nella sua totalità; egli creò, quindi, il concetto di identico (ταυτον), mentre Eraclito fu il fautore del diverso (μεταβολη). Se consideriamo, viceversa, l'aspetto moderno del problema, che prende l'avvio con l'empirista Locke e continua con Hume, ci accorgiamo che l'empirismo inglese esamina su cosa si fonda e in cosa consiste l'identità dell'io considerata nel suo protrarsi nel tempo e vista come distinta dalla pura identità dell'individuo. Alla domanda: in che cosa consiste l'identità personale o morale? Locke, nel *“Saggio sull'intelletto umano”*, risponde: l'identità personale o morale si concretizza nella coscienza, equivale alla coscienza. *«Per trovare in che cosa consista l'identità personale dobbiamo considerare per che cosa sta la parola persona; essa sta, credo, per un essere pensante intelligente, dotato di ragione e di riflessione, che può considerare se stessa come se stessa, cioè la stessa cosa pensante, in diversi tempi e luoghi, il che accade solamente mediante quella coscienza che è inseparabile dal pensare e, a me, risulta essenziale ad esso, giacché è impossibile che qualcuno percepisca senza percepire che percepisce. [...] Infatti, poiché la coscienza accompagna sempre il pensare ed è ciò che fa sì che ognuno sia quello che egli chiama*

---

<sup>70</sup> Da Parmenide e il suo *Essere* inteso come totalità, alla filosofia di Platone ed Aristotele.

<sup>71</sup> Si allude alla filosofia empirista di Locke e Hume.

io, distinguendo con ciò se stesso da tutti gli altri esseri pensanti, in questo solo consiste l'identità personale, cioè nel fatto che un essere razionale è sempre lo stesso. E fin dove questa coscienza può essere estesa indietro ad una qualsiasi azione o pensiero del passato, fin lì giunge l'identità di quella persona; si tratta dello stesso io ora e allora ed è dallo stesso io – lo stesso di quello attuale che ora riflette su di esso – che quella azione venne compiuta>>. La coscienza o riflessione su di sé è dunque il fondamento dell'identità personale in quanto <<È la stessa coscienza che unisce le azioni distanti nella stessa persona, qualunque siano le sostanze che hanno contribuito alla loro produzione>>. La definizione di persona o Io è perciò un'idea fondata sulla relazione, sul rapporto fra l'Io attuale, presente e l'Io "storico", passato; e in ciò bisogna vedere il fondamento della responsabilità morale e giuridica. <<Su questa identità personale – dice infatti Locke – è fondato tutto il diritto e la giustizia della ricompensa e del castigo>> perché solo sulla continuità della coscienza o Io , garantita dalla memoria, si può fondare l'aderenza o la difformità di un'azione ad una norma o legge e dare vita alle idee di bene e di male nell'accezione morale, giuridica e politica. Bisogna qui chiarire che tutte le suddette argomentazioni e deduzioni di Locke risultano valide in quanto il filosofo inglese fonda ogni cosa sulla certezza dell'io, certezza raggiunta attraverso un'intuizione di tipo cartesiano: <<Se dubito di tutte le altre cose, questo stesso dubbio mi fa percepire la mia propria esistenza e non mi permette di dubitarne<sup>72</sup>>>. Diversi invece sono i convincimenti e le certezze dell'altro famoso ed ultimo empirista inglese, Davide Hume. Questi attraverso la sua critica, così come demolisce le idee di sostanza, spazio, tempo, causalità, allo stesso modo abbatte anche il concetto di Io. Secondo Hume noi non percepiamo l'io come un'essenza unitaria e sempre identica a se stessa, ma avvertiamo solo i diversi stati d'animo susseguirsi nella coscienza. Ciò che noi crediamo sia l'Io è invece solo un insieme di impressioni. Così si esprime Hume: <<L'io, o la persona, non è un'impressione: è ciò a cui vengono riferite, per supposizione, le diverse nostre impressioni e idee. Se ci fosse un'impressione che desse origine all'idea dell'io, quest'impressione dovrebbe rimanere invariabilmente la stessa attraverso tutto il corso della nostra vita [...] Invece, non c'è

---

<sup>72</sup> <<L'esperienza ci convince che abbiamo una conoscenza intuitiva della nostra propria esistenza e una percezione interna infallibile che noi esistiamo. In ogni atto di sensazione, ragionamento o pensiero, noi siamo consci di fronte a noi stessi del nostro proprio essere e su questo punto non manchiamo del più alto grado di certezza.>> (Saggio sull'intelletto umano di John Locke, libro IV, capitolo IX, pag.706).

*nessuna impressione che sia costante e invariabile [...] Non può essere, dunque, da nessuna di queste impressioni, né da alcun'altra che l'idea dell'io è derivata: per conseguenza, non esiste tale idea.>>*<sup>73</sup> Per Hume, dunque, non sussistono se non impressioni e percezioni differenti, illimitatamente varie, e non compare mai la percezione pura dell'io al quale attribuiamo tutte le impressioni che riceviamo. Di conseguenza, *<<E' evidente che l'identità che si attribuisce alla mente umana, per quanto perfetta la si voglia considerare, non è in grado di risolvere la pluralità delle percezioni differenti in una sola[...] ne segue, evidentemente, che l'identità non appartiene realmente a quelle differenti percezioni, né le unifica affatto; ma è semplicemente una qualità a loro attribuita a causa dell'unione delle idee di esse nell'immaginazione, quando vi riflettiamo.>>*

Per spiegare come da questa mutevolezza, da questo fascio di impressioni, incessantemente mutevoli, possa nascere l'idea dell'identità personale, il filosofo di Edimburgo fa anch'egli leva sulla memoria. Leggiamo in proposito nel Trattato: *<<Poiché la memoria, sola, ci fa conoscere la continuità e l'estensione di questa successione di percezioni, essa deve essere considerata, per tal ragione principalmente, l'origine dell'identità personale. Se non avessimo la memoria, non si potrebbe avere nessuna nozione della causalità, né, per conseguenza, di quel concatenamento di cause ed effetti che costituisce il nostro io, o la nostra persona>>*.

Sembra qui esserci una sorta di identificazione dell'identità personale con la memoria, in quanto essa costituisce l'unico elemento che può permetterci di mettere in relazione le idee o impressioni passate con quelle attuali.

In ogni caso la memoria per esplicare la sua funzione ha bisogno del sostegno di tre elementi o presupposti: la rassomiglianza, la contiguità, e la causalità. *<<L'identità – sostiene Hume – dipende, dunque, da qualcuna di queste tre relazioni: di rassomiglianza, di contiguità, e di casualità; e poiché la vera essenza di queste tre relazioni consiste nel produrre un facile passaggio da un'idea a un'altra, ne segue che le nostre nozioni di identità personale derivano esclusivamente dal cammino piano e ininterrotto del pensiero attraverso una serie d'idee connesse>>*. Tutto ciò avviene nel dinamico dispiegarsi e svolgersi della vita psichica.

---

<sup>73</sup> *Trattato sulla natura umana* di Davide Hume, sez.VI: "L'identità personale", pag.263 e ss.

In questo modo, attraverso la sua critica demolitrice giunge a concepire l'identità personale come una struttura integralmente psicologica che non ci dà alcun diritto di presupporre come essenziale un'identità sostanziale, quale l'anima, come cardine e condizione indispensabile dell'io.

Quell'io che per Locke era una evidente certezza diventa, nell'ultimo degli empiristi, solo un fascio di percezioni e la nostra mente assume le funzioni di un teatro in cui le diverse percezioni diventano gli attori, senza che però, come sarebbe opportuno, esista il luogo fisico, la scena teatrale, per l'appunto, in cui possano comparire, senza cioè che esista un Io<sup>74</sup>.

Il concetto filosofico dell'identità, nella sua accezione più moderna, coincide dunque con quello di memoria. L'identità personale è data dalla memoria e, se vogliamo lasciar trasmigrare questa concezione dal piano filosofico a quello giuridico, non possiamo fare a meno di notare, alla luce di ciò che ci siamo detti nei precedenti paragrafi, come anche il diritto all'identità personale e la sua tutela siano riconnessi al diritto all'oblio, al diritto ad essere dimenticati; ciò affinché vicende negative del passato vengano rimosse dalla memoria, la quale molto spesso costruisce la nostra identità personale. L'identità dell'uomo, come abbiamo notato sostenere anche da Locke, è data dal rapporto tra l'io attuale e l'io passato e in ciò sta il fondamento della responsabilità morale e giuridica. L'identità dell'uomo, dunque, si costruisce col tempo e l'io di oggi non può non essere condizionato dall'io di ieri, vuoi sul piano giuridico che su quello morale. Non serve dunque cancellare o nascondere il passato, perché ciò significherebbe rinnegare una parte di quell'io che è inevitabilmente formato sì dal presente, ma anche, e forse soprattutto, dalla memoria.

---

<sup>74</sup> <<Io oso affermare che [...] noi non siamo altro che fasci o collezioni di differenti percezioni che si susseguono con una inconcepibile rapidità, in un perpetuo flusso in movimento[...] La mente è una specie di teatro, dove le diverse percezioni fanno la loro apparizione [...] E, non si fraintenda il paragone del teatro: a costituire la mente non c'è altro che le percezioni successive: noi non abbiamo la più lontana nozione del posto dove queste scene vengono rappresentate, o del materiale di cui è composta.>>

## ***Conclusioni***

La trattazione ha riguardato la responsabilità del motore di ricerca Google per quei suggerimenti di ricerca generati dal suo algoritmo che potrebbero avere significato offensivo o diffamatorio. Dalla descrizione delle singole avventure legali di Google abbiamo avuto modo di notare che alla base delle divergenze giurisprudenziali e delle difficoltà e che nell'ultimo decennio hanno interessato il diritto delle comunicazioni elettroniche, c'è un problema normativo e sociale di fondo: l'incapacità del diritto di mantenersi al passo con un'evoluzione tecnologica che sembra non arrestarsi e che entra in modo sempre più preponderante nella vita di ogni cittadino in modo invasivo e multiforme. La tecnologia invade ogni sfera della nostra vita, dal lavoro alla società, dalla politica al diritto e alla sfera di vita privata del singolo. Alla base dei differenti orientamenti giurisprudenziali in merito alla responsabilità del motore di ricerca ed alla rilevanza giuridica dell'attività dello stesso, si pone il ritardo normativo e soprattutto la non uniformità del diritto. Sono, infatti, sempre più evidenti i contrasti di opinione e i punti di vista differenti sul tema, che potremmo complessivamente racchiudere in due orientamenti di base: abbiamo bisogno di una "forte Costituzione"<sup>75</sup> per difenderci dai giganti del *web* o bisogna dare libero spazio alla rete e a chi opera in essa, assicurando piena libertà di iniziativa economica e libero sviluppo dell'innovazione e della conoscenza, senza limite alcuno all'informazione? Ci siamo ampiamente soffermati sul contemperamento di interessi in gioco: da un lato abbiamo analizzato l'esigenza di tutela della libertà di pensiero e di informazione, nonché della libertà e neutralità della rete; dall'altro abbiamo rilevato come sia difficile garantire sulla rete la protezione dei diritti della personalità, o meglio garantire la conservazione della propria identità, libera da condizionamenti e suggestioni. Sono questi interrogativi che principalmente emergono ogni qualvolta si tenta di analizzare una qualche attività svolta nell'immenso spazio del *web*, sia essa di natura economica o meramente tecnica o informativa. In quest'ultima analisi tentiamo dunque di ricavare le nostre ultime conclusioni, partendo dal generale, per poi scendere al particolare, ossia al caso di specie oggetto di

---

<sup>75</sup> Stefano Rodotà. «Perché Internet ha bisogno di nuove regole» *La Repubblica*.

trattazione sin dal primo capitolo. Seguiremo questo schema conclusivo in quanto, come ho già detto, i problemi legali connessi all'attività del motore di ricerca postulano delle criticità di ordine più generale e complesso che interessano il recente e continuo scontrarsi del diritto con l'evoluzione dei mezzi di comunicazione nell'era del digitale. Fino a qualche anno fa sembrava essersi consolidata un'impostazione che lasciava poco spazio ai diritti fondamentali della persona. Lo stesso Zuckerberg, fondatore del principale *social network* e *competitor* di Google+, aveva parlato di fine della privacy come regola sociale, di fronte alla preminenza della tecnologia e della logica economica. Erano state legittimate raccolte di dati sempre più imponenti, giustificandole in nome della sicurezza nazionale ed internazionale. Dunque, gli interessi della sicurezza e del mercato occupavano sempre di più l'orizzonte di Internet. Tuttavia, il cosiddetto Datagate, ossia il programma di sorveglianza di massa operato dai servizi di sicurezza americani ed inglesi, ha determinato reazioni negative che hanno messo in discussione la legittimità di una sorveglianza di massa, che non solo causa la violazione dei diritti individuali, ma sta determinando la creazione di una società di controllo. Abbiamo ampiamente analizzato come l'orientamento della giurisprudenza europea abbia risposto a questa recente esigenza di tutela dei dati personali, arrivando con la sentenza del 13 maggio 2014 a statuire che i diritti fondamentali riconosciuti dagli articoli 7 e 8 della Carte di Nizza <<*prevalgono sull'interesse economico degli operatori dei motori di ricerca*>>. La situazione è stata dunque capovolta e si è andata attribuendo una valenza costituzionale alla Carta dei diritti fondamentali dell'Unione europea. Si è rinnovata l'attenzione per un "Internet bill of rights" e proprio nel nostro Paese, una commissione istituita dalla Presidente della Camera dei deputati, ha elaborato una Dichiarazione dei diritti di Internet ed è stata aperta una consultazione svoltasi, dunque, in una sede istituzionale; ciò ha distinto la risposta del nostro Paese all'esigenza di costituzionalizzare Internet rispetto agli altri Stati membri. Uno spazio costituzionale, dunque, sembra essersi aperto e l'Unione Europea, ormai da più di due anni, discute sul Regolamento di cui abbiamo già analizzato freni, pressioni e tendenze innovatrici.

Nella situazione attuale, le modalità di raccolta ed utilizzo dei dati, possono arrecare un grande danno alle persone, ossia che la loro identità venga costruita da altri. Abbiamo analizzato come le informazioni vengano affidate ad algoritmi che costruiscono



un'identità ipotetica e persino distorcente, ma che diviene strumento di conoscenza e valutazione. Snowden, dopo aver svelato il piano di spionaggio digitale del governo statunitense, ha avvertito di non utilizzare strumenti come *Dropbox*, *Gmail* o *Facebook*. Egli ha sostenuto che tutti utilizziamo quotidianamente ed inconsciamente tali strumenti e nel momento in cui veniamo avvisati e messi in guardia delle ripercussioni sulla nostra *privacy*, la nostra risposta è: "Non mi interessa, non ho nulla da nascondere". In questo modo stiamo annullando il nostro diritto di proteggerci dalle intrusioni governative. Ma anche dagli avvertimenti dello stesso Snowden, se letti in un'ottica più leggera e meno cospirazionista, si scorge la mancata esigenza di regole rigide di salvaguardia della nostra *privacy*. Basterebbe infatti che i cittadini vengano avvisati e messi a conoscenza degli eventuali rischi e delle potenziali ripercussioni dell'utilizzo del *web* sulla loro vita privata; per il resto saranno in grado di compiere da soli le loro valutazioni e di comportarsi come meglio credono. Impiegare un minimo di accortezza nell'utilizzo del *web* non vuol dire essere paranoici, ma rispettare se stessi e la propria indipendenza, per non rischiare di non essere più cittadini e diventare sudditi, anche quando effettivamente "non si ha nulla da nascondere". Ma da queste considerazioni di normale e comune buon senso, sembra esagerato arrivare a sostenere che mezzi come *Google* o *Facebook* siano pericolosi e da evitare. Ogni cittadino ha le capacità intellettive giuste per riuscire a comprendere il confine tra un libero e critico utilizzo di Internet ed una condizione di sottomissione e condizionamento ad esso, o meglio ai soggetti che ne detengono il potere e il controllo. Non credo sia giusto rinunciare alla conoscenza globale e all'aggregazione e condivisione globalizzata che un mezzo come la rete è in grado di offrire, per il timore, sia esso fondato o infondato, che i nostri dati personali siano utilizzati in modo massiccio e così "oscuro". Il giorno dopo che sul *web* è stato rivelato che la NSA entrava nei *computer* spacciandosi per Facebook, Zuckerberg si è ampiamente schierato contro la condotta del governo americano ritenendo che la fiducia nella rete sia oggi un fattore importante e che, affinché la rete diventi più forte bisogna garantire che sia anche più sicura; rendere la rete più sicura significa proteggere gli utenti dai criminali e non dallo stesso governo. La talpa della NSA, parlando al Southwest Interactive technology festival ha sostenuto che: <<*Stanno appiccando un incendio al futuro della Rete (...) e voi che siete in questa sala, siete i pompieri*>>. E a proposito di fuoco, mi piace riprendere una metafora che ho già

utilizzato in questa trattazione, ossia quella del fuoco di Prometeo, del fuoco della tecnica rubato dalla divinità e posto nelle mani dell'uomo. È così che immagino Internet e la tecnologia nel suo complesso: un dono divino, messo nelle mani dell'uomo, affidato all'intelletto umano per farlo fruttificare e per garantire lo sviluppo dell'umanità e il progresso. Prometeo fu punito per aver rubato il fuoco agli dei e donato la tecnica agli uomini. Forse gli dei sapevano che gli umani con l'uso della tecnica avrebbero devastato il mondo, o forse temevano che avrebbero fatto grandi cose? Senza dubbio il potere della tecnologia è immenso e se non sfruttato con criterio potrebbe portare conseguenze devastanti sull'umanità, che vanno anche ad di là delle questioni connesse alla libertà di pensiero o al diritto alla riservatezza, sfociando in problemi di natura etica e di libertà morale. Ma se di uno strumento così potente si riesce a fare un sano e corretto utilizzo, allora sì che potrebbero raggiungersi grandi risultati. Ritornando alla rete, essa può essere davvero un mezzo salvifico e il diritto di accesso ad Internet dovrebbe essere garantito a tutti proprio per assicurare in modo paritario ad ogni individuo i benefici che la rete è in grado di offrire: una conoscenza senza confini, per dare all'uomo la possibilità di informarsi su ogni questione che gli interessa e per assicurargli una connessione, non semplicemente ad una rete, ma un'interazione col mondo intero, una comunicazione piena ed efficace, a trecentosessanta gradi. Si è tanto parlato, soprattutto negli ultimi tempi, di diritto di accesso ad Internet nelle recenti discussioni in merito all'introduzione dell'articolo 34-bis. L'attività di comunicazione posta in essere attraverso Internet rappresenta proprio uno degli effettivi modi di esercizio della libertà di manifestazione del pensiero. La rete può essere compresa nei cd. beni comuni, ossia quei beni che, indipendentemente da una preventiva individuazione da parte del legislatore, per la loro intrinseca natura o finalità, risultano funzionali al perseguimento e al soddisfacimento degli interessi della collettività. Per evitare il rischio che, in assenza di adeguate forme di regolamentazione, l'uso della rete possa essere rimesso al libero gioco dei grandi attori economici ed istituzionali è necessario che sia garantito un accesso paritario a tutti. Secondo l'opinione di Stefano Rodotà, bisognerebbe prevedere e nella Costituzione un comma aggiuntivo all'art. 21: "tutti hanno eguale diritto di accedere alla Rete Internet, in condizioni di parità, con modalità tecnologicamente adeguate e che rimuovano ogni ostacolo di ordine economico e sociale".

Internet non è più solo l'infrastruttura mediante la quale si può accedere alla conoscenza, ma è anche il luogo nel quale le persone possono esprimersi, costruire le proprie immagini pubbliche, partecipare alla cultura e al dibattito sociale e politico. Internet è da intendersi principalmente come strumento di comunicazione e per assicurarne a tutti il libero e pieno esercizio è importante garantirne il diritto di accesso. Si parla infatti di web 2.0, per differenziarlo dal cosiddetto web 1.0, rappresentato da siti informativi statici che non offrono la possibilità di interazione con l'utente, cioè la capacità di contribuire ai contenuti informativi. Oggi invece ciascun soggetto è contemporaneamente fruitore e produttore dei contenuti informativi. Il *cyber-spazio* ha infatti segnato il passaggio da una comunicazione verticale ad una comunicazione orizzontale basata sulla libera circolazione delle informazioni all'interno del *web*, in cui tutti sono fornitori e fruitori di dati al tempo stesso. I fattori a cui ciò è dovuto sono principalmente la crisi in cui versa la politica e il malcontento generale dei cittadini che accresce il personalismo dell'individuo, il quale aspira a realizzarsi da sé e Internet gli dà la possibilità di assumere il ruolo di attore nella produzione di informazioni. La conseguenza, però, da tenere in considerazione di tutto questo complesso sistema è data dal fatto che forniamo inconsapevolmente le nostre informazioni, contribuendo ad accrescere il valore di aziende che operano nel settore dell'acquisizione di informazioni in rete. La novità più significativa del *web 2.0* è sicuramente il fenomeno dei *social network*. Il primo *step* che bisogna affrontare quando ci si iscrive ad un *social network* è la costruzione del proprio profilo, e qui veniamo a toccare l'aspetto dell'identità. Gli utenti della rete creano profili che li rappresentano, grazie alla combinazione di informazioni personali di vario genere. Mediante il proprio profilo l'interessato esprime e costruisce la propria identità sociale, anzi le proprie diverse identità. Anche le varie attività che si svolgono nell'ambito del *social network* contribuiscono alla definizione dell'identità sociale, in quanto il fatto di essere amico di alcune persone, partecipare a certe iniziative, manifestare determinate preferenze e condivisioni, indica aspetti della personalità. La questione da porsi è quella relativa alla qualificazione giuridica. Nell'ipotesi in cui il *social network* fornisca dei veri e propri servizi di comunicazione elettronica, consentendo all'utente di inserire contenuti da loro stessi generati (foto, testi, musica etc.), ad esso si applicheranno le disposizioni della Direttiva relative alla

vita privata ed alle comunicazioni elettroniche. Anche Google ha creato un servizio che si basa sul modello bidirezionale dei *social network* con lo scopo di porsi in concorrenza con *Facebook*, si tratta di Google+. Da varie indagini è stato rivelato che il principale problema per il diritto alla riservatezza, in un mondo sempre più “*social*” non è tanto la mancanza di opzioni a livello di *privacy*, infatti, i giganti che operano nel settore, primi fra tutti Google e *Facebook*, stanno facendo ampi passi in avanti nel campo delle rispettive *privacy policy*; il vero problema è la quasi totale e inconsapevole adesione al modello e alle impostazioni della *privacy* stessa forniti dalle aziende. Moltissimi utenti, infatti, non sono neppure consapevoli dell’esistenza di sistemi di controllo della *privacy* dei *social network*. Quindi, ancora una volta, il problema a monte è l’inconsapevolezza dell’utente. C’è una totale fiducia e un affidamento inconsapevole, dettato dall’abitudine e dall’ ampia diffusione dell’uso dei *social*, che gli utenti utilizzano i servizi resi in modo ormai inconscio e automatico. Apparentemente l’utente sembrerebbe fruire in modo assolutamente gratuito dello spazio messo a disposizione dal fornitore del servizio. In realtà, il fine perseguito è quello di garantire a soggetti terzi, solitamente gli inserzionisti pubblicitari, che appaiono in diverse forme tra le pagine del *social network*, un flusso sempre più continuo e copioso di utenti registrati, collegati e attivi, o meglio di dati personali e preferenze a loro relativi; l’utente diverrebbe quindi un’entità di rilevanza economica. Google è l’azienda più temuta nel mondo dell’informazione poiché è il più grande ente di raccolta dati. Il suo *database* mondiale è un tesoro dal valore inestimabile, considerando che oggi la fonte di maggior valore non è più l’oro né giallo, né tantomeno nero, ma qualcosa di incolore ed immateriale. Il governo dei dati e delle informazioni conferiscono una posizione di rilevanza e di controllo a chi riesce a raccoglierne in così grandi quantità. Alla luce di queste considerazioni ben si spiega perché alcune aziende come Google, *Facebook*, *YouTube* forniscano ai propri utenti innumerevoli servizi gratuitamente. La valuta corrente in Internet non si quantifica in termini monetari ma è data dal numero di utenti presenti nei *database* di queste aziende.

È necessario garantire la neutralità della rete per salvaguardare l’uguaglianza e l’innovazione ed evitare che Internet divenga uno strumento sequestrato dai soggetti più forti. I soggetti più forti, che occupano il vertice nella scala degli utilizzatori e beneficiari della rete, non sono esclusivamente le grandi imprese che sulla rete svolgono

la propria attività economica; o meglio tali imprese, come Google, hanno affiancato nell'ultimo periodo all'attività meramente economica, una funzione di servizio pubblico, che esige un nuovo quadro istituzionale. È forse in quest'ottica che le grandi aziende di telecomunicazioni elettroniche potrebbero svolgere un'attività di controllo sulla rete e potrebbero scontrarsi con le norme a tutela dei diritti dell'individuo; ma occorre precisare che, da questa prospettiva, esse non operano in modo autonomo ma il più delle volte asservite al potere governativo. La rete è l'oggetto del desiderio di ogni potere totalitario e per preservarla da un potere di controllo sociale ed economico, forse non è produttivo concentrarsi solo su una regolamentazione diretta ad ostacolare la libera iniziativa economica delle imprese che operano in quel settore. La rete, infatti, è ormai a tutti gli effetti uno spazio economico, come lo è diventato il mondo intero d'altronde, con l'unica differenza che non si tratta di uno spazio fisico, ma virtuale. Le uniche regole esistenti dovrebbero essere quelle che comunemente disciplinano i rapporti tra imprese e consumatori e i soggetti che dovrebbero agire nello spazio del *web* dovrebbero essere unicamente gli utenti che ne usufruiscono e le imprese che lo gestiscono. È vero che si tratta di rapporti economici molto più complessi, considerando tra l'altro che il consumatore si trasforma anche in produttore, ma alla base rimane pur sempre un rapporto economico. La soluzione sarebbe dunque quella di escludere soggetti esterni a questo rapporto. Libertà d'impresa, anche nel *cyber spazio*, vuol dire non solo evitare ogni costrizione normativa che possa inibire il libero agire economico delle aziende che operano nel settore, ma vuol dire anche libertà delle imprese dalle pressioni esterne governative con cui spesso si ritrovano, obbligate o meno, a collaborare. In questi termini deve essere analizzata la questione dibattuta tra chi vede Internet come l'area della libertà e chi vi scorge invece l'area del controllo. Internet è uno spazio economico in cui si svolgono rapporti collaterali tra imprese e consumatori, ogni soggetto esterno rischierebbe di compromettere questo territorio.

Approcciandoci alla fine del nostro iter conclusivo e in seguito a tutte le considerazioni sopra esposte, è inevitabile sostenere che, di fronte al pericolo di espropriazione della nostra identità, l'unico strumento per garantire ad ogni individuo la titolarità di se stesso è la tutela dei diritti personali. Tuttavia, più che tutela si potrebbe parlare di "autotutela": l'individuo non può rimettere la protezione della propria identità esclusivamente nelle mani del legislatore, ma dovrebbe imparare a preservarla da sé,

coadiuvato sì da strumenti di natura normativa e costituzionale, ma anche facendo leva sul proprio buon senso e sulla normale diligenza.

Nel corso della trattazione abbiamo spesso fatto riferimento a quel nuovo e un po' misterioso diritto che ondeggia tra riservatezza, privacy e identità e di cui è spesso difficile riuscire ad individuarne natura e confini. Avvicinandoci dal generale al caso particolare della nostra trattazione, prendiamo di nuovo in esame la sentenza *Google Spain*, per ricavare da essa le criticità relative ad una concezione del diritto all'oblio che pregiudica eccessivamente l'attività regolarmente svolta da un motore di ricerca. Dire che il gestore di un motore di ricerca è titolare e responsabile dei singoli dati personali contenuti nei siti indicizzati, è come dire che il gestore di una catena di supermercati, che distribuisce al pubblico differenti prodotti, è responsabile non del prodotto, ma di ogni singolo ingrediente contenuto nella merce confezionata che egli semplicemente distribuisce e vende. Il dato personale è l'ingrediente dei prodotti del *web* che Google rende accessibili agli utenti con il suo servizio di ricerca; ma è evidente che quei dati sono trattati dal motore al solo fine di indicizzarli e solo chi ha immesso in rete il dato personale determina la finalità del suo trattamento e dell'informazione che da esso può trarsi; solo costui è il titolare responsabile del trattamento. Se il dato personale è illegittimamente trattato, l'informazione dovrà essere espunta dalla rete e il motore di ricerca dovrà eliminare gli eventuali risultati di ricerca o suggerimenti automatici correlati. Ma nessun obbligo di controllo *a priori* e nessuna responsabilità *a posteriori* può dirsi sorgere in capo al motore di ricerca. La Corte confonde la finalità economico-commerciale dei servizi forniti da Google con la finalità del trattamento dei singoli dati personali; Google non ha determinato né modificato la finalità di trattamento di un dato personale, ha semplicemente reso disponibile come informazione quel dato, così come era presente sul *web* in un determinato contesto.

Come dicevamo, non risulta ben definito il diritto all'oblio comparso nella proposta di modifica della normativa europea a tutela dei dati personali nel 2012. Esiste già da tempo il diritto alla cancellazione dei propri dati quando questi sono trattati da terzi senza consenso, oppure quando la motivazione a fondamento della richiesta di cancellazione, che deriva dal diritto fondamentale di ognuno di gestire e controllare la propria identità, risulti prevalente rispetto alle ragioni e finalità che invece giustificano il trattamento. Abbiamo già evidenziato come il fatto che Google gestisca un servizio

per fini economico-commerciali è irrilevante per il bilanciamento di interessi che deve essere effettuato, in quanto si può legittimamente trarre fonte di guadagno da servizi utili per la collettività. È invece l'utilità del trattamento del dato in sé che determina la prevalenza sulla richiesta dell'interessato. In conclusione il divieto di indicizzazione si riferisce a chi è titolare di quel dato e l'ha diffuso sul *web*; solo lui potrà valutare motivazioni e finalità del trattamento. La normativa, nel caso di specie, dovrebbe rivolgersi ai responsabili dei giornali e degli archivi storici su Internet. Pretendere che sia Google ad attivarsi per rettifiche e cancellazioni vuol dire negare la funzione stessa del servizio di indicizzazione. Vuol dire non aver compreso il ruolo dei servizi intermediari della comunicazione ed assegnare ad una compagnia commerciale, votata al profitto, il compito, per lei tecnicamente ed umanamente impossibile, di valutare, per l'intero pianeta, il corretto bilanciamento dei diritti fondamentali in gioco. Vuol dire, infine, delegare a Google la scelta di ciò che è reperibile in rete e ciò che deve rimanere nascosto. C'è un errore in diritto, in quanto si perde sempre di mira il reale ruolo di Google come azienda che facilita l'accesso alle informazioni e le si addebitano responsabilità che non le spettano. Tenendo presente questa ultima asserzione, scendiamo ancora più nel fulcro della nostra trattazione ad analizzare il problema dell'identità "suggestionata". Fino a che punto i suggerimenti automatici di Google possono "suggestionare" gli utenti, o più precisamente condizionarli in merito alla reputazione di una certa persona, fisica o giuridica che sia? Proviamo sempre a partire da ciò che accade nello spazio fisico e reale per tentare poi di estenderci, analogicamente, fin dove è possibile, alle medesime situazioni che si verificano però nello spazio virtuale. Quando un soggetto può essere influenzato dai "suggerimenti" nella vita quotidiana? Potremmo pensare ai cosiddetti fatti notori, ossia alle massime comuni di esperienza, all'*id quod plerumque accidit*, o meglio ancora alla *vox populi*. Ecco, i suggerimenti automatici di ricerca potrebbero essere paragonati alla *vox populi*, all'opinione comune che si forma "per sentito dire". La nostra reputazione è messa in discussione ogni giorno, non solo in ambiente virtuale, ma anche in quello reale. Anche nella realtà la gente può avere una visione di noi distorta dalla realtà a causa di ciò "che si dice su di noi". Sta a noi, se realmente interessati ad un'informazione, fare le opportune verifiche di approfondimento e comparazione, per testare la veridicità e affidabilità di una notizia. Allora, anche in rete, tutto è rimesso nelle mani dell'utente, al

suo senso critico. L'utente deve saper discernere ciò che è vero da ciò che è falso e, laddove realmente interessato ad un suggerimento o risultato di ricerca, deve andare più a fondo nella ricerca ed informarsi più dettagliatamente, senza lasciarsi suggestionare e condizionare dalla prima impressione. Ciò accade parimenti nella realtà: non bisogna formare la propria opinione e le proprie convinzioni sulla base di pregiudizi e presunzioni non provate. I suggerimenti di ricerca di Google non provano la responsabilità in capo al motore di ricerca; potrebbero essere qualificati come argomenti di prova che hanno bisogno di essere corroborati da ulteriori prove piene. L'algoritmo di Google agisce in questo modo: raccoglie le opinioni più comuni tra gli utenti e le suggerisce agli altri utenti. Funziona come la nostra mente: anche noi siamo soliti raccogliere più opinioni comuni tra la gente e poi riferirle ad altre persone. Potremmo grossolanamente identificare il suggerimento automatico come un pettegolezzo. E chi si sognerebbe mai di incolpare giuridicamente una persona per la diffusione di un pettegolezzo? Ora certamente è vero che un suggerimento può creare in noi una suggestione e indirizzarci a pensare in un certo modo, ma sta al buon senso dell'utente non lasciarsi ingannare e rimanere critico. Il singolo utente della rete deve essere messo nelle condizioni di poter operare un ragionamento inferenziale sulla base di suggerimenti automatici ed altri dati di vario genere di cui dispone o altri elementi che dovrà ricercare, per compiere così la propria libera valutazione di attendibilità del suggerimento. Google può essere sì in grado di "suggestionare", ma ciò fa parte della sua strategia, della propria attività di business. Sta all'uomo non lasciarsi suggestionare, o meglio farsi suggestionare solo in positivo, da quei suggerimenti e quelle informazioni che gli possono essere utili e che, qualora non ci fossero stati, gli avrebbero reso l'attività di ricerca più complessa o inutile. Internet è uno strumento salvifico se lo si utilizza con intelligenza.

Bisogna riconoscere che le norme del *cyber-spazio* oggi regolano gran parte della vita sociale e lavorativa degli uomini: si partecipa alla vita politica tramite forme di *e-democracy*, si intrattengono le relazioni sociali tramite i *social network*, si perfezionano rapporti contrattuali ed effettuano transazioni attraverso forme di *e-commerce*, si sperimentano nuovi profili nel mercato del lavoro, si utilizzano gli strumenti telematici per espandere gli ambiti in cui opera la libertà di informazione e di espressione. Dunque si rende necessario un intervento normativo per regolare gli



innumerevoli rapporti che interessano il *web*; ma è soprattutto necessaria una disciplina normativa che faccia scolorire l'immagine del *web* come uno spazio di libertà gestito in un regime di anarchia e che, nel contempo, non costringa la rete in un tramaglio di regole rigide e poco flessibili che mal si adattano al sistema cui si applicano e che finiscono per contraddire la natura stessa di Internet, quale area della libertà.

## BIBLIOGRAFIA

Corte di Giustizia dell'Unione Europea (Grande Sezione)- C-131/12 (13 maggio 2014).

Corte di Giustizia dell'Unione Europea (Grande Sezione)-C-288/12 (8 aprile 2014).

Corte di Giustizia dell'Unione Europea (Grande Sezione)-C-362/14 (6 ottobre 2015).

Bugiolacchi, Leonardo. «Ascesa e declino della figura del <<provider attivo>>? Riflessioni in tema di fondamento e limiti del regime privilegiato di responsabilità dell'hosting provider.» *Responsabilità civile e Previdenza*, 2015: 1261.

Caggiano, Giandonato. «L'interpretazione del "contesto delle attività di stabilimento" dei responsabili del trattamento dei dati personali.» *Diritto dell'Informazione e dell'Informatica*, 2014: 605.

Comella, Cosimo. «Indici, sommari, ricerche e aspetti tecnici della de-indicizzazione.» *In Il diritto all'oblio su Internet dopo la sentenza Google Spain*.

Cunha, Sartor Giovanni e Mario Viola De Azevedo. «Il caso Google e i rapporti regolatori USA/EU.» *In Il diritto all'oblio su Internet dopo la sentenza Google Spain*, a cura di Giorgio Resta e Vincenzo Zeno-Zencovich.

D'Antonio, Salvatore Sica e Virgilio. «La procedura di de-indicizzazione.» *In Il diritto all'oblio su Internet dopo la sentenza Google Spain*, a cura di Giorgio Resta e Vincenzo Zeno-Zencovich.

Finocchiaro, Giusella. «Il diritto all'oblio nel quadro dei diritti della personalità .» *In Il diritto all'oblio su Internet dopo la sentenza Google Spain*, a cura di Giorgio Resta e Vincenzo Zeno-Zencovich. 2015.

Finocchiaro, Giusella. «La protezione dei dati personali e la tutela dell'identità.» In *I diritti della personalità in rete*.

Flor, Roberto. «Dalla data retention al diritto all'oblio. Dalle paure orwelliane alla recente giurisprudenza della Corte di Giustizia.» In *Il diritto all'oblio su Internet dopo la sentenza Google Spain*, a cura di Giorgio Resta e Vincenzo Zeno-Zencovich. 2015.

Mantelero, Alessandro. «Il futuro regolamento EU sui dati personali ed il dilemma del caso Google: ricordare e dimenticare nella digital economy.» In *Il diritto all'oblio su Internet dopo la sentenza Google Spain*, a cura di Giorgio Resta e Vincenzo Zeno-Zencovich. 2015.

Niger, Sergio. «Il diritto all'identità personale.» In *Il diritto al nome e all'identità personale nella normativa, nella giurisprudenza e nella dottrina italiane*.

Peron, Sabrina. «Il diritto all'oblio nell'era dell'informazione on-line.» *Responsabilità civile e previdenza*, 2014: 1177.

Pirozzoli, Anna. «La responsabilità dell'Internet service provider. Il nuovo orientamento giurisprudenziale nell'ultimo caso Google.» *Associazione Italiana Dei Costituzionalisti*, n. 3/2012 (settembre 2012).

Pizzetti, Franco. «Le Autorità garanti per la protezione dei dati personali e la sentenza della Corte di Giustizia sul caso Google Spain: è tempo di far cadere il "Velo di Maya".» In *Il diritto all'oblio su Internet dopo la sentenza Google Spain*, a cura di Giorgio Resta e Vincenzo Zeno-Zencovich.

Pollicino, Oreste. «"Suggest search": le posizioni del giudice di Milano e di Parigi.» *Diritto* 24.

Pollicino, Oreste. «Un digital right to privacy preso (troppo) sul serio dai giudici di Lussemburgo? Il ruolo degli artt. 7 e 8 della Carta di Nizza nel reasoning di Google Spain.» In *Il diritto all'oblio su Internet dopo la sentenza Google Spain*, a cura di Giorgio Resta e Vincenzo Zeno-Zencovich.

Resta, Giorgio. «Identità personale e identità digitale.» *Il diritto dell'informazione e dell'informatica* (Milano, Giuffrè Editore).

Richmond, Shane. «"Islam is" not being censored by Google.» *The Telegraph*, Gennaio 2010.

Scannicchio, Tommaso. «La responsabilità del motore di ricerca per la funzione "auto-complete".» *Il diritto dell'informazione e dell'informatica* (Milano Giuffrè Editore), 2012.

Stavroula - Borghi, S. «Search engine liability for autocomplete suggestions: personality, privacy and the power of the algorithm.» *International Journal of Law and Information Technology*, 2015: 1-29.

Synodinou, Tatiana-Eleni. «Google versus the law.»

Tosi, Emilio. «La responsabilità civile per fatto illecito degli Internet service provider e dei motori di ricerca a margine dei recenti casi "Google suggest" per errata programmazione del software di ricerca e "Yahoo! Italia" per "link" illecito in violazione dei diritti di proprietà intellettuale.» *Rivista di Diritto Industriale*, 2012: 44.

*YAHOO!/Mediaset*. 29 (Corte di Appello di Milano, 7 gennaio 2015).

*Lyonnaise de garantie/ Google Inc.*, Cour d'appel de Paris Pôle 2, chambre 7 Arrêt du 14 décembre 2011

Trib. Milano, ord., 24 marzo 2011

Trib. Milano, ord., 23 marzo 2013

Trib. Pinerolo, ord., 2 maggio 2012

*Direct Energie/ Google Inc.*, Tribunale de Commerce de Paris , 7 mai 2009

BGH Case VI ZR 269/12, del maggio 2013

Oberlandesgericht Köln, 15 U 199/11, del 10 maggio 2012

*Search King, Inc. v Google Technology, Inc.*, No 02-1457, 2003 (WD Oklahoma, 27 May 2003).

*Langdon v Google, Yahoo! and Microsoft Corp.*, 474 F Supp 2d 622 (D Del 2007).  
Proposal for a regulation of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final, Brussels, 25/01/2012.

2012/0011 (COD)- 12/03/2014 Text adopted by Parliament, 1st reading.

Locke, John. <<Saggio sull'intelletto umano>>, UTET.

Hume, David. <<Trattato sulla natura umana>>, Editori Laterza.

