Diritto, Economia e Tecnologie della Privacy

Anno V, Numero 3, 2014

Istituto Italiano Privacy

Diritto, Economia e Tecnologie della Privacy

Rivista quadrimestrale dell'Istituto Italiano per la Privacy e la valorizzazione dei dati

Diritto, Economia e Tecnologie della Privacy

Anno V, n. 3, 2014
Registrazione al Tribunale di Arezzo n. 1P/10RS del 26 ottobre 2010
Rivista quadrimestrale

Provider: Aruba S.p.A., P.zza Garibaldi 8 – 52010 Soci (AR). Autorizzazione Ministero delle Comunicazioni n. 473. Server collocati in Via Sergio Ramelli, 8 - 52100 Arezzo (AR).
Stampa: Daniele Mosera, via Giulio Pittarelli, 23, 00166, Roma.

Direttore: Giovanni Crea

Comitato scientifico: Umberto Fantigrossi, Elena Ferrari, Edoardo Giardino, Michele Iaselli, Rosario Imperiali, Laura Liguori, Andrea Lisi, Marco Marazza, Massimo Melica, Maurizio Mensi, Rocco Panetta, Norberto Patrignani, Roberto Tunioli.

Caporedattore: Marianna Quaranta

Segreteria di redazione:
e-mail: rivista@istitutoitalianoprivacy.it

Comitato di redazione: Paolo Balboni, Tommaso Bonetti, Manuel Cacitti, Matteo D'Argenio, Nicola Fabiano, Elena Finotti, Chiara Fonio, Guglielmo Forgeschi, Massimo Fubini, Giovanni Cucchiarato, Andrea Maggipinto, Luigi Massa, Marco Maria Mattei, Stefano Mele, Alessandro Rapisarda, Alessandro Rodolfi, Lucio Scudiero, Guglielmo Troiano.

Direzione e redazione: Piazza di San Salvatore in Lauro, 13, 00186, Roma; Direttore responsabile: Giovanni Crea

Proprietà della rivista: Istituto Italiano per la Privacy e la valorizzazione dei dati. Consiglio di Amministrazione dell'Istituto Italiano per la Privacy e la valorizzazione dei dati: Luca Bolognini – Presidente; Diego Fulco – Direttore; Pietro Paganini – Segretario Generale.

Editore: Istituto Italiano per la Privacy e la valorizzazione dei dati, Piazza di San Salvatore in Lauro, 13, 00186, Roma
www.istitutoitalianoprivacy.it
info@istitutoitalianoprivacy.org
tel.: +39 06 97842491
fax: +39 06 23328983
Tutti i diritti riservati. Qualsiasi uso o riproduzione di contenuti anche solo parziali della presente rivista richiede la preventiva autorizzazione dell'editore. Il marchio "Istituto Italiano Privacy" con relativo logo figurativo appartiene all'Istituto Italiano per la Privacy e la valorizzazione dei dati.

Condizioni economiche

- singolo numero: € 25,00
- abbonamento annuale (tre numeri): € 70,00 (L'abbonamento decorre dal mese di gennaio di ciascun anno. La sottoscrizione dell'abbonamento nel corso dell'anno dà diritto a ricevere i numeri arretrati). Il pagamento può essere effettuato mediante versamento bancario sul conto intestato a Istituto Italiano per la Privacy e la valorizzazione dei dati – IBAN – IT75C0316501600000110403686

INDICE

Editoriale pag. 385

GIOVANNI CREA
Alcune riflessioni in tema di sicurezza delle ICT in una prospettiva di *law and technologies* » 385

Contributi » 389

LUCA BOLOGNINI, GIUSEPPE RAGUSA, CAMILLA BISTOLFI, FRANCESCO COREA, LUCIO SCUDIERO
Effetti dei motori di ricerca sul pluralismo dell'informazione. Aspetti giuridici e di analisi econometrica » 389

ALESSIA FARANO
Mind detection e protezione dei dati neurogenetici. Alcune riflessioni sulla privacy mentale » 433

LUIGI PRINZI
Problematiche nella tutela dei dati personali e riflessi nei servizi cloud computing. » 449

Rassegna giuridica » 509

GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI
Opinion 9/2014 on the application of Directive 2002/58/EC to device fingerprinting » 509

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI
Informazioni sulle convinzioni religiose dei pazienti: i casi in cui possono essere raccolte durante il ricovero - 12 novembre 2014 » 523

Provvedimento generale prescrittivo in tema di biometria - 12 novembre 2014 » 531

Giurisprudenza » 551

CORTE DI CASSAZIONE, sez. I civile – sentenza 28 marzo – 7 ottobre 2014, n. 21107.
Offerte di prestazioni sessuali a pagamento "dati sensibili" » 551

CORTE DI CASSAZIONE, sez. V penale – 16 giugno 2014, n. 25774.
Reato di sostituzione di persona » 561

Editoriale

Alcune riflessioni in tema di sicurezza delle ICT in una prospettiva di *law and technologies*

GIOVANNI CREA

La sicurezza è un bisogno innato nell'essere umano, le cui origini, con ogni probabilità, vanno ricondotte alla costante presenza nell'ambiente di condizioni di imprevedibilità che determinano nell'uomo lo stato emozionale dell'insicurezza, della paura. Nella sua analisi delle motivazioni del comportamento, lo psicologo statunitense Abraham Maslow intuì il carattere esplicativo del bisogno di sicurezza – l'essere, cioè, 'motivante' di un comportamento teso alla sua stessa soddisfazione – collocandolo gerarchicamente dopo i bisogni primari legati alla sopravvivenza (A. MASLOW, *Motivation and personality*, New York, Harper and Brothers, 1954). Nella prospettiva di Maslow, dunque, la sicurezza descrive una condizione di protezione che, una volta risolti i problemi fondamentali, l'uomo ricerca (aspetto comportamentale) per la tutela dei propri interessi e della propria persona nell'ambiente in cui egli è attivo.

La rivoluzione *post*-industriale si è caratterizzata principalmente per l'avvento delle *Information and communication technologies* (ICT) e in particolare di internet che, a partire dalle prime esperienze degli *hacker* virtuosi fondate sulla cooperazione nei progetti di sviluppo della grande rete e sulla diffusione della conoscenza, ha assunto progressivamente le caratteristiche di un ecosistema alternativo a quello fisico. La 'colonizzazione' di internet (il termine è di G. SARTOR, *Il diritto della rete globale*, in *Ciberspazio e diritto*, vol. IV, n. 1, 2003) ha fatto il resto con l'ingresso, a partire dagli anni novanta del secolo scorso, di figure portatrici di interessi diversi e talvolta confliggenti – consumatori, imprese, pubbliche amministrazioni – ma anche di individui e organizzazioni con intenti illeciti, la cui portata arriva a integrare condotte rilevanti sotto il profilo penale. Quest'ultimo esito descrive l'altra faccia delle ICT che si contrappone

all'utilità delle stesse rinvenibile sotto diversi profili (socioeconomico, cognitivo; sull'argomento si veda, per tutti, M. CASTELLS, *La nascita della società in rete*, Milano, Ed. Università Bocconi, 2002): oltre a rappresentare un fattore di evoluzione nella commissione dei reati 'tradizionali', le tecnologie predette sono alla base dell'emergenza di nuove fattispecie di reato (V. SCALIA, *Criminalità informatica vs diritto alla riservatezza e protezione dei dati personali. I legislatori (europeo e nazionale) alla ricerca del giusto punto di equilibrio nell'epoca della globalizzazione digitale*, in AA.VV, *Diritto alla privacy e trattamento automatizzato dei dati fra diritto civile, diritto penale e diritto internazionale ed europeo*, Università di Catania, 2014, 24-41. P. GALDIERI, *Reati informatici: normativa vigente, problemi e prospettive*, in *Diritto, economia e management*, n. 3, 2013).

La sicurezza, dunque, è questione che si ripropone nell'ecosistema digitale con l'emergere di stati emozionali (paure) nei *digital user* legati sia alla consapevolezza che la grande Rete è anche il luogo di comportamenti antisociali che possono arrecare pregiudizio alle "attività digitali" – e, più in generale, a tutto quel che dipende dalle ICT – sia all'incapacità delle autorità di contrasto di risalire agli autori di detti comportamenti. Sotto quest'ultimo aspetto, con riguardo alle prospettive di *cyber war* delineatesi con l'impiego delle ICT, è stato osservato come il carattere globale di internet – e dunque l'assenza di riferimenti territoriali – renda più difficoltosa l'individuazione dei responsabili delle azioni offensive per tal via attuate (G.T. MERLO, *Il dominio degli spazi: il cosmo la cyber war e l'urgenza di una dottrina operativa per la guerra futura*, in *La comunità internazionale*, n. 4, 2010).

Le conseguenze economiche generate dai crimini informatici non sono trascurabili; al riguardo, basti pensare al furto di conoscenze scientifiche e tecnologiche di un'impresa e alle ricadute sulla sua capacità di innovare e di essere competitiva sui mercati internazionali. In questi e altri casi di intrusione in sistemi costruiti sulle ICT vanno considerati anche i costi, reali e intangibili, che un'organizzazione deve sostenere *ex post*; costi di ripristino del servizio, perdita di utenti, eventuali risarcimenti, caduta d'immagine. Peraltro, la dimensione economica dei reati informatici ha assunto nel tempo una

connotazione di mercato; sotto questo aspetto, va osservato come il fenomeno abbia generato un vero e proprio *digital crime market*, luogo di scambio di 'prodotti' fraudolentemente acquisiti (codici di carte di credito e bancomat) ma anche di tecnologie di supporto ai comportamenti illegali (Cfr. PRESIDENZA DEL CONSIGLIO DEI MINISTRI, *Quadro strategico nazionale per la sicurezza dello spazio cibernetico*, dicembre 2013; T. MOORE, R. CLAYTON, R. ANDERSON, *the economics of online crime*, in *Journal of economic perspectives*, vol. 23, n. 3, 2009). In questo scenario 'industriale' le organizzazioni criminali hanno assunto caratteristiche d'impresa – specie nel caso della produzione di *software* – disponendo sia di risorse per le attività di *R&D* sia del processo produttivo per realizzare programmi idonei a eludere i *firewall* posti a difesa dei sistemi.

Sul fronte europeo, a partire dalla Raccomandazione (89) 9 del Consiglio d'Europa, il legislatore ha elaborato nuove ipotesi delittuose connesse all'avvento delle ICT; ipotesi in cui le stesse tecnologie possono essere strumento od oggetto di reato, e che la letteratura sviluppatasi in tale contesto ha sintetizzato nella categoria *computer crimes* (V. FROSINI, *La criminalità informatica*, in *Instrumenta*, n. 4, 1998; G. TADDEI ELMI, R. ORTU, P. CIFALDI, *La Raccomandazione del Consiglio d'Europa del 9 settembre 1989 n. R (89)-9 e la Legge 23 dicembre 1993 n. 547 in materia di computer crimes: una analisi comparativa*, in *Informatica e diritto*, n. 1, 1996). Nella sua traiettoria evolutiva, culminata nell'adozione della direttiva n. 40/2013, il *framework* di regolamentazione ha configurato il profilo di reato per talune condotte che investono i sistemi realizzati con le ICT laddove non siano state autorizzate dai titolari dei diritti su tali sistemi (o su una loro parte) ovvero non siano consentite dalle legislazioni degli Stati membri. Al riguardo, rileva sottolineare come, tra le condotte predette, la direttiva abbia incluso anche le attività, proprie di un ambiente di mercato, di produzione e scambio di codici di accesso e programmi utilizzabili per accessi e perturbazioni illeciti. L'intervento nella sfera del *cyber crime* ad opera della direttiva 2013/40 ha un evidente carattere dissuasivo alla luce dell'adozione di misure sanzionatorie di tipo detentivo e della previsione di una responsabilità delle persone giuridiche. Peraltro, internet ha messo a nudo l'incapacità del diritto tradizionalmente inteso di regolare i

comportamenti che si svolgono al suo interno per i ben noti aspetti di *enforcement* dovuti al disallineamento territoriale tra internet e gli ordinamenti; ma anche per le difficoltà di identificare gli *internet user* che violano le norme. La struttura della grande Rete e le regole tecniche che ne governano il funzionamento costituiscono dunque un limite all'efficacia del diritto. Alla luce di tale insufficienza, è stata da più parti messa in evidenza l'opportunità di un approccio di tipo *law and technologies* in cui le regole giuridiche e le regole tecniche (*software*) operano congiuntamente per garantire la prestazione dei servizi della società dell'informazione (pubblici e privati) e la protezione dei contenuti. In questa prospettiva, le misure *software* rappresentano una forma di regolazione che agisce dall'«interno» di internet per impedire i comportamenti illeciti, in tal modo delimitando l'ambito delle azioni ammissibili; un esempio in tal senso è rappresentato dalle tecnologie di protezione di contenuti digitali (conservati in archivi informatici) coperti da diritti di proprietà (*Digital rights management*). Dal canto loro, le regole giuridiche non si limitano a svolgere una funzione di disincentivazione dell'uso di programmi per l'intrusione nei sistemi che gestiscono contenuti, servizi digitali e infrastrutture critiche, ma si spingono a prescrivere l'adozione di opportune misure tecniche tali da garantire livelli quantomeno minimi di sicurezza.

La previsione di un siffatto intervento pubblico riposa evidentemente sulla considerazione che la sicurezza dei predetti sistemi, nella misura in cui questi sono uno strumento di trattamento di dati e di erogazione di servizi, è un bene giuridico i cui *standard* non possono essere rimessi alle valutazioni soggettive delle figure intervenienti (titolari del trattamento e *service provider*). Il rapporto tra regole tecniche e regole giuridiche si caratterizza pertanto per la conformità delle ICT al dettato normativo al fine di renderlo più efficace.

Contributi

Effetti dei motori di ricerca sul pluralismo dell'informazione. Aspetti giuridici e di analisi econometrica

di LUCA BOLOGNINI*, GIUSEPPE RAGUSA**, CAMILLA BISTOLFI*, FRANCESCO COREA**, LUCIO SCUDIERO*

SOMMARIO: 1. La libertà di informazione e la tutela internazionale – 2. Il bilanciamento tra l'articolo 10 della CEDU e gli altri diritti secondo la Corte Europea – 3. L'impatto di internet sul pluralismo dell'informazione e il ruolo dei motori di ricerca – 4. *Search engines responsibility* ed estensibilità del concetto di "editore" al motore di ricerca – 5. *Search engines*: un'analisi econometrica – 6. Diritto di accesso, pluralismo e motori di ricerca a seguito della recente giurisprudenza della Corte di Giustizia dell'Unione Europea sul diritto all'oblio: potenziale contrasto con l'articolo 10 della CEDU

1. La libertà di informazione e la tutela internazionale.

Il concetto di "libertà di informazione" porta con sé moltissime questioni ancora parzialmente irrisolte, sia in termini sociali sia in termini giuridici ed economici. Già di primo acchito, appare evidente come non si tratti soltanto del diritto di produrre, pubblicare, diffondere, condividere i dati (profilo attivo), ma anche di poter essere informati da coloro che si occupano di elaborare e diffondere le notizie di interesse pubblico (profilo passivo) e di poter accedere alle informazioni stesse. Già se si considerano questi tre profili di base, è chiaro che siffatta libertà si fonda anche sul diritto alla ricerca dei dati e delle fonti e sulle garanzie di pluralismo, che però necessitano di essere, entrambi, mediati con gli altri interessi o diritti dei soggetti di volta in volta coinvolti. Un tema attualmente molto dibattuto, a mero

* Istituto italiano per la privacy e la valorizzazione dei dati.
** Luiss Guido Carli.

titolo di esempio, è quello del costante conflitto e del necessario bilanciamento tra due principi cardine: da un lato il diritto degli individui ad essere protetti rispetto all'uso dei dati che li riguardano (*protezione dei dati personali*); dall'altro, il diritto della persona, intesa come membro della società civile, di poter accedere alle informazioni e di poterle ricevere oltreché trasmettere/condividere (*libertà d'informazione*). La protezione dei dati personali e la trasparenza delle notizie chiamano continuamente in causa il parallelo – o spesso confliggente – riconoscimento del diritto alla privacy rispetto all'interesse pubblico, per esempio quello perseguito dalla stampa libera e da chiunque eserciti il diritto di cronaca e/o di critica, che gode di pieno riconoscimento in quanto estrinsecazione della libertà di espressione. Altrettanto rilevante, in tema di diritti individuali, è poi la questione della responsabilità editoriale, i cui caratteri costitutivi – in primis l'esercizio di un controllo effettivo su contenuti - ne rendono problematica l'imputazione ai diversi *providers* che forniscono servizi o contenuti nel web.

Ma per comprendere appieno i confini fondamentali della libertà di informazione, ricordiamo innanzitutto – e prima di addentrarci nelle problematiche di relazione tra tale libertà e altre libertà o diritti fondamentali degli individui – che essa viene protetta dai principali trattati internazionali sui diritti umani, prima ancora che dalle Costituzioni e dalle leggi dei singoli Stati.

La Dichiarazione Universale dei Diritti dell'Uomo, promossa dall'ONU nel 1948, fa riferimento alla suddetta libertà nell'articolo 19, ove si stabilisce che: «*Ogni individuo ha il diritto alla libertà di opinione e di espressione, incluso il diritto di non essere molestato per la propria opinione e quello di cercare, ricevere e diffondere informazioni e idee attraverso ogni mezzo e senza riguardo a frontiere*». Queste previsioni sono riprese dall'ONU nel 1966, nella *International Covenant on Civil and Political Rights* che, sempre all'articolo 19, ribadisce quanto stabilito nella Dichiarazione Universale, inserendo la precisazione che la circolazione delle informazioni deve comunque rispettare i diritti e la reputazione altrui nonché la sicurezza nazionale, l'ordine pubblico, la salute pubblica o la morale. Dunque, come si accennava poc'anzi, anche in tale testo il soddisfacimento dell'interesse a ricevere, a far circolare e ad avere

accesso alle notizie viene bilanciato con la tutela di altri diritti fondamentali, che ovviamente non possono essere trascurati. Sulla stessa direttrice si muove la *Convention Against Corruption* redatta dall'ONU nel 2003, il cui articolo 13 fa riferimento alla libertà di informazione intesa come "*Participation of society*", sottoposta agli stessi limiti di cui sopra. Restringendo il campo, è impossibile non fare riferimento alla Carta dei Diritti Fondamentali dell'Unione Europea, che all'articolo 11 fissa la "Libertà di espressione e d'informazione" stabilendo che:«*1. Ogni individuo ha diritto alla libertà di espressione. Tale diritto include la libertà di opinione e la libertà di ricevere o di comunicare informazioni o idee senza che vi possa essere ingerenza da parte delle autorità pubbliche e senza limiti di frontiera. 2. La libertà dei media e il loro pluralismo sono rispettati.*».

In questo caso, dunque, non si introduce soltanto una libertà attiva (comunicare) e passiva (ricevere), ma si stabilisce l'impossibilità per le autorità pubbliche di ostacolare tali diritti e l'obbligo di garantire che i media rispondano alle esigenze di un'informazione democratica e plurale. La differenza rispetto alle previsioni dell'ONU risiede nella mancanza, nelle disposizioni della Carta, di un termine che indichi il diritto di accesso all'informazione, valorizzato espressamente, invece, nella Dichiarazione Universale.

Il tema, peraltro, non si pone in Europa solo con riferimento alla libertà di informazione intesa come diritto di cronaca e critica, ma anche da un punto di vista di accesso alle informazioni generate e/o possedute da istituzioni pubbliche (dati *in re ipsa* di interesse pubblico). Già nel Trattato di Maastricht del 1992, la dichiarazione numero 17 (*Declaration on the right of access to information*) recitava – con un'ottica al diritto di accesso alle informazioni pubbliche: «*The Conference considers that transparency of the decision-making process strengthens the democratic nature of the institutions and the public's confidence in the administration. The Conference accordingly recommends that the Commission submit to the Council no later than 1993 a report on measures designed to improve public access to the information available to the institutions.*».

Nel 2008 è stata anche redatta a Budapest da un gruppo di esperti internazionali la *Declaration on the Right of Access to Information*,

finalizzata al riconoscimento del diritto di accesso all'informazione come diritto umano fondamentale. L'accento è stato posto anche sul problema di considerare le implicazioni giuridiche e pratiche di questa libertà, proprio perché, come si diceva poc'anzi, possono esservi delle eccezioni al suo esercizio, come la tutela dei dati personali o il diritto all'oblio, cui si farà riferimento più avanti.

Rimanendo sempre in ottica eurocentrica, il Consiglio d'Europa con la Convenzione Europea dei Diritti dell'Uomo, all'art. 10 stabilisce che: *«1. Ogni persona ha diritto alla libertà d'espressione. Tale diritto include la libertà d'opinione e la libertà di ricevere o di comunicare informazioni o idee senza che vi possa essere ingerenza da parte delle autorità pubbliche e senza limiti di frontiera. Il presente articolo non impedisce agli Stati di sottoporre a un regime di autorizzazione le imprese di radiodiffusione, cinematografiche o televisive. 2. L'esercizio di queste libertà, poiché comporta doveri e responsabilità, può essere sottoposto alle formalità, condizioni, restrizioni o sanzioni che sono previste dalla legge e che costituiscono misure necessarie, in una società democratica, alla sicurezza nazionale, all'integrità territoriale o alla pubblica sicurezza, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, alla protezione della reputazione o dei diritti altrui, per impedire la divulgazione di informazioni riservate o per garantire l'autorità e l'imparzialità del potere giudiziario».*

Ancora una volta, dunque, emerge la delicata questione del bilanciamento tra l'interesse pubblico all'informazione con altri diritti o interessi di pari rango, che la Corte Europea dei Diritti dell'Uomo si è trovata più volte ad effettuare nell'interpretazione del diritto previsto dall'articolo 10 della CEDU. Ad esso, infatti, fanno seguito delle eccezioni ritenute "necessarie" in una società democratica i cui fondamenti devono essere previsti con legge proprio a garanzia dell'esclusione di un'ingiustificata restrizione della libertà di informazione. Per queste ragioni, la Corte di Strasburgo ha disciplinato i diversi casi a partire dalla valutazione della legge nazionale, accessibile e conoscibile, per verificare che l'interferenza di quest'ultima sulla libertà di informazione sia proporzionata in relazione al fine per cui è stata adottata la norma.

Qualora le limitazioni alla libertà di cui all'articolo 10 della CEDU siano necessarie al mantenimento dei valori democratici, allora esse avrebbero ragione di compiersi nonostante la legge domestica possa sembrare in apparente contrasto con la Convenzione. Per inquadrare questo tipo di approccio, si può partire dalla celebre sentenza del 1976, *Handyside v. United Kingdom*, in cui la Corte ha ritenuto che la condanna del titolare di una casa editrice, che aveva pubblicato un manuale di educazione sessuale per studenti, costituisse una violazione delle libertà di cui all'art. 10 CEDU. Infatti, pur riconoscendo l'intento di proteggere la morale (ex art. 10 comma 2 CEDU), la Corte ravvisava l'assenza di uno standard europeo che configurasse proprio il concetto di "morale", spiegando che l'assenza di un concetto uniforme di "morale" nello spazio giuridico di vigenza della Convenzione non legittimasse tuttavia lo Stato membro nel limitare il pluralismo informativo a priori, poiché una tale limitazione doveva comunque essere commisurata alle necessità della società democratica, che la stessa Corte interpretava nel modo che segue: «*La libertà di espressione costituisce uno dei fondamenti essenziali di una tale società, una delle condizioni fondamentali per il progresso e per lo sviluppo di ogni uomo [...] E' applicabile non solo alle "informazioni" o "idee" che sono ricevute con favore o considerate come inoffensive o con indifferenza, ma anche a quelle che offendono, creano shock o disturbano lo Stato o qualsiasi parte della popolazione. Tali sono le esigenze di pluralismo, tolleranza e apertura mentale, senza le quali non vi è "società democratica"*»[1].

Non è un caso, infatti, che alcuni dei verdetti più rilevanti in rapporto alla tutela dei diritti di cui all'articolo 10 della CEDU riguardino l'editoria – in particolare i giornali – rispetto alla libertà di informazione nel contesto della discussione delle questioni di interesse pubblico. Per esempio, nella causa *Sunday Times c. Regno Unito (n. 1)*[2] (1979) il ricorrente si accingeva a pubblicare un articolo scientifico sulle procedure compiute da una società farmaceutica prima di

[1] Handyside v. United Kingdom, N. 5493/72, §41, ECHR 1976 in hudoc.echr.coe.int.

[2] The Sunday Times v. The United Kingdom, N. 6538/74, §42, ECHR 1979 in hudoc.echr.coe.int.

commerciare un sedativo, considerato da diversi cittadini la causa di difetti genetici di alcuni neonati. Ciò era confermato dal fatto che molte famiglie stavano negoziando con la società e vi erano altrettanti processi in corso. Per questo motivo, un tribunale britannico aveva accolto un'ingiunzione della casa farmaceutica con la quale giustificava il divieto di pubblicazione con il fatto che la diffusione dell'articolo avrebbe pregiudicato i procedimenti pendenti.

La Corte Europea, in proposito, pur riconoscendo che la sentenza nazionale era stata emessa al fine di garantire l'imparzialità del giudizio, in realtà costituiva una limitazione del diritto all'informazione che sarebbe andata ad inficiare l'interesse pubblico. Al contrario, invece, nel caso *Du Roy e Malaurie c. Francia*[3] la Corte ha ritenuto legittima ai sensi dell'articolo 10 della CEDU la condanna civile di un editore e di un giornalista a seguito della pubblicazione su una rivista di un articolo contenente informazioni su un procedimento penale a carico di alcuni politici, che per la legge francese avrebbero dovuto rimanere riservate così da non violare il principio della presunzione d'innocenza. In questo caso, pur potendo rilevare a primo impatto un interesse pubblico nel venire a conoscenza di simili fatti, in realtà le disposizioni statali sarebbero state violate al trapelare delle notizie.

Come emerge dagli esempi riportati, nel caso di limitazioni, è indispensabile che vi sia un'esigenza legittima interpretata accuratamente e stabilita con certezza, che giustifichi il blocco della circolazione delle notizie, come stabilito nel caso *Observer and Guardian v. The United Kingdom*[4].

2. Il bilanciamento tra l'articolo 10 della CEDU e gli altri diritti secondo la Corte Europea dei Diritti dell'Uomo.

Come si accennava poc'anzi, la Corte Europea dei Diritti dell'Uomo ha dovuto affrontare i diversi casi che le sono stati

[3] Du Roy e Malaurie v. France, N. 34000/96, ECHR 2001 in hudoc.echr.coe.int.
[4] Observer and Guardian v. The United Kingdom, N. 13585/88, §45, ECHR 1991in hudoc.echr.coe.int.

sottoposti, domandandosi molto spesso se effettivamente la tutela di altri diritti costituisse un'interferenza prevalente rispetto all'art. 10 della CEDU. Per procedere alla gestione di una simile eventualità, si è interrogata su quale fosse la legge nazionale da considerare, analizzandone la sua accessibilità e conoscibilità. Inoltre, dal momento che solo un'esigenza legittima può limitare la libertà di informazione, la Corte ha analizzato la proporzionalità della suddetta restrizione ai fini prefissati dalla disposizione, domandandosi se tale contrasto fosse giustificabile in quanto necessario in una società democratica.

Il criterio della "necessità", comunque, non deve essere confuso con un giudizio arbitrario sull'utilità della limitazione poiché, per quanto le decisioni vengano prese caso per caso, l'interferenza deve sempre rispondere ad un urgente bisogno sociale, essere commisurata allo scopo perseguito nonché avere ragioni adeguate e rilevanti . Ad esempio, nel 2012, la sentenza Von Hannover c. Germania ha visto il tentativo di bilanciare la tutela della vita privata (art. 8 CEDU) con l'interesse pubblico a ricevere le notizie relative alla ricorrente e alla sua famiglia. Nel caso in esame, la principessa Carolina di Monaco e il marito Ernst von Hannover si erano rivolti a un tribunale tedesco per impedire che due settimanali pubblicassero un articolo e diverse fotografie della Principessa in vacanza con la famiglia. La Corte, partendo dalle disposizioni relative alla tutela della vita privata, ha sentenziato che la divulgazione del materiale non avrebbe comportato alcuna violazione dei diritti sanciti dall'art. 8 della CEDU, visto il ruolo pubblico dei ricorrenti e dal momento che le foto erano state scattate in un luogo pubblico. Anche in questo caso, il ragionamento giuridico della Corte è partito dall'individuazione della norma che tutela l'obbligo positivo, in capo agli Stati aderenti alla Convenzione, di assicurare la protezione della vita privata di ciascun individuo sotto la propria giurisdizione (art. 8 CEDU), effettuando in seguito un bilanciamento tra il diritto al rispetto della vita privata e la libertà di informazione garantita dall'articolo 10. Secondo l'opinione della Corte, la libertà d'informazione, non si limita alla diffusione di notizie di natura politica, ma può anche esplicitarsi nella pubblicazione di notizie relative alla vita privata di personaggi pubblici. Nel caso di Carolina di Monaco, la liceità della pubblicazione delle foto che la

ritraevano con la famiglia, era anche garantita dal fatto che la ricorrente fosse a conoscenza degli scatti, avvenuti in un luogo pubblico ancorché durante un momento privato.

Viceversa, nella causa Axel Springer AG c. Germania (n.2) del 2012, la Corte ha stabilito la colpevolezza dello Stato tedesco per violazione dell'articolo 10, condannandolo a risarcire i danni all'editore ricorrente. Nel caso in esame, la società editrice del quotidiano Bild si accingeva a pubblicare la vicenda di un attore televisivo, condannato in recidiva per consumo e possesso di una modica quantità di stupefacenti. L'uomo si era rivolto ai tribunali nazionali per ottenere il divieto di pubblicazione, accolto dalla corte domestica la quale aveva sentenziato la ridotta importanza del suo reato rispetto alla rilevanza data alla notizia dal giornale. Secondo il tribunale il caso aveva ricevuto più attenzione di quanta ne servisse per soddisfare l'interesse pubblico di mettere i cittadini a conoscenza dei fatti, considerata la scarsa fama dell'attore. La Corte di Strasburgo, a seguito del ricorso, ha cercato di bilanciare la libertà di stampa con il diritto alla riservatezza, applicando i criteri relativi all'interesse generale in rapporto alla notorietà della persona e alla veridicità delle informazioni. Così, essa è giunta alla conclusione che l'attore aveva una notorietà sufficiente a considerarlo "personaggio pubblico" e che, per questo, il pubblico aveva interesse ad essere informato sui fatti, peraltro esposti in modo veritiero e senza conseguenze pregiudizievoli per l'uomo, giacché egli stesso aveva rilasciato numerose interviste sull'uso di stupefacenti. In questo caso, dunque, lo Stato fu condannato al risarcimento dei danni al quotidiano ricorrente, utilizzando il criterio elaborato nella sentenza von Hannover, il cui esito era stato il prevalere della libertà di informazione sul diritto al rispetto della vita privata.

A dimostrazione dell'importanza data all'articolo 10 della CEDU, vi è anche il celebre caso Casado Coca c. Spagna del 1994, nel quale la Corte ha dimostrato che la libertà di informazione non vale soltanto per le notizie di interesse pubblico, ma anche per quelle relative all'ambito commerciale. In tale caso, infatti, un avvocato spagnolo aveva pubblicato annunci relativi alla sua professione, su alcuni giornali barcellonesi e sulla Rivista tedesca di Spagna, a seguito dei quali il Consiglio dell'Ordine Nazionale aveva comminato varie

sanzioni e richiami, giacché le informazioni non ricadevano sotto la tutela dell'articolo 20 della Costituzione spagnola che, pur tutelando la libertà di espressione, non considera la diffusione di pubblicità come un diritto fondamentale. Oltretutto, l'intento dell'uomo non era informativo ed andava contro il Regolamento dell'Ordine degli Avvocati di Barcellona poiché era da ritenersi una forma di concorrenza sleale nei confronti degli altri colleghi. In seguito a ciò, dopo aver adito tutti i gradi di giudizio nazionali, l'uomo si era rivolto all'organo europeo, che però aveva confermato quanto stabilito dai tribunali domestici. In effetti, nonostante la Corte ritenesse anche il "commercial speech" tutelabile ai sensi dell'articolo 10 della CEDU, nel caso di specie la pubblicità serviva un interesse privato, non pubblico, fuoriuscendo dall'ambito di applicazione delle disposizioni in esame. Per questo motivo, le attività di advertising possono essere limitate se il fine è quello di prevenire la concorrenza sleale e impedire la pubblicità ingannevole e, in tal senso, sia l'Ordine degli Avvocati sia il tribunale spagnolo avevano compiuto un corretto bilanciamento tra la libertà di informazione e i diritti degli altri avvocati stabiliti nel Regolamento.

In sostanza, dunque, se da un lato la libertà di cui all'articolo 10 si estende fino al punto da ricomprendere la diffusione al pubblico di informazioni che possono essere ritenute scomode o seccanti, dall'altro essa non può minare altri valori egualmente protetti dalla Convenzione, senza che vi sia un bilanciamento tra essi. Un esempio di questa impostazione è rappresentato dal caso Herczegfalvy c. Austria (1992), in cui la Corte riscontrò una violazione del diritto di ricevere informazioni laddove ad un uomo in stato di detenzione psichiatrica era stato negato l'accesso a letture, radio e televisione, pur non essendoci alcuna legge nazionale che prevedeva siffatto diritto.

Parallelamente, anche nel caso di Open Door e Dublin Well Woman c. Irlanda (1992) è stato sanzionato lo Stato che ha impedito il rilascio da parte di due centri erogatori di servizi sanitari rivolti alle donne, di informazioni relative all'aborto negli altri stati. La decisione nazionale, per la Corte, andava contro le libertà di cui all'art. 10 CEDU in quanto tali informazioni non solo sarebbero state reperibili altrove, ma soprattutto non erano vietate da alcuna legge irlandese.

In conclusione, la libertà di espressione e la libertà di informazione vengono tutelate per garantire il mantenimento dei valori democratici e l'interesse pubblico alla notizia, che però non va confuso con l'interesse a soddisfare la curiosità del pubblico. Talvolta, tali libertà prevalgono perfino su interessi e diritti soggettivi perfetti come esemplificato, da un lato, dal caso von Hannover, in cui la Corte ha fatto prevalere l'articolo 10 sull'articolo 8 della Convenzione, e dall'altro dal caso Casado Coca, nel quale l'interesse individuale del ricorrente a pubblicizzare la propria attività professionale ha dovuto cedere il passo a interessi pubblici nazionali confliggenti, come quello alla tutela della concorrenza.

3. L'impatto di internet sul pluralismo dell'informazione e il ruolo dei motori di ricerca.

Quando si parla di interesse pubblico all'informazione, non si può prescindere dal considerarlo legato al pluralismo delle fonti, fondamentale per ogni stato democratico poiché direttamente connesso con il profilo passivo della libertà di informazione stessa, inteso come il diritto a ricevere le notizie da fonti il più possibile diversificate. Per garantire che i cittadini possano esercitare i loro diritti e le loro libertà di scelta e di giudizio, ad essi deve essere garantito il libero accesso alle informazioni che, non a caso, viene considerato un diritto fondamentale. Il controllo sui flussi di notizie e di dati, al contrario, preluderebbe alla manipolazione dell'opinione pubblica nonché alla concentrazione di potere cui hanno sempre aspirato i regimi autoritari attraverso la censura e il controllo delle reti di informazione. Per questi motivi, il già citato articolo 11 della Carta dei Diritti Fondamentali dell'Unione europea afferma che la libertà e il pluralismo dei mezzi di comunicazione devono essere rispettati come elementi essenziali della democrazia promossa dall'Unione, mentre l'articolo 10 della CEDU esclude che «*vi possa essere ingerenza da parte delle autorità pubbliche*».

La tutela del pluralismo dell'informazione, inoltre, non può essere circoscritta alla questione del mantenimento di un mercato dei *media* concorrenziale, ovvero alla limitazione di concentrazioni proprietarie,

ma necessariamente comprende una regolazione capace di perseguire finalità extra-giuridiche ed extra-economiche, quali la promozione e la protezione della libertà di stampa, della diversità culturale, della libertà di ricerca e dell'indipendenza editoriale. Per questo, lo sviluppo della società dell'informazione ha un forte legame con la questione del pluralismo dei mezzi di comunicazione: all'interno di essa i cittadini sono in grado di contribuire al dibattito democratico attraverso diversi canali che vanno ad aggiungersi a quelli tradizionali. Questo tipo di *struttura organizzativa* dell'informazione e la nozione multidimensionale di pluralismo sono alla base della democrazia, la quale deve necessariamente affondare le sue radici in una sfera pubblica bene informata, inclusiva e pluralista che riceva dai media informazioni di natura diversa ed indipendente dal potere politico. Si può dire, dunque, che il pluralismo nel contesto europeo si è tradotto in un approccio normativo che tende a garantire che gli stati adottino politiche funzionali a promuovere la libertà di informazione sia dal punto di vista degli operatori sia da quello degli utenti. Infatti, i governi hanno un ruolo attivo nel garantire la circolazione e il reperimento di diversi punti di vista funzionali alla formazione dell'opinione pubblica (vedi ancora gli articoli 10 CEDU e 11 Carta dei Diritti Fondamentali dell'UE). In tal senso, la nascita del web ha favorito l'incremento del pluralismo, poiché la Rete ha contribuito all'aumento quantitativo delle fonti e dei punti di vista consultabili nella valutazione delle notizie, grazie alla neutralità del mezzo rispetto alle informazioni veicolate e all'assenza di controllo da parte dei poteri pubblici o privati – almeno nei paesi democratici – favorita dall'a-territorialità del web. In questa ottica, il pluralismo dell'informazione ha conosciuto un incremento dato dalla possibilità per le nuove organizzazioni di entrare a far parte del panorama informativo, affiancandosi alle fonti tradizionali e consolidate.

Peraltro, secondo l'indagine conoscitiva sul settore dei servizi internet e sulla pubblicità online dell'AGCOM[5], redatta nel 2013, in Italia il 42,1% degli individui si informa sulle notizie (locali, nazionali e internazionali) attraverso internet, che è la terza fonte più usata dopo televisione e quotidiani. Questo dato dimostra la primaria importanza

[5] Allegato A alla Delibera n. 19/14/CONS, in www.agcom.it.

che la rete sta assumendo nel soddisfare la ricerca di notizie sull'attualità, tant'è che nel rapporto dell'Indagine si afferma: *«[...] occorre poi tenere conto della crescente rilevanza del mezzo di comunicazione sotto il profilo del pluralismo informativo, stante la diffusione tramite il web di nuovi modelli di informazione e nuovi servizi di erogazione delle news, con evidenti riflessi sugli assetti tradizionali e sulle dinamiche dei mercati della comunicazione»*[6].

In effetti, tenendo conto del fatto che i contenuti informativi del web sono spesso gratuiti, ciò stimola l'interesse e il dibattito pubblico anche di coloro che non acquistano i quotidiani o che non ascoltano il telegiornale. Questa estrema apertura di internet, però, ha spesso portato a riflettere sulla qualità delle notizie offerte, che molti considerano di scarsa qualità, poiché, logicamente, le fonti non sono sempre verificate o verificabili e costituiscono, in alcuni casi, opinioni del tutto arbitrarie. La multipolarità di internet è dunque la sua forza ma un po' anche il suo limite, dal momento che ogni utente può pubblicare contenuti senza essere vincolato da norme giornalistiche o etica professionale, bensì agendo semplicemente sulla base del suo diritto alla libertà di espressione e informazione, garantito a partire dai trattati internazionali. L'estrema facilità di accesso alla rete internet e di generazione di contenuti per il suo tramite non va considerato in termini negativi, poiché siffatte possibilità hanno consentito di veicolare istanze di libertà di parola, come nel caso del *citizen journalism* da cui è in parte scaturita la Primavera araba tra il 2010 e il 2011. E' chiaro che, in un contesto del genere, i motori di ricerca hanno un forte impatto sulla mediazione tra interessi così diversi, poiché essi si pongono come "intermediari digitali" che forniscono l'accesso all'informazione, aiutando il pluralismo inteso tanto come accesso quanto come scelta delle informazioni da parte degli utenti. In tal senso, infatti, i *search engines*, aumentano le fonti da cui attingere e garantiscono la totale personalizzazione dell'esperienza informativa, amplificando il surplus informativo tipico dell'*information society*. Il loro servizio supporta orizzontalmente coloro che si approcciano al web, aiutandoli a navigare tra le risorse disponibili in rete e orientandoli nel reperimento delle informazioni. Essi, infatti,

[6] Allegato A alla Delibera n. 19/14/CONS, pag. II, in www.agcom.it.

contrariamente a quanto accade con i siti internet e i prodotti editoriali, non nascono per soddisfare bisogni specifici, bensì indirizzano l'utente verso il servizio che sta cercando. Ciò acquista maggior rilevanza se si tiene conto del fatto che, proprio grazie ai motori di ricerca, anche le persone più giovani hanno incrementato il loro interesse alle notizie, amplificando i caratteri originari di libertà informativa della società dell'informazione. In ogni caso, si può sicuramente affermare che, nonostante anche nelle democrazie si sia storicamente abituati ad avere mezzi di informazione proprietari, internet ha consentito il decentramento e l'interconnessione, amplificata dalla capacità dei *search engines* di aggregare diverse fonti contribuendo all'informazione e alla formazione dell'opinione pubblica. Questi ultimi, infatti, come rilevato dall'Indagine dell'AGCOM, sono utilizzati da una gran parte della popolazione mondiale («*In Italia pari al 12,4% della popolazione e al 21,6% degli utenti che navigano*»[7]) per ricercare notizie di ogni genere e Google rappresenta il portale più utilizzato a questi fini, sia in Italia (21,5% degli utenti[8]) che nel mondo (76,6%[9]). In proposito, però, si è criticata la capacità dei motori di ricerca di creare la cd. "*filter bubble*",[10] cioè quel meccanismo prodotto grazie ad un algoritmo che "indovina" selettivamente quali informazioni l'utente desidera ottenere in base alle informazioni di cui dispone su di esso. Ciò, se non gestito correttamente e con trasparenza, può comportare non soltanto l'allontanamento dell'individuo dalle informazioni contrarie al suo punto di vista, ma anche il suo isolamento in vere e proprie "bolle" culturali ed ideologiche.

A questa riflessione si affianca quella relativa alla questione del difficile bilanciamento tra l'interesse pubblico e la tutela di altri diritti, come la privacy, la reputazione, il diritto al controllo sui propri dati e l'accesso, accentuata proprio dalla pervasività del mezzo, il cui raggio di azione si estende oltre i confini nazionali e comporta la reperibilità del materiale ovunque ed in qualsiasi momento. In questo senso, nel

[7] Ibid. pag. XXI.
[8] Ibid.
[9] Indagine comScore, febbraio 2013, in www.comscore.com.
[10] Cfr. E. PARISIER, *The Filter Bubble: How the New Personalized Web Is Changing What We Read and How We Think*, The Penguin Press, New York, 2011.

settembre del 2011, il Comitato dei Ministri del Consiglio d'Europa ha adottato la Dichiarazione sugli *Internet Governance Principles*, nella quale si è stabilito proprio come primo assunto che la rete debba assicurare la protezione di tutti i diritti e le libertà fondamentali, affermando la loro universalità in accordo con i diritti umani riconosciuti a livello internazionale, nella garanzia del rispetto delle leggi esistenti e della democrazia.[11]

Tornando ai motori di ricerca, in un simile contesto essi hanno l'importante funzione di mediare tra le fonti di informazione e il pubblico, mettendo a disposizione degli utenti uno strumento essenziale per il reperimento delle notizie che consente di aggregare diverse fonti, siano esse giornalistiche o meno. A ciò giova il fatto che il fenomeno del cd. "*filter bubble*" non sembra essersi affatto tradotto in una riduzione della varietà dell'offerta. Al contrario, i diversi *search engines* forniscono molte opportunità per scoprire fortuitamente nuovi risultati (ad esempio con funzione di ricerca casuale che estrae un link in modo aleatorio) oppure di incrementare il panorama di notizie a partire da suggerimenti a proposito di "ricerche correlate". Inoltre, i meccanismi di semplificazione che aiutano l'utente a soddisfare le sue esigenze lo incoraggiano anche a confrontarsi con altri argomenti di cui può avere scarsa conoscenza, proprio perché stimolato dalle agevolazioni nella ricerca permesse dal servizio. Dunque, come sottolineato dallo *Study on liability of internet intermediaries*[12], realizzato nel 2006 per verificare le modalità di recepimento da parte dei diversi Stati membri della direttiva sul commercio elettronico, i motori di ricerca soddisfano un bisogno sociale attraverso la facilitazione della navigazione per gli utenti.

Per tutte queste ragioni, si sono configurati due scenari di estrema rilevanza nella valutazione del ruolo dei *search engines*, che hanno trovato riscontro nelle più recenti decisioni europee. Da un lato, è sorta spontanea la riflessione sul ruolo dei provider di ricerca rispetto alla figura tradizionale dell'editore, che non pare essere

[11] Declaration by the Committee of Ministers on Internet governance principles, *Human rights, democracy and the rule of law*, Committee of Ministers, 21 September 2011, in wcd.coe.int.

[12] G. SPINDLER, G.M. RICCIO, A. VAN DER PERRE, *Study on liability of internet intermediaries*, Thibault Verbiest, 2007, in ec.europa.eu.

sovrapponibile *sic et simpliciter* a quella dei *content* e *service providers, soprattutto in ragione della problematica attribuzione a questi ultimi soggetti* della cd. responsabilità editoriale. Dall'altro, invece, si è tentato di capire in che modo tutelare il diritto di accesso all'informazione rispettando altri diritti degli individui, eventualmente confliggenti col primo. Infatti, la pervasività di internet, cresciuta grazie ai motori di ricerca, fornisce un'ampia pubblicità alle notizie, aprendo il dibattito su tutta una serie di questioni, non ultima quella del diritto all'oblio correlata al soddisfacimento dell'interesse pubblico a ricevere informazioni.

4. *Search engines responsibility* ed estensibilità del concetto di "editore" al motore di ricerca.

La società dell'informazione si fonda sui servizi erogati dalle tecnologie Internet e da quelle della telefonia mobile, e si è sviluppata entro il perimetro di politiche previste dal Titolo XIX del Trattato sul funzionamento dell'Unione europea ("Ricerca e Sviluppo Tecnologico e Spazio")[13]. Nel quadro della *information society* è stata adottata la direttiva 2000/31/CE sul commercio elettronico, che «*mira a contribuire al buon funzionamento del mercato garantendo la libera circolazione dei servizi della società dell'informazione tra Stati membri*»[14].

All'interno di questa cornice legale, gli intermediari dei servizi della società dell'informazione (*information society service providers*) sono stati genericamente definiti dalla direttiva come macrocategoria, a sua volta ricompresa sotto la figura dei "prestatori" di servizi della società dell'informazione, che racchiude diversi tipi di fornitori, poiché per "prestatore" si intende in generale «*la persona fisica o giuridica che presta un servizio della società dell'informazione*».[15] All'interno dell'insieme dei "prestatori", dunque, si possono

[13] Titolo XIX – Ricerca e sviluppo tecnologico e spazio, Trattato sul funzionamento dell'Unione Europea, in eur-lex.europa.eu.
[14] Direttiva 2000/31/CE, Art. 1 – Obiettivi e campo di applicazione, in eur-lex.europa.eu.
[15] Direttiva 2000/31/CE, Art. 2, punto b) – Definizioni, in eur-lex.europa.eu.

individuare sia gli editori – che immettono direttamente i contenuti – sia i *providers* di servizi intermediari quali *mere conduit*, *caching* e *hosting*, nonché quei prestatori che non si occupano di elaborare i contenuti, bensì di indicizzarli, come avviene nei motori di ricerca. A tal proposito, la direttiva del 2000 si sofferma sull'individuazione delle responsabilità dei prestatori intermediari escludendo la possibilità di attribuire loro un obbligo generale di sorveglianza o di ricerca attiva degli illeciti. Infatti, all'art. 15 si afferma che: «*Nella prestazione dei servizi di [mere conduit, caching e hosting] gli Stati membri non impongono ai prestatori un obbligo generale di sorveglianza sulle informazioni che trasmettono o memorizzano né un obbligo generale di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite. Gli Stati membri possono stabilire che i prestatori di servizi della società dell'informazione siano tenuti ad informare senza indugio la pubblica autorità competente di presunte attività o informazioni illecite dei destinatari dei loro servizi o a comunicare alle autorità competenti, a loro richiesta, informazioni che consentano l'identificazione dei destinatari dei loro servizi con cui hanno accordi di memorizzazione dei dati*». Tutto ciò avviene fermo restando che, per i servizi di *mere conduit*, *caching* e *hosting*, gli artt. 12, 13 e 14 lasciano «*impregiudicata la possibilità, per un organo giurisdizionale o un'autorità amministrativa, in conformità agli ordinamenti giuridici degli Stati membri, di esigere che il prestatore ponga fine ad una violazione o la impedisca*». Chiaramente, vista la peculiarità dei servizi di hosting, coloro che li forniscono possono anche essere soggetti a «*procedure per la rimozione delle informazioni o la disabilitazione dell'accesso alle medesime*»[16] definite dagli Stati membri.

All'interno di questo contesto e considerate le caratteristiche dei motori di ricerca, essi si identificano come un *internet service provider*, e non come un *editore*, proprio perché non hanno alcun potere di controllo sui contenuti e per questo è esclusa la loro responsabilità editoriale. Queste posizioni vengono confermate dalla CGE nelle sentenze in cui essa ha escluso che i motori di ricerca potessero essere considerati responsabili di violazioni di diritti di

[16] Art. 14 comma 3, Direttiva 2000/31/CE, in eur-lex.europa.eu.

proprietà industriale. Un esempio è costituito dalla causa Google c. Vuitton[17], relativa alla visualizzazione tra i risultati di ricerca di link pubblicitari «a partire da parole chiave corrispondenti a marchi di impresa a prodotti o servizi identici a quelli per cui detto marchio è registrato»[18]. In proposito, la Corte ha affermato che «qualora la pubblicità di cui trattasi non consenta, o consenta soltanto difficilmente, all'utente medio di Internet di sapere se i prodotti o i servizi indicati nell'annuncio provengano dal titolare del marchio o da un'impresa economicamente connessa a quest'ultimo o invece da un terzo»[19], l'articolo 14 della direttiva sul commercio elettronico 200/31/CE «deve essere interpretato nel senso che la norma ivi contenuta si applica al prestatore di un servizio di posizionamento su Internet qualora detto prestatore non abbia svolto un ruolo attivo atto a conferirgli la conoscenza o il controllo dei dati memorizzati. Se non ha svolto un siffatto ruolo, detto prestatore non può essere ritenuto responsabile per i dati che egli ha memorizzato su richiesta di un inserzionista, salvo che, essendo venuto a conoscenza della natura illecita di tali dati o di attività di tale inserzionista, egli abbia omesso di prontamente rimuovere tali dati o disabilitare l'accesso agli stessi»[20]. Dunque, la sentenza esclude la responsabilità del motore di ricerca proprio perché i dati che esso memorizza provengono da una richiesta dell'inserzionista e su di essi non può esercitare alcun tipo di controllo editoriale. Per lo stesso principio, si può escludere la responsabilità editoriale dei *search engines* quando essi forniscono risultati di ricerca che costituiscono semplicemente un collegamento con le pagine dei *content providers*. Si tratta infatti di un'operazione che risponde a criteri di organizzazione automatica e dalla quale non consegue alcuna modifica dei contenuti, se non una loro citazione in ordine di rilevanza e di pertinenza. Volendo riprendere la sentenza di

[17] Procedimenti riuniti da C-236/08 a C-238/08, Corte di Giustizia Europea, Sezione Grande, 23 marzo 2010, in curia.europa.eu.

[18] Punto 2, Procedimenti riuniti da C-236/08 a C-238/08, Corte di Giustizia Europea, Sezione Grande, 23 marzo 2010, in curia.europa.eu.

[19] Punto 121, Procedimenti riuniti da C-236/08 a C-238/08, Corte di Giustizia Europea, Sezione Grande, 23 marzo 2010, in curia.europa.eu.

[20] Punto 120, Procedimenti riuniti da C-236/08 a C-238/08, Corte di Giustizia Europea, Sezione Grande, 23 marzo 2010, in curia.europa.eu.

cui sopra, dunque, si può affermare che nel caso in cui un utente effettui una ricerca, i risultati proposti dal *service provider* derivano dalla scansione di tutti i contenuti già presenti nel web e sui quali il motore di ricerca non può esercitare alcun tipo di controllo editoriale. Peraltro, il Considerando n. 42 della direttiva 2000/31/CE stabilisce che: «*Le deroghe alla responsabilità stabilita nella presente direttiva riguardano esclusivamente il caso in cui l'attività di prestatore di servizi della società dell'informazione si limiti al processo tecnico di attivare e fornire accesso ad una rete di comunicazione sulla quale sono trasmesse o temporaneamente memorizzate le informazioni messe a disposizione da terzi al solo scopo di rendere più efficiente la trasmissione. Siffatta attività è di ordine meramente tecnico, automatico e passivo, il che implica che il prestatore di servizi della società dell'informazione non conosce né controlla le informazioni trasmesse o memorizzate*».

All'interno di queste attività, ovviamente, ricade quella del *search engine*, poiché esso fornisce l'accesso ai contenuti della rete mediante l'indicizzazione dei risultati di ricerca per renderne più facile il reperimento, nonché per garantire all'utente il diritto di accesso alle informazioni che circolano sul web. Un altro aspetto rilevante dei servizi offerti dai motori di ricerca è quello di consentire la navigazione tra le risorse della rete attraverso l'inserimento di alcune parole chiave gestite da un algoritmo che indicizza i dati individuati. Attraverso la scansione del web, infatti, i *search engines* costruiscono un indice, calcolando l'attinenza rispetto alle parole chiave e ordinando i risultati in base alla popolarità delle pagine, in modo da poter fornire risposte utili ai criteri di ricerca dell'utente. In questo senso, il *search engine* si serve di un software (cd. *spider*) che crea liste di parole trovate sui siti, sia nella pagina che in sequenza (cd. *web crawling*). A conclusione di questo processo, il motore di ricerca indicizza i risultati trovati ordinando le pagine sia per il numero di volte in cui compare la parola ricercata sia in funzione del numero di citazioni della pagina (popolarità). Per tale motivo, la reperibilità di informazioni pone la delicata questione dell'impatto degli algoritmi sulla diffusione dei dati sia dal punto di vista degli operatori che da quello degli utenti, poiché in entrambi i casi la maggiore o minore rilevanza del risultato viene decisa da criteri automatici di selezione.

5. *Search engine*: un'analisi econometrica empirica.

La conseguenza naturale di quanto precedentemente affermato era verificare il tipo di impatto che i motori di ricerca hanno avuto sui siti, sul numero di visite ricevute e quindi sulla rilevanza che i siti stessi ottengono grazie ai motori di ricerca.

L'avvento di motori di ricerca sempre più efficienti e numerosi ha sicuramente permesso la nascita di più siti internet, ed in particolare di siti di qualità superiore. Difatti, classificando i siti in base al numero assoluto di visite ricevute o secondo la numerosità di link esterni che rimandano al sito stesso, si ha la virtuale certezza che un sito con una informazione di migliore qualità sia più facilmente accessibile di altri aventi informazioni meno rigorose. Purtroppo tale certezza è solo teorica dal momento che I) i più efficaci metodi di ranking garantiscono l'equivalenza "informazione migliore uguale ranking più elevato" solo nella quasi totalità dei casi, poiché potrebbero essere soggetti ad errore, e II) gli algoritmi di classificazione potrebbero essere volutamente distorti al fine di garantire una visibilità più elevata ad alcuni siti specifici. Tali algoritmi non sono inoltre così semplici ma, anzi, tanto complicati da non essere pienamente compresi se non da un ristretto gruppo di persone tecnicamente molto qualificate. Il regolatore si trova quindi ad affrontare l'eterno dilemma del libero mercato: obbligare ogni agente a fornire una piena *disclosure* sul funzionamento della *"black box"*, ma erodendone cosi ogni fonte di vantaggio competitivo, o lasciare che il mercato si autoregoli con il rischio, però, che qualche manipolazione possa essere perpetuata da un singolo a danno di molti.

Esiste, tuttavia, una soluzione mediana che, invece di preoccuparsi della causa del problema (apparentemente irrisolvibile), ne cura perlopiù gli effetti. In questo scenario, ciò di cui un regolatore dovrebbe preoccuparsi non è effettivamente capire i meccanismi interni agli strumenti utilizzati, quanto piuttosto assicurarsi che gli effetti e le potenziali esternalità non si rivelino essere lesivi per il libero mercato. Pertanto, ciò che quindi diventa rilevante per regolare i motori di ricerca da un punto di vista normativo, è verificare che il traffico derivante da tali motori non distorca in alcun modo la concorrenza e che non permetta ad alcuni siti di beneficiare

sistematicamente di eventuali singolarità strutturali. In altri termini, un motore di ricerca non dovrebbe avere preferenze proprie, bensì esprimere le preferenze degli utenti della rete. Più specificatamente, si è voluto constatare da un punto di vista empirico che i siti che dipendono maggiormente dal *traffico search*, ovvero dal traffico derivante dai motori di ricerca, crescono in modo rapido e sostanziale nel numero di visualizzazioni ricevute e nel ranking dei siti più visualizzati, sebbene ad una crescita percentuale del numero di visite non corrisponda una crescita della stessa intensità all'interno della classifica dei siti più visitati. Le implicazioni derivanti da questa analisi mostrerebbero che i motori di ricerca sono strumenti fondamentali per la visibilità di un sito poiché permettono ad una base di utenti più ampia di accedervi, ma che uno sbilanciamento eccessivo verso tali motori potrebbe essere controproducente a livello competitivo. In altre parole, un sito che si affida unicamente (o principalmente) ad un motore di ricerca come canale divulgativo diventa sì più popolare, ma non quanto, ad esempio, un suo competitor che si avvale in egual misura di motori di ricerca e social networks.

Inoltre, sebbene sia possibile verificare che siti dipendenti maggiormente dal *traffico search* crescono nel ranking (anche se non come siti con fonti di accesso multiple), è possibile anche osservare che siti che inizialmente si collocano negli ultimi percentili della distribuzione crescono invece più rapidamente, ovvero i siti che in principio occupano le posizioni più basse nella classifica scalano la graduatoria più rapidamente grazie al *traffico search* rispetto a quelli che inizialmente erano posizionati più in alto nel ranking. Quindi, siti inizialmente meno visitati godono maggiormente degli effetti di una ricerca effettuata su un motore rispetto a siti molto più noti e conosciuti. Sembra infatti intuitivo che un utente non usi un motore di ricerca per cercare un sito di cui conosce esattamente l'URL perché estremamente famoso (come ad esempio la BBC), ma piuttosto utilizzi il motore per ricercare siti meno noti (come ad esempio "La gazzetta di Parma" o "Noz").

Ricapitolando, un sito che sfrutta intensamente i motori di ricerca come canali di accesso sembra ricevere un numero più elevato di visualizzazioni poiché essi sono oggigiorno fondamentali e, tanto più piccolo è il sito, tanto maggiore è l'effetto positivo dei motori di

ricerca. Tuttavia, non ci si dovrebbe concentrare unicamente su questo mezzo di comunicazione bensì avvantaggiarsi di un portafoglio variegato di fonti, come ad esempio social networks, mailing lists o pop-up pubblicitari. Al fine di verificare le ipotesi sopra proposte, sono stati quindi raccolti dati riguardanti il traffico Internet da SimilarWeb.com, un sito che fornisce principalmente dati grezzi sull'audience di un sito, sulle sue fonti e sui re-indirizzamenti dal sito verso altri siti e viceversa. I dati selezionati riguardano il settore *News and Media* in Italia e Germania, paesi ritenuti significativi per quanto riguarda il quadro legale e la diffusione dell'informazione. Per ogni paese, sono stati estratti i primi cento siti internet classificati in base al numero di visite ricevute e i relativi *Global ranking*, *Country ranking* e *Category ranking*, rispettivamente le posizioni nella classifica globale (rispetto, quindi, ad ogni altro sito), nel paese dove il sito è più utilizzato e all'interno della categoria *News and Media*. Per ogni sito è stato quindi calcolato il volume totale di visite ricevute e la relativa scomposizione delle fonti che l'utente ha utilizzato per accedere a tale sito. Nel dettaglio, sono state raccolte informazioni riguardo l'esatto numero di visite per i mesi di Giugno 2013 e Maggio 2014 (l'arco temporale è dunque annuale), derivanti da una ricerca diretta del sito stesso (*Direct*), da link forniti tramite email (*Mail*), da altri siti con click diretti verso il sito considerato (*Referrals*), da motori di ricerca (*Search*), da social networks (*Social*) ed infine da annunci pubblicitari (*Display ads*). I dati sono stati quindi inizialmente sottoposti ad una convalida incrociata intervistando casualmente alcune tra le maggiori testate giornalistiche italiane per verificare la veridicità delle informazioni fornite da SimilarWeb.com.

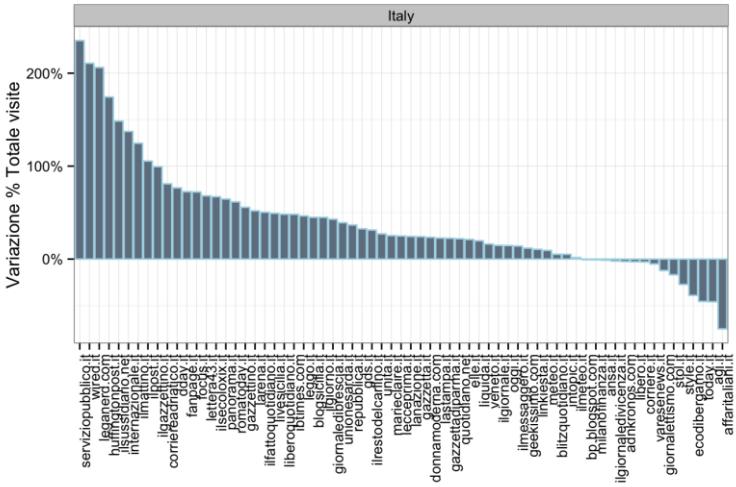
Infine, dati riguardanti il tempo trascorso in media sul sito internet cercato, le pagine del sito internet in media visualizzate durante ogni visita ed il *bounce rate*[21], sono stati usati in fase di preliminare per accertare la classifica fornita e controllare che fosse consistente non solo in base al numero complessivo di visite ricevute nel periodo considerato, ma anche rispetto a parametri qualitativi più robusti. In questo modo, si è avuta la certezza che nella classifica non ci fossero

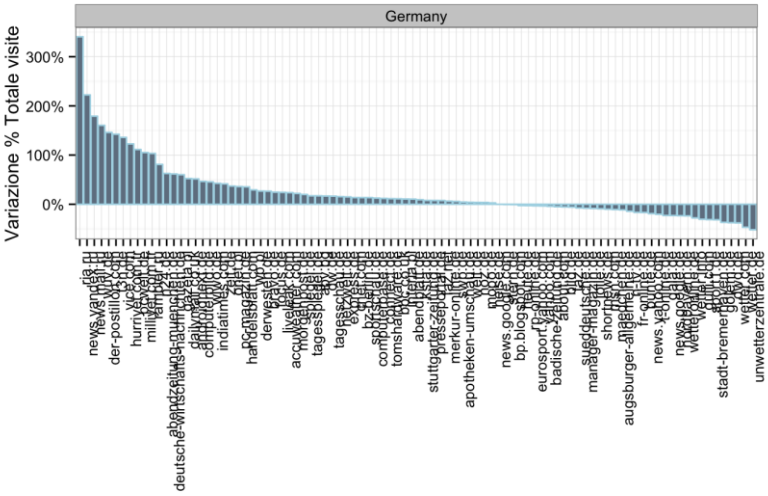
[21] Il *Bounce Rate* é un indicatore della percentuale di utenti che abbandonano il sito solo dopo pochi secondi ed avendo visto solo la prima pagina del sito.

siti internet "sospetti", ovvero siti internet che vengono cliccati molte volte anche solo casualmente o perché compaiono sotto forma di pubblicità o pop-up. Le prime statistiche descrittive che risultano da un'analisi preliminare del dataset così costruito mostrano la crescita mensile dei singoli siti dovuta all'insieme di fonti di accesso utilizzate. Quindi, grazie ai primi due grafici, è possibile rispondere alla seguente domanda: indipendentemente da quanto un sito sfrutti i social networks o i motori di ricerca, di quanto ha aumentato (diminuito) il numero di visite ricevute nel mese passato? Le figure seguenti mostrano come sia per l'Italia (prima figura) che per la Germania (seconda figura), la maggior parte dei siti abbia incrementato il loro numero di contatti tra Giugno 2013 e Maggio 2014. Questo sembra essere tanto più vero quanto più è piccolo il sito, idea intuitiva se si considera che si stanno analizzando le variazioni percentuali di crescita e non quelle assolute. Usando un esempio, difficilmente "libero.it", che riceve quasi cento milioni di visite mensili, potrà raddoppiare il suo volume di contatti in un mese, essendo un sito già maturo e con una base di lettori molto consolidata. Tutto ciò risulta essere molto più semplice, ad esempio, per "leganerd.com", sito che riceve mensilmente "solo" 350.000 visite circa. Bisogna tuttavia specificare che, per tutte le analisi compiute, non esiste una relazione causale univoca ma che molti altri fattori potrebbero essere utili e da considerare per spiegare i vari fenomeni. Ciò nondimeno, si ritiene che i dati raccolti e le analisi effettuate siano in grado di catturare un trend più generale in modo alquanto accurato.

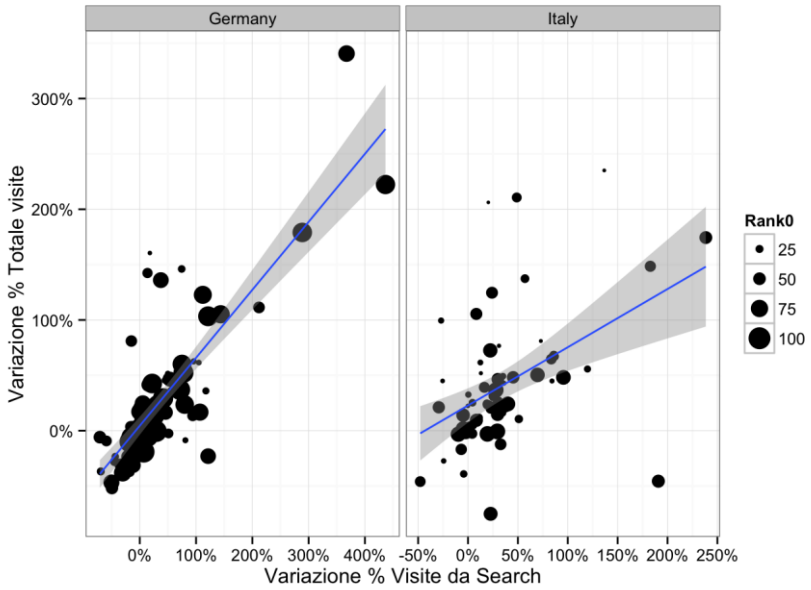
Per quanto riguarda la situazione italiana, l'istogramma mostra che i primi siti ("Serviziopubblico.it", etc.) addirittura raddoppiano di dimensione grazie all'insieme indistinto di fonti utilizzate, mentre soltanto pochissimi siti sembrano perdere visitatori ("Affaritaliani.it", ad esempio). La Germania sembra avere anche caratteri più accentuati. Il primo sito, infatti, triplica di dimensione in un mese, mentre per i restanti siti la crescita è molto simile a quella osservata in Italia. L'unica differenza sostanziale tra i due paesi è che in Germania si osserva una base di utenti ancora più disposti a visitare frequentemente piccoli e nuovi siti rispetto alle grandi testate, utenti disposti a lasciare il vecchio e dare spazio al nuovo. Quindi, sia in Italia che in Germania, gli utenti della rete si informano di più,

compiono più ricerche sul web e spesso preferiscono visitare nuovi siti più piccoli rispetto ai soliti noti, forse alla ricerca di informazioni proposte con punti di vista differenti e innovativi. È possibile trarre una *prima conclusione: il pluralismo dell'informazione è in continuo aumento.* Ma quanto di questo incremento è dovuto ai motori di ricerca?





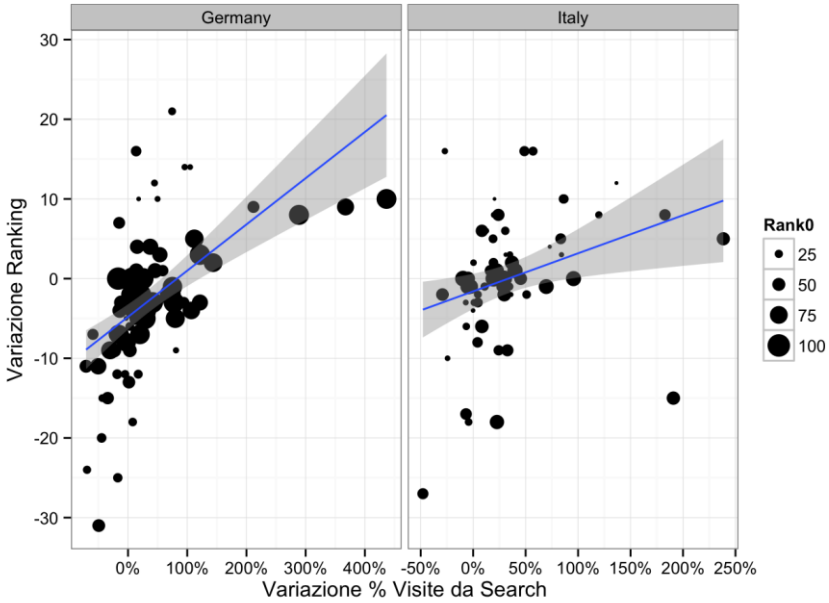
Per rispondere, basta guardare attentamente il prossimo grafico. Esso mostra la variazione nel *traffico search* di inizio periodo con quello di fine periodo (in termini percentuali) in relazione alla variazione totale delle visite ricevute. Ogni sito è identificato da un punto nella distribuzione, punto che è tanto grande quanto maggiore era il suo rank all'inizio del periodo. L'effetto è chiaramente positivo, dal momento che la retta di tendenza (in blu) è positivamente inclinata. L'inclinazione di tale retta mostra l'impatto dei motori di ricerca rispetto alle altre fonti. Se la linea fosse inclinata a quarantacinque gradi esatti, questo significherebbe che l'intero aumento delle visite totali in un mese proverrebbe completamente del *traffico search*. Ciò che la figura suggerisce è comunque che i motori di ricerca sono responsabili solo di parte del traffico in entrata per ogni sito. Ancora una volta, la Germania mostra un comportamento estremizzato, in quanto la maggior parte delle nuove visite è imputabile al *traffico search*. In Italia lo stesso effetto persiste, sebbene in forma più lieve (circa la metà del nuovo traffico in entrata può essere attribuita ai motori di ricerca)



La figura rivela quindi che effettivamente il *traffico search* incrementa le visite totali che un sito riceve nell'arco di un mese in modo sostanziale e che sfruttare i motori di ricerca è a tutti gli effetti una strategia corretta al fine di aumentare la propria visibilità. Per la maggioranza dei siti, l'uso intensivo dei motori di ricerca permette di ricevere più contatti mensili e questo sembra essere tanto più vero quanto più piccolo è il sito. Se, come illustrato prima, i siti piccoli crescono in media di più e la metà di tale crescita è attribuibile ai motori di ricerca (come ad esempio nel caso italiano), si può affermare che i motori di ricerca abbiano un effetto più intenso su siti di dimensioni minori. *Seconda conclusione: i motori di ricerca aumentano il pluralismo dell'informazione, aiutando anche i piccoli siti ad emergere ed acquisire visibilità.*

Un'analisi più approfondita mostra inoltre che esiste una correlazione positiva tra il traffico derivante dai motori di ricerca e la variazione di posizione occupata da un sito nella classifica, dal momento che il grafico seguente è stato costruito attribuendo al sito primo in classifica un punteggio di cento, mentre all'ultimo in classifica un punteggio di uno. In altri termini, più un sito si affida ai motori di ricerca per aumentare la sua visibilità, più la sua posizione nel ranking migliora, come mostrato nella figura. Come esempio esplicativo per tale conclusione, si assuma che un sito I) in precedenza attirava visitatori sfruttando al 50% il *traffico search* ed al 50% i social networks, e che II) fosse al cinquantesimo posto nella classifica dei siti più visitati. Se tale sito decidesse di aumentare il suo *traffico search* fino al 75% (riducendo il traffico social al 25%), esso vedrebbe aumentare la sua posizione in classifica. Sulla base di studi e analisi dei dati raccolti e qui non presentate per evitare eccessive complicazioni, tale effetto sembra essere tanto maggiore quanto più bassa era la posizione in classifica prima di decidere per l'aumento di *traffico search*. Quindi, un sito che inizialmente si collocava all'ottantesima posizione beneficerebbe di più dall'aumento del *traffico search* rispetto ad un sito che si posizionava in sessantesima posizione. Tuttavia, come il grafico evidenzia, la crescita di ranking non può essere attribuita interamente al *traffico search*, bensì è probabilmente frutto di un portafoglio più bilanciato di strumenti di visibilità. La spiegazione di questo fenomeno è perfettamente

intuitiva. Affidarsi completamente ad un solo mezzo di comunicazione come i motori di ricerca è sensato ma potrebbe essere non efficiente, poiché si trascurano altre importanti fonti di traffico. I motori di ricerca aumentano il pluralismo dell'informazione, ma non essendo la panacea per tutti i mali, devono sempre rappresentare solo una frazione delle fonti di visibilità utilizzate da un sito. Ancora una volta, i dati confermano che tali deduzioni sono valide maggiormente in Germania che in Italia. La maggiore inclinazione della retta di tendenza (in blu) nel caso della Germania rispetto al caso italiano è sintomo di come, in Germania, lo sfruttamento intensivo dei motori di ricerca dia frutti migliori e permetta ai siti di aumentare la loro posizione nella classifica dei siti maggiormente visualizzati più di quanto non succeda in Italia. *Terza conclusione: il traffico search permette di aumentare notevolmente la visibilità di un sito (ed è tanto più vero quanto più il sito è piccolo), sebbene sia sicuramente meglio non dipendere unicamente dal traffico search ma avere un portafoglio bilanciato di canali di traffico in entrata (che è tanto più vero quanto più il sito è grande)*



In conclusione, sebbene come sopra menzionato non esista una relazione causale univoca, l'evidenza empirica suggerisce che in Italia e Germania l'uso dei motori di ricerca favorisca il pluralismo dell'informazione e non distorca il mercato, permettendo anche a piccoli siti di incrementare la propria visibilità. I *search engines* non sono un rimedio certo per ogni problema, ma piuttosto uno strumento da usare con saggezza e ritegno insieme con altre fonti. Da un uso bilanciato e accorto dei motori di ricerca i singoli siti non traggono null'altro che benefici, cosi come anche i consumatori che hanno la possibilità di accedere ad un volume ed una qualità delle informazioni mai raggiunta prima.

Alla luce delle considerazioni esposte sopra, non si può non prendere atto dell'impatto positivo dei *search engines* sulla diversità e sul pluralismo dell'informazione, entrambi elementi incrementati dalle funzioni che essi offrono nel quadro realizzativo delle libertà di cui all'art. 10 della CEDU. Tuttavia, è bene non dimenticare che, nel momento in cui si fa riferimento alla libertà di informazione, si chiamano in causa tre diversi soggetti. In primo luogo, i fornitori di informazioni intesi come le figure editoriali che immettono i dati in rete, ponendosi come *content providers*. In secondo luogo, vi sono i motori di ricerca che garantiscono all'utente l'accesso e l'effettiva reperibilità delle informazioni. In ultimo, vi sono i consumatori finali di dati, ovvero gli utenti stessi, che per fruire delle risorse dei fornitori di informazioni passano attraverso l'algoritmo del *search engine*, il quale a sua volta filtra le risorse della rete a partire dalle parole chiave inserite. A questo punto, però, un primo problema si pone nel momento in cui il *service provider* viene assimilato in singoli ordinamenti nazionali alla figura editoriale, da cui invece è bene tenerlo distinto proprio perché i servizi forniti dai *search engines* non vanno a modificare i contenuti, ma semplicemente a veicolarli garantendone la reperibilità e l'accessibilità. Sul piano del diritto interno italiano, questa operazione di assimilazione tra le due figure sopra richiamate viene compiuta dal decreto cd. Romani (D. Lgs. 15 marzo 2010 n. 44), approvato per recepire la direttiva 2007/65 (*Audiovisual Media Services*) in materia di servizi audiovisivi, prescindendo dalle tecniche di trasmissione. Per via di tale decreto il legislatore ha posto le condizioni per il controllo sugli operatori

audiovisivi finalizzato a prevenire la creazione di posizioni dominanti nel Sistema Integrato delle Comunicazioni (SIC), con l'obiettivo di dare piena attuazione al principio pluralistico nel settore dell'informazione. Sulla base del decreto, l'Autorità per le garanzie nelle comunicazioni (AGCOM) ha il potere di valutare annualmente le dimensioni economiche del Sistema Integrato delle Comunicazioni (SIC) per cui «*i soggetti tenuti all'iscrizione nel registro degli operatori di comunicazione costituito ai sensi dell'articolo 1, comma 6, lettera a), numero 5), della legge 31 luglio 1997, n. 249, non possono né direttamente, né attraverso soggetti controllati o collegati ai sensi dei commi 14 e 15, conseguire ricavi superiori al 20 per cento dei ricavi complessivi del sistema integrato delle comunicazioni*».[22]

All'articolo 4 del decreto Romani, viene elencato l'insieme delle categorie non soggette agli obblighi posti dal decreto, poiché non rientranti nella definizione di "servizio di media audiovisivo". Tra di esse, vi sono «*i servizi nei quali il contenuto audiovisivo è meramente incidentale e non ne costituisce la finalità principale, quali, a titolo esemplificativo: a) i siti internet che contengono elementi audiovisivi puramente accessori, come elementi grafici animati, brevi spot pubblicitari o informazioni relative a un prodotto o a un servizio non audiovisivo; […] c) i motori di ricerca […]*»[23]. Dunque, almeno in un primo momento, l'intera attività dei *search engines* (intesi come *internet service providers*) era stata esclusa dal Sistema Integrato delle Comunicazioni proprio perché estranea alla fornitura di servizi di media audiovisivi, in quanto tale ultima attività presuppone l'esercizio di un potere di controllo sui contenuti da parte di un soggetto con responsabilità editoriale. Tuttavia, l'AGCOM ha in passato più volte sollecitato il legislatore italiano, affinché rivedesse le aree economiche rilevanti ai fini della tutela del pluralismo in modo da tenere conto della rilevanza del ruolo di internet rispetto alle dinamiche limitative del pluralismo. Ciò ha comportato l'inclusione del web (compresi i motori di ricerca) tra i mercati oggetto di vigilanza da parte dell'Autorità per le Garanzie nelle Comunicazioni. Così, con legge n.

[22] Art. 43 comma 9 del Decreto legislativo 31 luglio 2005 n. 177, come riformato dal Decreto legislativo 15 marzo 2010 n. 44 (Decreto Romani).
[23] Art. 4 comma 1, punto a) del D. Lgs. 44/2010.

103 del 2012, l'art. 43 del D. Lgs. 177/2005 è stato modificato per accogliere parzialmente le richieste dell'Autorità, introducendo tra l'analisi dei ricavi anche quelli derivanti dalla «*pubblicità online e sulle diverse piattaforme anche in forma diretta, incluse le risorse raccolte da motori di ricerca, da piattaforme sociali e di condivisione*».[24]

In questo modo, dunque, la funzione svolta dall'algoritmo dei *search engines* è stata assimilata a quella editoriale, commettendo, ad avviso di chi scrive, un errore di fondo che va ad inficiare la stessa libertà di informazione tutelata dall'art. 10 della CEDU e le garanzie di libertà e di pluralismo assicurate dalla rete. Infatti, considerare gli introiti pubblicitari del motore di ricerca all'interno dei mercati rilevanti per la regolazione *ex ante* a fini di tutela del pluralismo dell'informazione, significa ritenerlo responsabile dei contenuti stessi che indicizza, come se questi avesse la possibilità di controllarne il merito. A ben guardare, il decreto Romani e le sue successive modifiche contraddicono le prescrizioni della direttiva sul commercio elettronico 2000/31/CE relative agli ISPs che offrono servizi di *mere conduit*, *caching* e *hosting*, giacché l'indicizzazione dei dati raccolti dai motori di ricerca risponde ai criteri pre-determinati neutralmente dell'algoritmo, senza alcun intervento sui contenuti da parte del provider. Invero, prima della legge 103/2012, il legislatore poneva alla base del sistema integrato delle comunicazioni la responsabilità editoriale degli operatori che producevano contenuti nei mercati rilevanti e, proprio per questo motivo, escludeva dal SIC gli *internet service providers*, nel rispetto della qualificazione che di essi è data dalla direttiva 2000/31/CE. Il fatto che la raccolta di risorse da parte dei motori di ricerca sia entrata a far parte di questo panorama ha confermato l'approccio errato della legislazione italiana alle potenzialità dei *search engines* in materia di pluralismo dell'informazione. Per usare una metafora naturalistica, si è confuso l'albero (l'editore) con il sentiero che porta ad esso (il motore di

[24] Art. Legge n. 103 del 2012 che converte il decreto-legge 18 maggio 2012, n. 63, recante «Disposizioni urgenti in materia di riordino dei contributi alle imprese editrici, nonché di vendita della stampa quotidiana e periodica e di pubblicità istituzionale».

ricerca). Si può dunque concordare con chi ha commentato la novella legislativa dicendo che in Italia si è assistito «*ad alcuni tentativi, specialmente di matrice giurisprudenziale, di prefigurare un ruolo partecipativo da parte dei provider rispetto alla creazione di contenuti, ossia di un ruolo di "non neutralità" o "non passività" in relazione alle attività eseguite dagli utenti*».[25]

In tale frangente, l'elemento che rischia di inficiare la libertà di informazione risiede nella confusione di fondo da parte della normativa italiana che assimila il motore di ricerca all'editore, come se esso avesse la capacità di elaborare o modificare i contenuti. Su questi ultimi, però, le regole selettive dell'algoritmo non hanno alcun effetto, nonostante li indicizzino in ordine di rilevanza. Per di più, come già affermato, mentre gli editori guidano l'esperienza informativa del consumatore, i motori di ricerca si limitano ad aggregare le notizie presenti in rete per parole chiave, selezionando contenuti provenienti da fonti molto diverse tra loro. Gli editori online "puri", infatti, non assemblano i risultati e fanno soprattutto uso di contenuti che loro stessi immettono in quanto *content providers*, una potestà che invece non appartiene in alcun modo ai *search engines*, la cui attività è unicamente basata sull'individuazione di informazioni già presenti nel web, al fine di facilitare e personalizzare la ricerca e l'accesso dell'utente alle suddette notizie, fornite in prima istanza dagli editori online. Anche se i motori di ricerca vendono spazi pubblicitari agli inserzionisti – e in tal senso "competono" con gli editori tradizionali – i loro ricavi non hanno alcun rapporto con il livello di *audience* tipico dei media audiovisivi, proprio perché essi non sono "fornitori di servizi di media audiovisivi". Infatti, i loro guadagni derivano dall'utilizzo, da parte degli utenti, dei servizi internet offerti dai *search engines* e non dalla consultazione dei contenuti. Il fatto che, raccogliendo anch'essi pubblicità commerciale, i motori di ricerca producano un potenziale (e tutto da dimostrare) decremento degli investimenti pubblicitari nei media audiovisivi classici, non restringe affatto il pluralismo informativo e non porta con sé alcun pericolo di concentrazione del mercato. Al contrario,

[25] O. POLLICINO, *Tutela del pluralismo nell'era digitale: ruolo e responsabilità degli Internet service provider*, 2014, in www.giurcost.org, pag. 3.

l'inserimento dei motori di ricerca nel SIC sembra suggerire che essi rappresentino per il legislatore italiano una minaccia per il pluralismo dell'informazione, così come può avvenire nel caso di monopolio in mercati quali quelli tipici dell'audiovisivo.

Anche alla luce delle considerazioni espresse fin qui, l'approccio recentemente seguito dal legislatore italiano si espone a più di un dubbio di fondatezza, come pare confermare il fatto che inizialmente le disposizioni dell'art. 4 del Decreto Romani escludevano dalla definizione di "servizio di media audiovisivo" proprio i motori di ricerca. Come si diceva poc'anzi, essi hanno semmai il merito di facilitare la ricerca di fonti informative, senza alcuna possibilità di intervenire sui contenuti, in quanto semplicemente utilizzano un algoritmo per aggregare e indicizzare i contenuti forniti da altri. Quindi, se si dovesse riflettere sul ruolo che essi hanno rispetto al pluralismo, si potrebbe ragionevolmente affermare che lo hanno incrementato, garantendo l'accesso ad informazioni molto differenziate e assicurando anche un aumento delle visite ai siti degli editori tradizionali oltreché a quelli minori o rivolti ad un pubblico più ristretto e di nicchia. Queste posizioni vengono rafforzate dalle sentenze emanate nei diversi stati europei a proposito dell'auto-completamento e dei suggerimenti di ricerca, che hanno richiamato l'effettiva diversità tra *content* e *service provider*. Le due funzioni menzionate consentono agli utenti di «*completare la chiave di ricerca o di visualizzare le più comuni ricerche correlate effettuate da terzi. Tali operazioni sono svolte da un algoritmo che effettua in modo automatico un'associazione tra le parole chiave che risultano maggiormente ricercate dagli utenti*».[26] A volte, però, l'auto-completamento genera risultati che rischiano di danneggiare i soggetti a cui rinviano, ad esempio nei casi in cui le parole che compaiono in automatico abbiano valenza negativa. Per questo motivo non è stato infrequente che utenti, associazioni o categorie di persone si rivolgessero a un giudice, citando in giudizio il motore di ricerca, per chiedere che fosse ritenuto responsabile per la lesione della propria reputazione. E' il caso, ad esempio, di quanto avvenuto recentemente a Milano, dove il Tribunale, con ordinanza 25 marzo 2013, ha

[26] O. POLLICINO, *Tutela del pluralismo nell'era digitale*, *op. cit.*, pag. 15.

smentito le posizioni del ricorrente che riteneva Google un *content provider* dal momento che le funzioni di auto-completamento verrebbero progettate dallo stesso motore di ricerca, per questo responsabile dei contenuti derivanti dall'attività dell'algoritmo. I giudici hanno rigettato questa ipotesi asserendo che Google «*riproduce statisticamente il risultato delle ricerche più popolari effettuate dagli utenti, laddove "Ricerche Correlate" riproduce i risultati delle pagine web indicizzate e rese accessibili dal motore di ricerca, partendo dai termini in questione*».[27] Nella decisione, le fonti normative considerate sono state quelle relative all'attività di *mere conduit*, *caching* e *hosting*, disciplinate dal D. Lgs. 70/2003 che recepisce la già citata direttiva sul commercio elettronico 2000/31/CE. Inoltre, è stato sottolineato anche il collegamento di dette previsioni con il Considerando n. 42 della direttiva, nel tentativo di distinguere la responsabilità dei *service providers* da quella dei fornitori di contenuti. Ebbene, per il Tribunale di Milano, «*Google, in quanto soggetto che offre servizi di ricerca via internet, è certamente un Internet Service Provider*»[28] ed in proposito viene citata l'Ordinanza del 24 marzo 2011, dello stesso Tribunale, in cui era stato stabilito che: «*I motori di ricerca sono data-base che indicizzano i testi sulla rete e che offrono agli utenti un accesso per la consultatone: sono dunque sostanzialmente una banca dati più un software*».

Tuttavia, anche se le funzioni di *auto-completamento* e quella di "Ricerche correlate" (situata in fondo alla pagina contenente i risultati di ricerca forniti a seguito dell'inserimento di parole chiave) differiscono «*da quelle di semplice memorizzazione passiva delle informazioni [caching] e realizza[no] associazioni di parole grazie a sistemi — algoritmi matematici — pacificamente ideati, elaborati e adottati da Google*», le associazioni di parole «*non costituiscono una frase di senso compiuto né una manifestazione di pensiero, né dunque 'quello che Google pensa', né un pensiero, né un pensiero attribuibile a Google, ma esclusivamente il risultato delle ricerche più popolari effettuate dagli utenti, ovvero la visualizzazione dei termini ricorrenti*

[27] Ordinanza del Tribunale di Milano, 25 Maggio 2013, Sezione I Civile, in www.oppic.it.
[28] Ibid.

nelle pagine web incluse tra i risultati di ricerca di una determinata query, entrambi resi disponibili agli utenti come strumenti di aiuto alla ricerca».[29]

Che i motori di ricerca non abbiano responsabilità editoriale e non siano assimilabili agli *editori* è dimostrato proprio dal fatto che la funzione di aggregazione di parole per l'auto-completamento è basata su un algoritmo che calcola matematicamente la ricorrenza della ricerca da parte degli utenti. Inoltre, è bene sottolineare il fatto che, per quanto possano essere offensivi gli abbinamenti proposti, essi pur sempre integrano un'ipotesi di esercizio della libertà di informazione, intesa sia come libertà di ricevere notizie che come libertà di avervi accesso, proprio per il fatto che l'*auto-completamento* mostra le ricerche effettuate più spesso, il che costituisce di per sé un'informazione. Nello stesso filone giurisprudenziale si colloca, la sentenza del 31 ottobre 2012[30] con la quale il Tribunal de Grande Instance de Paris ha annullato la condanna precedentemente inflitta a Google per il risultato fornito da un *auto-completamento*, contestato da un utente francese il cui nome veniva affiancato alla parola "*secte*" (setta). Benché nell'ambito di un giudizio vertente sull'accertamento di un'attività diffamatoria, il giudice francese ha comunque colto l'occasione per ricordare che i suggerimenti proposti dalla stringa di Google mediante la funzione di auto-completamento vengono determinati da un algoritmo basato su criteri oggettivi e senza alcun intervento umano. A conferma dell'impossibilità di assimilare il motore di ricerca ad un *content provider* e, quindi, ad un editore, si riporta anche la decisione della Cour de Cassation francese, che nel febbraio 2013 ha sentenziato che Google non è direttamente responsabile per il funzionamento del motore di ricerca in quanto egli non elabora gli elementi offensivi (cioè i contenuti), ma semplicemente si limita ad utilizzare un algoritmo che fornisce risultati oggettivi basati su calcoli matematici[31]. Quest'indirizzo

[29] Ibid.

[30] Antonino M. / Google Inc. et autres, Tribunal de grande instance de Paris – 17ème chambre, Jugement du 31 octobre 2012, in www.legalis.net.

[31]«Mais attendu que, par motifs tant propres qu'adoptés, la cour d'appel a relevé que la société Google France sollicitait à bon droit sa mise hors de cause dès lors qu'elle n'avait pas de responsabilité directe dans le fonctionnement du moteur de recherche

giurisprudenziale contrario all'assimilazione tra ISPs e fornitori di contenuti è coerente con i risultati a cui addiveniva il già citato *Study on liability of internet intermediaries*, dove si rilevava come in molti paesi europei, a seguito del recepimento della direttiva 2000/31/CE i motori di ricerca vengano considerati come *access providers* oppure come *host providers*, perciò disciplinati dalle regole sui *service providers*. Un simile approccio è evidente in paesi come l'Austria, l'Ungheria, il Portogallo e la Spagna, che hanno disposto un'esplicita esenzione di responsabilità per i *search providers*, in quanto essi hanno la sola funzione di agevolare la navigazione degli utenti che ricercano informazioni in rete. La Francia e la Germania, invece, pur non avendo apposite previsioni in materia, considerano i motori di ricerca come s*ervice providers*, così come suggerito anche dalla giurisprudenza italiana – come dimostrato dall'assoluzione di Google nel caso che lo vedeva citato in giudizio dall'associazione Vividown Onlus.[32]

Alla luce di queste considerazioni, si capisce come il decreto Romani presenti profili di incompatibilità con l'interpretazione europea dei principi di pluralismo dell'informazione e tutela della libertà del web come mezzo espressivo, soprattutto nell'ambito della giurisprudenza relativa all'articolo 10 della Convenzione Europea dei Diritti dell'Uomo, che va ritenuta parte integrante dell'ordinamento giuridico dell'Unione Europea in forza del riferimento esplicito contenuto nel Trattato sull'Unione Europea.[33] Inoltre, le disposizioni italiane contrastano anche con le esclusioni di responsabilità di cui alla direttiva 2000/31/CE che differenziano il *content provider* dall'*internet service provider*, individuando come tipica di

---

ni dans le site google.fr et qu'elle n'était pas concernée par l'élaboration des items incriminés; qu'elle a ainsi nécessairement répondu aux conclusions prétendument délaissées; que le moyen manque en fait. Par ces motifs: rejette le pourvoi», Cour de cassation, 1ère chambre civile, 19/02/2013, in www.courdecassation.fr.

[32] Caso Google-Vividown, Sentenza 17 dicembre 2013 – 3 febbraio 2014, n. 5107, Corte di Cassazione, Sez. III Penale, in www.dirittoegiustizia.it.

[33] Trattato sull'Unione Europea, articolo 6, comma 3: "*I diritti fondamentali, garantiti dalla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali e risultanti dalle tradizioni costituzionali comuni agli Stati membri, fanno parte del diritto dell'Unione in quanto principi generali*".

quest'ultimo un'attività assolutamente distinta da quella editoriale, caratterizzata invece dal potere di intervento sui contenuti, e come più volte confermato dalle già citate sentenze sulla funzione di *auto-complete*.

Considerati questi due profili, il Decreto Romani pone le basi per un controllo sui motori di ricerca che non trova alcun fondamento né nella loro natura né nella tipologia di servizi forniti, in quanto essi si basano esclusivamente sull'aggregazione di dati già presenti in rete ed immessi da terzi. In tal modo, la legislazione italiana presenta due profili di problematicità ineludibili. Innanzitutto, essa contrasta con il significato dato a livello europeo al concetto di "pluralismo", inteso come diversità delle fonti: si è più volte ricordato che esso risulta potenziato – e non compromesso – dalla diffusione dei motori di ricerca che hanno facilitato la reperibilità delle notizie nonché incrementato il diritto di accesso alle informazioni. In secondo luogo, anche il diritto di informazione nel suo profilo passivo, inteso come libertà di dare notizie in qualità di editore, viene leso nel momento in cui l'indicizzazione di contenuti preesistenti viene considerata un'operazione editoriale. In tal senso, il fatto che i risultati di ricerca rimandino a fonti tra loro molto diverse si pone come strumento di tutela rispetto alla libertà di espressione, poiché i diversi link riportati aumentano la visibilità di posizioni meno diffuse, note o comunque non convenzionali. E' proprio la neutralità dei *search engines* rispetto ai contenuti, infatti, che consente agli utenti di reperire notizie contrastanti con i propri punti di vista o comunque lontane dalle loro posizioni di partenza o inaspettate. In effetti, nell'*information society* coloro che navigano devono possedere delle capacità che possano consentire di reperire ciò che stanno cercando, selezionando i contenuti autonomamente, senza il supporto di un editore che li ordina, orientando il percorso da seguire. Non essendo ancora possibile considerare che ciascuno disponga di questo tipo di abilità, i s*earch engines* hanno il merito di agevolare il processo di ricerca ordinando i risultati in base alla loro popolarità, dando all'utente quantomeno un criterio per muoversi all'interno della rete.

E' innegabile, dunque, che i motori di ricerca costituiscano una risorsa preziosa per gli utenti, giacché essi hanno la capacità di ricondurre a dati estremamente differenziati – ma pertinenti – rafforzando sia il

diritto di accesso alle informazioni nel *mare magnum* di internet, che la capacità degli editori tradizionali di diffondere le notizie. Ecco che il fatto che essi vengano assimilati alle figure editoriali tradizionali accompagna l'inesatta considerazione che «il soggetto che esercita un'attività di controllo sull'informazione, abbia un ruolo rilevante ai fini della tutela del pluralismo»[34]. Il ruolo e l'attività dei motori di ricerca dimostrano, al contrario, che l'incremento delle fonti informative, della diffusione e dell'accesso alle notizie può essere ottenuto anche mediante criteri neutri e matematici di selezione delle fonti – quali quelli propri dell'algoritmo – senza che vi sia alcuna necessità di controllo sui contenuti da parte di chi offre un servizio di indicizzazione dei risultati.

6. Diritto di accesso, pluralismo e motori di ricerca a seguito della recente giurisprudenza della Corte di Giustizia dell'Unione Europea sul diritto all'oblio: potenziale contrasto con l'articolo 10 della CEDU.

In tema di sovrapposizione tra editore e motore di ricerca e di come essa rischi di comprimere la libertà di informazione, si può considerare uno spartiacque la sentenza della Corte di Giustizia dell'Unione Europea relativa al caso Google Spain[35]. Nella pronuncia, infatti, si sono rinvenuti in capo al motore di ricerca Google i requisiti del titolare del trattamento dei dati personali, derivando quindi un onere per tutti i *search providers* di mettere a disposizione dell'utente metodi di rimozione dei link a tutela del loro diritto alla cancellazione dei dati che li riguardano. Tale decisione ha scosso le fondamenta giuridiche di Internet in Europa, al punto che si continua a discutere se un diritto alla cancellazione, così configurato, non prefiguri quel diritto all'oblio la cui definizione impegna ormai da due anni il legislatore europeo nell'ambito della riforma della normativa privacy

[34] O. POLLICINO, *Tutela del pluralismo nell'era digitale: ruolo e responsabilità degli Internet service provider*, 2014, in www.giurcost.org, pag. 27.

[35] Causa C‑131/12, Corte di Giustizia Europea, Grande Sezione, Sentenza 13 maggio 2014, in www.altalex.it.

comunitaria. Ciò che interessa in questa sede, comunque, non sono tanto le tante - pur cruciali - questioni di diritto della protezione dei dati personali implicate nella causa (sulle quali molti dubbi interpretativi ha generato e continua a generare la decisione nella comunità di giuristi esperti della materia), quanto evidenziare un aspetto specifico del ragionamento giuridico della Corte di Giustizia circa il ruolo effettivo dei *search engines* che, pur venendo assimilati alla figura del "titolare del trattamento"[36] cionondimeno non finiscono per essere equiparati *tout court* ad un *content provider*/editore. Il fatto che ha dato origine alla causa citata può essere sinteticamente riassunto come segue. Nel 1988 erano stati pubblicati sul quotidiano spagnolo *La Vanguardia* – per ordine del Ministero del Lavoro e degli Affari sociali spagnolo – due annunci riguardanti la vendita forzata dei beni a causa dei debiti contratti, resi poi disponibili anche sul web. Nella descrizione di una delle proprietà, veniva citato il nome di uno dei proprietari, cioè il signor Mario Costeja González. Nel novembre 2009, l'uomo aveva contattato il giornale per ottenere la rimozione dei dati che lo riguardavano, giacché la vendita si era conclusa anni prima ed aveva perso il suo rilievo informativo. *La Vanguardia* si era opposta alla cancellazione e. per questo, nel febbraio 2010 González aveva formulato la medesima richiesta a Google Spain, i cui risultati di ricerca conducevano agli annunci del 1988 se si inseriva il nome dell'uomo come "parola chiave" nella stringa di ricerca. Il ricorrente aveva anche presentato una denuncia all'Agencia Española de Protección de Datos (AEPD) chiedendo sia la rimozione delle informazioni che lo riguardavano da parte del giornale, sia da parte di Google Spain o Google Inc.Nel luglio 2010, il direttore dell'AEPD, pur respingendo il reclamo contro *La Vanguardia*, aveva accolto le istanze contro il motore di ricerca, in modo che esso rendesse impossibile l'accesso ai dati mediante l'uso del suo portale. In seguito a questa decisione, Google Spain e Google Inc. avevano proposto ricorsi distinti all'Audiencia Nacional contro quanto disposto dall' all'Agencia Española de Protección de Datos, asserendo non soltanto

[36] Nella sentenza "Responsabile del trattamento". La diversa traduzione italiana del medesimo concetto è dovuta alla definizione data dal Codice in materia di protezione dei dati personali, D. Lgs. 196/2003, in www.garanteprivacy.it.

che all'interno della funzione di ricerca non vi era alcun trattamento dei dati personali, ma soprattutto che l'attività del *search engine* non aveva nulla a che vedere con l'applicazione della direttiva 95/46/CE[37] sulla protezione dei dati, pertanto era impossibile considerare Google come un *data controller*.

Per inquadrare la rilevanza della vicenda è necessario porre l'accento sulle previsioni della direttiva privacy che definisce «"titolare del trattamento"[38] [*data controller*]: la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che, da solo o insieme ad altri, determina le finalità e gli strumenti del trattamento di dati personali»[39], distinguendo questa figura dall'«"responsabile del trattamento"[40] [*data processor*]: la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che elabora dati personali per conto del responsabile del trattamento»[41]. L'articolo 23, poi, fa riferimento alle "Responsabilità" stabilendo che: «*Gli Stati membri dispongono che chiunque subisca un danno cagionato da un trattamento illecito o da qualsiasi altro atto incompatibile con le disposizioni nazionali di attuazione della presente direttiva abbia il diritto di ottenere il risarcimento del pregiudizio subito dal responsabile del trattamento*». *Dunque, quest'ultima figura è a tutti gli effetti responsabile salvo che provi «che l'evento dannoso non gli è imputabile» poiché in tal caso verrebbe «esonerato in tutto o in parte da tale responsabilità*».

---

[37] Recepita nell'ordinamento spagnolo mediante Ley Orgánica n. 15/1999, del 13 dicembre 1999, relativa alla tutela dei dati personali.

[38] In Italia la traduzione ufficiale della direttiva 95/46/CE definisce "Responsabile del trattamento" il soggetto identificato nel D. Lgs. 196/2003 come "Titolare del trattamento" (Cfr. Art. 4 comma 1 punto f del D. Lgs. 196/2003, in www.garanteprivacy.it).

[39] Articolo 2 – Definizioni, Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, in eur-lex.europa.eu.

[40] In Italia la traduzione ufficiale della direttiva 95/46/CE definisce "Incaricato del trattamento" il soggetto identificato nel D. Lgs. 196/2003 come "Responsabile del trattamento" (Cfr. Art. 4 comma 1 punto g del D. Lgs. 196/2003, in www.garanteprivacy.it).

[41] Ibid.

A ciò, poi, si contrappone la tutela della persona interessata, laddove l'articolo 12 della direttiva stabilisce che: «*Gli Stati membri garantiscono a qualsiasi persona interessata il diritto di ottenere dal responsabile del trattamento: […] b) a seconda dei casi, la rettifica, la cancellazione o il congelamento dei dati il cui trattamento non è conforme alle disposizioni della presente direttiva, in particolare a causa del carattere incompleto o inesatto dei dati*»[42]. L'articolo 14, inoltre, impone agli Stati membri di riconoscere «alla persona interessata il diritto: a) almeno nei casi di cui all'articolo 7, lettere e) e f),[43]di opporsi in qualsiasi momento, per motivi preminenti e legittimi, derivanti dalla sua situazione particolare, al trattamento di dati che la riguardano, salvo disposizione contraria prevista dalla normativa nazionale. In caso di opposizione giustificata il trattamento effettuato dal responsabile non può più riguardare tali dati»[44]. Considerate queste premesse, l'Audiencia Nacional aveva unito le due azioni legali ed aveva sospeso il processo in attesa di pronuncia pregiudiziale della Corte di Giustizia dell'Unione Europea sulla possibilità di applicare le previsioni della direttiva 46/95/CE ai motori di ricerca (intesi come *service providers*). In particolare, il tribunale domestico aveva sollevato tre questioni pregiudiziali, che includevano i seguenti quesiti, concernenti, in sintesi:

---

[42] Art. 12 – Diritto di accesso, Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, in eur-lex.europa.eu.

[43] «Gli Stati membri dispongono che il trattamento di dati personali può essere effettuato soltanto quando: […] e) è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il responsabile del trattamento o il terzo a cui vengono comunicati i dati, oppure f) è necessario per il perseguimento dell'interesse legittimo del responsabile del trattamento oppure del o dei terzi cui vengono comunicati i dati, a condizione che non prevalgano l'interesse o i diritti e le libertà fondamentali della persona interessata […]».

[44] Art. 14 – Diritto di opposizione della persona interessata, Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, in eur-lex.europa.eu.

- l'ambito materiale di applicazione della direttiva, cioè la sua applicabilità ai motori di ricerca, chiedendo se il tipo di attività compiuta dai motori di ricerca sui dati da essi indicizzati potesse configurare un trattamento di dati personali;
- l'ambito territoriale di applicazione della direttiva privacy a Google Inc., società di diritto statunitense con una sussidiaria in Spagna;
- la possibilità di qualificare Google come un Titolare del Trattamento;
- la responsabilità di un motore di ricerca come Google alla luce della direttiva privacy;
- la derivabilità di un "diritto all'oblio" nella normativa privacy europea vigente.

Nel valutare se fosse configurabile un trattamento di dati personali da parte di Google, la Corte, ha preso le mosse dalla formulazione letterale dell'articolo 2, lettera b), della direttiva 95/46/CE, che definisce "trattamento di dati personali" «*qualsiasi operazione o insieme di operazioni compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali, come la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione o la modifica, l'estrazione, la consultazione, l'impiego, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, nonché il congelamento, la cancellazione o la distruzione*», precisando, alla luce della giurisprudenza *Lindqvist*,[45] che: «*per quanto riguarda in particolare Internet, la Corte ha già avuto modo di constatare che l'operazione consistente nel far comparire su una pagina Internet dati personali va considerata come un «trattamento» siffatto ai sensi dell'articolo 2, lettera b), della direttiva 95/46 v. sentenza,*».[46]

Ciò significa, secondo la Corte, che se il motore di ricerca, nel fornire risultati, fa apparire i dati riferibili a persone fisiche, allora compie un trattamento per il fatto stesso che tali dati sono presenti

[45] Punto 25, Causa-101/01, Corte di Giustizia Europea , Sentenza 13 maggio 2002, in www.altalex.it

[46] Punto 26, Causa C‑131/12, Corte di Giustizia Europea, Sezione Grande, Sentenza 13 maggio 2014, in www.altalex.it.

nella pagina, anche se provengono da siti i cui contenuti non sono da lui controllati dove le informazioni sono state lecitamente pubblicate Poco dopo la CGE precisa proprio che: *«[…] occorre constatare che, esplorando Internet in modo automatizzato, costante e sistematico alla ricerca delle informazioni ivi pubblicate, il gestore di un motore di ricerca «raccoglie» dati siffatti, che egli «estrae», «registra» e «organizza» successivamente nell'ambito dei suoi programmi di indicizzazione, «conserva» nei suoi server e, eventualmente, «comunica» e «mette a disposizione» dei propri utenti sotto forma di elenchi dei risultati delle loro ricerche. Poiché tali operazioni sono contemplate in maniera esplicita e incondizionata all'articolo 2, lettera b), della direttiva 95/46, esse devono essere qualificate come «trattamento» ai sensi di tale disposizione, senza che rilevi il fatto che il gestore del motore di ricerca applichi le medesime operazioni anche ad altri tipi di informazioni e non distingua tra queste e i dati personali*».[47]

In questo passaggio della sentenza e in quelli successivi la Corte di Giustizia riconosce, più o meno esplicitamente, che l'attività di Google è distinta da quella degli editori. I giudici non identificano il "titolare del trattamento" con un "editore", ma individuano una sorta di "terzo genere di soggetto attivo del trattamento". Scrivono, infatti, che «*nella misura in cui l'attività di un motore di ricerca può incidere, in modo significativo e in aggiunta all'attività degli editori di siti web, sui diritti fondamentali alla vita privata e alla protezione dei dati personali, il gestore di tale motore di ricerca quale soggetto che determina le finalità e gli strumenti di questa attività deve assicurare, nell'ambito delle sue responsabilità, delle sue competenze e delle sue possibilità, che detta attività soddisfi le prescrizioni della direttiva 95/46(...)*».[48]

Dunque, la Corte distingue tra l'attività di produzione, selezione e controllo dei contenuti tipica di un editore, e quella di organizzazione e aggregazione delle informazioni della rete internet da parte del

[47] Punto 28, Causa C‑131/12, Corte di Giustizia Europea, Sezione Grande, Sentenza 13 maggio 2014, in www.altalex.it.

[48] Punto 38, Causa C‑131/12, Corte di Giustizia Europea, Sezione Grande, Sentenza 13 maggio 2014, in www.altalex.it.

motore di ricerca. E' eloquente, al riguardo, il passaggio in cui la Corte spiega che: «*il trattamento da parte dell'editore di una pagina web, consistente nella pubblicazione di informazioni relative a una persona fisica, può, eventualmente, essere effettuato «esclusivamente a scopi giornalistici» e beneficiare così, a norma dell'articolo 9 della direttiva 95/46, di deroghe alle prescrizioni dettate da quest'ultima, mentre non sembra integrare tale ipotesi il trattamento effettuato dal gestore di un motore di ricerca. Non si può dunque escludere che la persona interessata possa, in determinate circostanze, esercitare i diritti contemplati dagli articoli 12, lettera b), e 14, primo comma, lettera a), della direttiva 95/46 contro il suddetto gestore del motore di ricerca, ma non contro l'editore della pagina web*». [49]

Ne derivano due conseguenze. La prima è che la Corte disconosce la neutralità dei motori di ricerca, ma non al punto da attribuire loro lo statuto "protetto" degli editori/giornalisti. La seconda è che, con questo approccio, la Corte rivede – con criterio discutibile sul piano giuridico - anche la propria giurisprudenza in tema di bilanciamento tra il diritto alla privacy e la libertà d'informazione, a partire dalla sentenza *Satamedia.*[50] In quella sentenza la medesima Corte aveva ricondotto sotto lo scudo dell'eccezione "giornalistica", facendola dunque prevalere sul diritto alla privacy, perfino l'attività di un editore che inviava dati concernenti la posizione fiscale e reddituale di contribuenti finlandesi sul cellulare di utenti che la richiedevano dietro corrispettivo.

Per quanto riguarda la pronuncia pregiudiziale relativa alla corretta interpretazione dell'espressione "titolare del trattamento", nuovamente il *search provider* non viene assimilato ad un *content provider* nella parte in cui la Corte afferma che «*è il gestore del motore di ricerca a determinare le finalità e gli strumenti di tale attività e dunque del trattamento di dati personali che egli stesso effettua nell'ambito dell'attività medesima, ed è di conseguenza lui a dover essere*

[49] Punto 85, Causa C‑131/12, Corte di Giustizia Europea, Sezione Grande, Sentenza 13 maggio 2014, in www.altalex.it.

[50] Causa C‑73/07, *Tietosuojavaltuutettu contro Satakunnan Markkinapörssi Oy, Satamedia Oy*, Corte di Giustizia Europea, Sezione Grande, sentenza del 16 dicembre 2008.

considerato come il «titolare» di tale trattamento a norma del citato articolo 2, lettera d)»[51]. L'aspetto saliente risiede nel fatto che il giudice non mette in dubbio la legittimità del trattamento, cioè non si sofferma sulla questione della regolarità della raccolta dei dati intesa come diffusione dell'informazione già presente in rete, il che significa che non viene contestata l'attività di base del motore di ricerca consistente nell'indicizzazione dei contenuti[52] e non nella loro produzione/edizione. E' qui il cuore della differenziazione tra *search provider* e *content provider*. Pur volendo considerare il motore di ricerca come un *host provider*, l'articolo 14 della direttiva 200/31/CE afferma che esso non è responsabile a condizione che «non selezioni né modifichi le informazioni trasmesse». Posto, dunque, che non vi è alcuna modifica effettuata dai motori di ricerca sulle informazioni che essi indicizzano potrebbe risultare controversa l'interpretazione del termine "selezionare". Questo dubbio, comunque, può essere facilmente superato se si considera che l'algoritmo dei motori di ricerca compie una indicizzazione dei contenuti, non adopera alcuna selezione delle informazioni trasmesse, ma semplicemente le ordina per criterio di rilevanza e popolarità, compiendo un tipo di attività organizzativa e non selettiva.

Queste note dimostrano il carattere multiforme del *search engine*, che, normalmente, si pone come "*tertium genus*" tra *content provider* e *service provider*, e che comunque non rispecchia una figura editoriale propriamente intesa. Paradossalmente, dunque, tale sentenza implica valutazioni nettamente favorevoli alla tesi qui sostenuta, della differenza ontologico-funzionale tra motore di ricerca ed editore. Resta, tuttavia, una sentenza comunque criticabile, sul piano scientifico-giuridico e non solo per aspetti privacy qui non trattati: è impossibile non ravvisare uno strabismo interpretativo quando, imponendo comunque la decisione della Corte a Google di oscurare i risultati delle ricerche intorno a una determinata "chiave" in presenza di un "diritto all'oblio" di taluno, vengono limitati sia il pluralismo

[51] Punto 33, Causa C‑131/12, Corte di Giustizia Europea, Sezione Grande, Sentenza 13 maggio 2014, in www.altalex.it.

[52] Cfr. Punto 93, Causa C‑131/12, Corte di Giustizia Europea, Sezione Grande, Sentenza 13 maggio 2014, in www.altalex.it.

dell'informazione che le libertà di cui all'articolo 10 della CEDU, e in particolare il diritto di accesso all'informazione stessa, poiché le notizie di interesse pubblico vengono eliminate non a livello editoriale (*La Vanguardia*) ma a livello di raggiungibilità delle stesse (Google Search). In tal senso, non è possibile rintracciare il corretto bilanciamento di cui si è detto a proposito dei casi sottoposti alla Corte Europea dei Diritti dell'Uomo in merito alla limitazione delle libertà di cui all'art. 10, poiché la Corte di Giustizia bilancia il diritto alla protezione dei dati personali e la libertà di espressione nei confronti del soggetto sbagliato, il motore di ricerca, senza considerare il *content provider*, in capo al quale, da ultimo, va fatta risalire l'immissione dei dati personali e dei contenuti. In questo caso, cioè, si compie un errore di fondo nel separare l'interesse pubblico alla libertà di informazione dall'azione di ricerca intesa come "libertà di poter ricercare le notizie". Infatti, se il *content provider* (*La Vanguardia* nel caso in esame) è legittimato a pubblicare, allora è altrettanto lecito l'accesso fornito dal *search engine*: queste posizioni sono sostenute dalla lettura del contenuto stesso dell'articolo 10 della CEDU che configura la libertà di informazione anche come libertà di accesso alle notizie.

Non è chiaro come sia possibile pensare che vengano rispettate le disposizioni della Convenzione se la notizia rimane in rete, ma l'interesse pubblico ad avervi accesso non può essere soddisfatto. Considerando quanto detto sinora, è chiaro che alterare i risultati di ricerca, pur essendo disponibili e reperibili i materiali sul sito di origine, va contro la nozione di pluralismo e quella di libertà di informazione, ponendo la decisione della Corte di Giustizia europea in contrasto con quanto previsto dalla Convenzione Europea dei Diritti dell'Uomo all'articolo 10.

Mind detection e protezione dei dati neurogenetici. Alcune riflessioni sulla *privacy* mentale

di ALESSIA FARANO [*]

SOMMARIO: 1. Cenni preliminari sul rapporto tra neuroscienze e diritto – 2. Verso la *neuro-data protection* – 3. I nostri pensieri ci appartengono? Privacy mentale e *lie detection*.

1. Cenni preliminari sul rapporto tra neuroscienze e diritto.

I rapporti tra neuroscienze e diritto hanno assunto, da almeno un decennio e soprattutto negli Stati Uniti, lo status di vero e proprio settore scientifico disciplinare, con il dichiarato intento di studiare effetti attuali o potenziali dell'irrompere del discorso neuroscientifico nel diritto. Il perché di un interesse, che si è andato consolidando sempre più nel torno dell'ultimo decennio, va ricercato in primo luogo accostandosi alla definizione di neuroscienze, da intendersi come «sistema integrato di discipline che ha per oggetto lo studio del cervello e del sistema nervoso degli organismi viventi a livello molecolare, biologico e genetico», aventi come scopo «quello di evidenziare la base biologica delle espressioni mentali e comportamentali dell'animale e dell'uomo a partire dalla singola cellula nervosa (neuroni) e di piccoli sistemi neuronali»[1].

Come di recente sostenuto[2], ove si consideri che il diritto ha ad oggetto il controllo del comportamento, e le neuroscienze lo studio e la spiegazione di questo (a partire, come si è visto, dalle connessioni neuronali), risulta agevole intendere la portata potenzialmente

[*] Luiss Guido Carli, Roma.

[1] U. GALIMBERTI, *Enciclopedia di Psicologia*, Garzanti, Milano 1999, p. 686. Per una introduzione utile ai non addetti ai lavori si veda A. OLIVERIO, *Prima lezione di neuroscienze*, Laterza, Roma-Bari 2011.

[2] THE ROYAL SOCIETY, *Brain Waves Module 4: Neuroscience and Law*, 2011, p. 1.

corrosiva della spiegazione del comportamento umano offerta dalle neuroscienze:

> Because law is, at base, about changing behavior, and because behavior, at base, comes from brains, it follows that deeper understandings of the relationships between brains and behaviors (and, relatedly, about perception, judgment, decision-making, and the like) may aid efforts to increase the effectiveness, efficiency, and justness of law[3].

Nonostante la varietà delle posizioni avanzate all'interno del vivace dibattito internazionale, che ha visto nella conferenza del 2002 a San Francisco il primo momento di mappatura dei temi coinvolti[4], è stato prevalentemente il problema epistemologico a impegnare giuristi, filosofi e neuroscienziati stessi[5] che intendessero ascriversi alle fila dei cultori di *Law and Neuroscience* o *Neurolaw*: il numero monografico delle *Philosophical Transactions* della *Royal Society* del 2004, che data la nascita formale della materia, ha dato l'avvio ad una polarizzazione tra quanti ritenevano che le neuroscienze avrebbero definitivamente messo in scacco le categorie giuridiche tradizionali (Green e Cohen[6], tra tutti), e quanti, invece, non si dichiaravano disposti a riconoscere l'eccezionalismo neuroscientifico, invocando

---

[3] O.D. JONES, *Seven Ways Neuroscience Aids Law*, in A. BATTRO, S. DEHAENE, W. SINGER (a cura di), *Neurosciences and the Human Person: New Perspectives on Human Activities: Proceedings of the working group 8-10 November 2012*, Pontificia Academia Scientiarum, Città del Vaticano 2013, p. 14.

[4] Gli atti sono oggi pubblicati: S.J. MARCUS (a cura di), *Neuroethics: Mapping the Field, Conference Proceedings*, The Dana Foundation, New York 2002. Un resoconto efficace è quello di A. ROSKIES, *Neuroethics for the New Millenium*, in *Neuron*, 35, 2002, pp. 21 e ss., in cui l'Autrice dà conto anche delle perplessità relative alla scelta del termine 'neuroetica'.

[5] Tra i più noti vi è il neuroscienziato Micheal Gazzaniga, a più riprese intervenuto sui rapporti tra diritto e neuroscienze: M.S. GAZZANIGA, *The Law and Neuroscience*, in *Neuron*, 60, 2008, ; ID., *Who is in charge? Free will and the science of the brain*, Harper Collins, New York 2012.

[6] J.GREENE, J.COHEN, *For the law, neuroscience changes nothing and everything*, in THE ROYAL SOCIETY, *Philosophical Transactions of the Royal Society B: Biological Sciences*, 359, 2004, pp. 1775-1785.

una svolta verso la *neuromodesty* (Morse[7]). Il primo assestarsi del tema, allora, può essere rappresentato nelle forme dello scontro tra diritto e scienza, coinvolgendo temi per altro non nuovi per la scienza giuridica, da tempo impegnata a far fronte alla sfida tecnologica[8]. La posta in gioco di questo conflitto è chiara, e riguarda la possibilità di sostituire all'immagine di uomo capace di rispondere delle sue azioni, in quanto essere razionale, quella di 'uomo neuronale', secondo una celebre espressione del neuroscienziato Changeux[9].

Sotteso al tema dello statuto epistemologico delle neuroscienze e dell'autonomia della ragione giuridica, cioè, giace il problema antropologico[10]. L'immagine dell'uomo restituita da un certo discorso neuroscientifico è quella di un animale determinato nei suoi processi comportamentali, prevedibili in quanto non liberi, dotato dell'illusione della volontà cosciente per meri fini evoluzionistici[11]. Nessuna

---

[7] L'articolo di green e Cohen costituisce in parte una replica agli argomenti espressi da Morse in S.J. MORSE, *New Neuroscience, Old Problems*, in B. GARLAND, *Neuroscience and the law: brains, minds and the scales of justice*, Dana press, New York 2004, pp. 157-198. Sull'invito alla 'neuromodestia' si veda dello stesso autore S.J. MORSE, *Avoiding Irrational NeuroLaw Exuberance: A Plea for Neuromodesty*, in *Mercer Law Review*, 62, 2011.

[8] Il sintagma è di Sergio COTTA, *La sfida tecnologica*, Il Mulino, Bologna 1968. Il progetto di naturalizzazione del diritto era a ben vedere già presente nel programma della Scuola Positiva del diritto penale, sulle cui affinità con le moderne neuroscienze si veda E. MUSUMECI, *Cesare Lombroso e le neuroscienze: un parricidio mancato. Devianza, libero arbitrio, imputabilità tra antiche chimere ed inediti scenari*, Milano, 2012. Così anche P. MARCHETTI, *Il cervello a giudizio. Le lontane origini di due recenti sentenze italiane*, in *Psicologia e Giustizia*, 2, 2012, pp. 1 e ss. A.C. PUSTILNIK, *Violence on the Brain: A Critique of Neuroscience in Criminal Law*, in *44 Wake Forest Law Review*, 2009, pp. 183 ss.

[9] J.-P. CHANGEUX, *L'homme neuronal*, Fayard, Paris 1983, trad. it. *L'uomo neuronale*, Feltrinelli, Milano 1988.

[10] Se è vero, con Kant, che la domanda su cosa è possibile conoscere è sempre una domanda su chi è il soggetto della conoscenza, sostanziandosi la filosofia nell'antropologia. Così, provando tuttavia a leggere le neuroscienze come emersione di un'altra antropologia, non riduzionista, S. FUSELLI, *Diritto neuroscienze filosofia. Un itinerario*, Franco Angeli, Milano 2014, in particolare pp. 20 e ss.

[11] R. WEGNER, *L'illusione della volontà cosciente*, in M. DE CARO, A. LAVAZZA, G. SARTORI, *Siamo davvero liberi? Le neuroscienze e il mistero del libero arbitrio*, Codice, Torino 2010, spec. p. 29. Così anche M. GAZZANIGA, *La mente inventata. Le basi biologiche dell'identità e della coscienza*, Guerini e Associati, Milano 1999.

discontinuità tra uomo e natura dunque, nell'attuazione di un antico sogno di riduzione dell'umano al naturale[12], che si staglia in netta contrapposizione all'antropologia dualistica emergente dai moderni sistemi giuridici[13]. Le neuroscienze del comportamento deviante[14] sono state così al centro della riflessione neurogiuridica degli ultimi anni, anche per i primi segnali di accoglimento da parte della giurisprudenza, soprattutto italiana[15]: gli ormai celebri casi Como e Trieste hanno dato ingresso a perizie neuroscientifiche volte ad accertare, per l'appunto, una preesistente debolezza neurogenetica, tale da inficiare la capacità di intendere e di volere dell'imputato.

Non è tuttavia questo il solo campo di osservazione delle intersezioni tra neuroscienze e diritto, e da una prospettiva più marcatamente filosofica, e – distinguendo con una evidente forzatura i due piani[16] – rispetto a modalità e condizioni di possibilità di utilizzo dei dati provenienti dalle neuroscienze nel sistema giuridico. Oltre cioè alla lettura neuroscientifica del comportamento deviante, le

---

[12] Le radici dell'antropologia riduzionista sono rintracciate nel materialismo illuminista da A. PUNZI, *L'ordine giuridico delle macchine. La Mettrie Helvétius D'Holbach: L'uomo macchina verso l'intelligenza collettiva*, Giappichelli, Torino 2003.

[13] A. LAVAZZA, L. SAMMICHELI, G. SARTORI, *Cervello, diritto e giustizia*, in A. LAVAZZA, G. SARTORI (a cura di), *Neuroetica. Scienze del cervello, filosofia e libero arbitiro*, Il Mulino, Bologna 2011, p. 135.

[14] Sulla individuazione di due macroaree nelle applicazioni delle neuroscienze al diritto, A. LAVAZZA, L. SAMMICHELI, *Diritto e neuroscienze*, in *RIFD. Rivista internazioneale di filosofia del diritto*, 4, 2013, pp. 545 e ss.

[15] Corte d'Assise d'Appello Penale di Trieste, n. 5/2009, Pres. Rel. Rainotti, in *Rivista Penale*, 1, 2010, pp. 70 e ss. Per un primo resoconto della sentenza in oggetto si vedano A. LAVAZZA, L. SAMMICHELI, *Se non siamo liberi possiamo essere puniti?*, in M. DE CARO, A. LAVAZZA, G. SARTORI, *Siamo davvero liberi?*, cit., pp. 156 e ss.; nonché, e in questo caso uno degli autori è lo stesso perito, G. SARTORI, A. LAVAZZA, L. SAMMICHELI, *Cervello, diritto e giustizia*, in A. LAVAZZA, G. SARTORI (a cura di), *Neuroetica*, cit., pp. 135 e ss; S. CODOGNOTTO, G. SARTORI, *Neuroscienze in Tribunale: la sentenza di Trieste*, in *Sistemi intelligenti*, 2, 2010, pp. 269 e ss. Nel 2011 un'altra sentenza ha dichiarato la semi-infermità sulla base di una perizia neurogenetica: Tribunale di Como, dott.ssa Lo Gatto, 29 agosto 2011.

[16] Distinguono nettamente tra la novità filosofica rappresentata dalle neuroscienze e le modalità di accoglimento della giurisprudenza A. LAVAZZA, L. SAMMICHELI, *Diritto e neuroscienze*, in *RIFD. Rivista internazioneale di filosofia del diritto*, 4, 2013, p. 549.

tecniche di scansione cerebrale si propongono di rendere intellegibili una serie ulteriore di dati. Il sentimento religioso, l'istinto di proprietà, l'esistenza di pregiudizi razziali (testimoniati dalla non attivazione dei neuroni specchio, i neuroni dell'empatia), la rilevazione del dolore, fino ai residui di coscienza nei soggetti affetti da stato vegetativo permanente: sono dati, questi, che coinvolgono oltre al profilo della immediata rilevanza giuridica – potendo in futuro consentire ad esempio di ricusare il giudice affetto da pregiudizi, o di invertire una diagnosi di stato vegetativo permanente qualora si riscontri ulteriore attività cerebrale prima non rilevata – un ordine di questioni filosoficamente rilevanti, che ancora una volta mettono in gioco l'immagine dell'uomo, scrutato nell'intimità della sua costituzione neurobiologica e pensato come la sommatoria delle informazioni che lo riguardano.

2. Verso la *neuro-data protection*.

Le tecniche di *mind detection*, allora, investono senza riserve il tema della privacy: dalla domanda di regolamentazione dell'uso e del trattamento di quei particolari dati emergenti dalla scansione cerebrale origina l'esigenza di riperimetrare la nozione di identità personale per il cui sereno sviluppo il nostro ordinamento pone a presidio la disciplina di tutela della *privacy*. Ci si è chiesti così se la disciplina europea in tema di protezione di dati personali, poi recepita e rafforzata dal cd. Codice della privacy[17], potesse ricomprendere nella nozione di dato sensibile il dato neurobiologico, considerando la stretta parentela che questo dato palesa con le informazioni genetiche. Come i dati genetici, infatti, che avevano fatto parlare di *genetic exceptionalism*[18] – formula poi prestata al presunto cambio di paradigma inaugurato dalle neuroscienze – i dati neurobiologici vengono presentati come espressivi di una capacità predittiva che

[17] *Codice in materia di protezione dei dati personali*, d. lgs 30 giugno 2003, n. 196.

[18] La formula è comunemente attribuita a T.H. MURRAY, *Genetic Exceptionalism and «Future Diaries»: Is Genetic Information Different from Other Medical Information?*, in M. ROTHSTEIN (a cura di), *Genetic Secrets: Protecting Privacy and Confidentiality in the Genetic Era*, Yale University Press, New Haven 1997.

richiede, oltre ad una riflessione sui limiti epistemologici della stessa, un inquadramento nel sistema di tutele. Il potenziale stigmatizzante dischiuso da un'informazione riguardante, ad esempio, la predisposizione neurogenetica ad un comportamento violento – come nei casi oggetto della giurisprudenza nostrana – ci interroga sulle linee di continuità che è possibile tracciare con la riflessione articolatasi intorno ai dati genetici. La medesima preoccupazione – nel senso della possibilità che poteri privati si approprino di tali informazioni per uso discriminatorio – animava, infatti, il Congresso statunitense, che nel 2008 approvava il *Genetic Information Nondiscrimination Act* (GINA), contenente il divieto espresso per assicurazioni e datori di lavoro di utilizzare a fini discriminatori i dati genetici[19].

Vale la pena ripercorrere schematicamente gli argomenti posti a fondamento del rafforzamento di tutela previsto per i dati genetici (il GINA arrivava a concludere il suo *iter* di approvazione dopo tredici anni di dibattito pubblico). Il primo argomento è quello epistemologico: tra la predisposizione genetica e l'insorgenza della malattia esiste un *gap* che può essere descritto solo in termini probabilistici, non già di causalità lineare[20]. L'incertezza costitutiva della genetica, allora, invita alla 'precauzione' nel trattare di dati rappresentativi di un mero rischio, che di certo non esauriscono l'identità del soggetto cui si riferiscono. Il secondo profilo è legato al

[19] La *Equal Emplyment Opportunity Commission* (EEOC), l'organo deputato a vigilare sul rispetto anche del GINA, ha avuto qualche difficoltà di funzionamento iniziale per i limitati poteri ispettivi di cui è in possesso. Nel 2012 per la prima volta è stato condannato un datore di lavoro che, a seguito di una visita medica implicante anche la raccolta di dati genetici, ha ritirato l'offerta di lavoro a tempo indeterminato a una sua precedente impiegata, nella quale avevano rilevato una predisposizione al tunnel carpale. EEOC v. Fabricut, Inc., 7 maggio 2013, U.S. District Court for the Northern District of Oklahoma.

[20] I soggetti geneticamente vulnerabili diventano così «malati di rischio», ed è a loro stessi che è demandata la gestione di questa incertezza, al «controllo di sé». Così V. MARZOCCO, Dominium sui. *Il corpo tra proprietà e personalità*, Editoriale Scientifica, Napoli 2012, pp. 40 e ss. Sul punto si veda anche *ex multis* A. SANTOSUOSSO, *Corpo e libertà*, spec. p. 254. Una lettura in termini di possibilità liberatoria offerta dai test genetici è offerta da S. SALARDI, *Test genetici tra determinismo e libertà*, Giappichelli, Torino 2010.

disvalore che gli ordinamenti dotati di un sistema di tutela della *privacy* assegnano ad un certo trattamento di dati 'sensibili', quali appunto quelli genetici. I rapporti che i limiti epistemologici intrattengono con il rafforzamento della tutela sono senza dubbio rilevanti; tuttavia sarà a questo punto utile rintracciare le consonanze tra gli argomenti posti a fondamento della privacy genetica e quelli – ancora da delineare – per la privacy mentale.

Sotto il primo aspetto, può essere utile riferire di un recente caso editoriale. Un noto neuroscienziato, James Fallon, pubblica nel 2013 un libro che riscuote molto successo, in cui racconta della sua esperienza: nel corso di alcuni esperimenti si è trovato a riscontrare nel suo stesso cervello le anomalie tipicamente presenti nei cervelli di psicopatici, pur non avendo questi mai manifestato una particolare aggressività[21]. Questo consentirebbe di approssimarsi alle perplessità sollevate a proposito di quell'incertezza costitutiva dei test genetici, che dicono di una probabilità tra gene e insorgenza della malattia, piuttosto che di una correlazione rappresentabile in termini di causalità lineare.

Quanto al secondo profilo – quello della tutela rinforzata rispetto ad altri dati, pure definiti sensibili – sarà opportuno operare delle precisazioni. La specificità del dato neuroscientifico, infatti, è da alcuni considerata tale da richiedere una messa in discussione della utilizzabilità della categoria della *privacy*, ritenuta non più adatta a rendere conto dei bisogni tutti nuovi di tutela innescati dalle neuroscienze[22]. I principali motivi di attrito, individuati a partire dalla regolamentazione europea in tema di protezione dei dati personali[23], sono in primo luogo attinenti alla tassatività dell'elencazione di dati sensibili operata dalla direttiva europea. Oltre a motivi formali, rileverebbe altresì l'impossibilità di tutelare con l'anonimato un dato

[21] J. FALLON, *The Psycopath Inside. A Neuroscientist's Personal Journey into the Dark Side of the Brain*, Current, New York 2013.

[22] D. HALLINAN, P. SCHÜTZ, M. FRIEDEWALD E P. DE HERT, *Neurodata and Neuroprivacy: Data Protection Outdated?*, in *Surveillance & Society*, 1, 2014, pp. 55-72.

[23] Il riferimento, com'è noto, è alla direttiva 95/46/EC del 1995.

che è *in se* rivelatore dell'identità di un individuo[24] (non a caso si parla di *brain fingerprint*), e la difficoltà di soddisfare quella *accuracy* richiesta ai gestori dei dati personali sia per l'intrinseca indeterminatezza nella rilevazione degli stessi, sia per la limitata capacità rappresentativa dell'identità nel tempo[25].

La rilevanza dei problemi sinora sollevati destano tante più perplessità quanto più si ponga mente al fatto che la scienza giuridica si è ben poco occupata del tema. E ciò nonostante quello della *privacy* mentale sia apparso sin dai primi esperimenti di *neurolaw* come banco di prova della disciplina: nel 2005 il *Committee on Science and Law* rendeva infatti pubblico un documento, *Are Your Thoughts Your Own?: "Neuroprivacy" and the Legal Implications of Brain Imaging*, ammonendo già all'epoca che «with the development of "brain fingerprinting" and other technologies, privacy concerns about advances in neuroscience are increasing». E in quegli stessi anni un accorto editorialista del *Philadelphia Inquirer*, John Timpane, scriveva:

> What if a brain-scan screener at the airport goes off, and I'm not allowed on the plane because I might be a troublemaker or a terrorist? Previously private aspects of my personality have been rendered public. Which leads to a chilling question: What if my thoughts cease to be my property?[26]

Queste ultime affermazioni consentono di rilevare due questioni, tra loro non irrelate: la prima proietta nel futuro i risvolti securitari dell'uso di informazioni neuronali. Il difficile bilanciamento tra *privacy* e sicurezza nella società dell'informazione costringe a ri-

[24] Difficoltà comune ai dati genetici: «[t]he concerns that have been expressed about using genetic information as a means of identification of one individual would apply to brain imaging information as well». Così Committee on Science and Law, *Are Your Thoughts Your Own?: "Neuroprivacy" and the Legal Implications of Brain Imaging*, 2005, p.11.

[25] *Ivi*, p. 66. L'articolo 6 della Direttiva afferma: «data must be: accurate and, where necessary, kept up to date» (European Parliament and Council 1995: Article 6(d)).

[26] John TIMPANE, Philadelphia Inquirer, 25 Gennaio 2004; Così anche Carey GOLDBERG, *Some Fear Loss of Privacy as Science Pries into Brain*, in *Boston Globe*, I Maggio 2003.

declinare i rapporti tra pubblico e privato, provando a superare le due tendenze reazionarie che la circolazione sempre più massiva di informazioni – implementata dalle nuove tecnologie di informazione e rilevazione – ha prodotto. La disponibilità a lasciarsi invadere dallo sguardo altrui in nome di una visibilità a tutti i costi, e senza il tentativo di distinguere tra ciò che è tecnologicamente possibile e ciò che deve essere giuridicamente consentito, legittimerebbe il pubblico, nonché i privati al tramonto del *Welfare*, ad un uso indiscriminato di ogni informazione riguardante i cittadini. Ogni aspettativa di *privacy* sarebbe così illegittima in una società trasparente che potrebbe attualizzare quel programma di controllo diffuso – dalla sorveglianza alla governamentalità – prospettato da Foucault[27].

Reazione opposta sarebbe quella di esacerbare le richieste di protezione della propria riservatezza, sottraendosi del tutto allo sguardo del potere pubblico. Tuttavia questa seconda opzione cela un paradosso: affinché il cittadino veda effettivamente tutelata la sua riservatezza nei confronti della pretesa di controllo esercitata dal potere pubblico, sarà quello stesso potere ad essere chiamato a garantire il diritto invocato. E perché la tutela richiesta sia effettiva il cittadino sarà poi costretto a fornire allo Stato tutte quelle informazioni che pure intendeva custodire gelosamente[28].

La posta in gioco, intorno a cui si definisce un possibile statuto di gestione delle informazioni neuronali, torna ad essere il modo di intendere la nozione di identità personale che, sebbene in affanno laddove la si pensi in esclusivo riferimento a categorie umanistiche, non può lasciarsi colonizzare dal linguaggio informazionale, che esaurisce l'uomo nella sua identità numerica. Questa riflessione

[27] Sulla nascita della società disciplinare il riferimento è al classico M. FOUCAULT, *Sorvegliare e punire. Nascita della prigione*, Einaudi, Torino 1993. La governamentalità è categoria su cui riflette Foucault nei corsi tenuti al Collège de France dal 1977 al 1979: ID., *Sicurezza territorio popolazione. Corso al Collège de France 1977-1978*, Feltrinelli, Milano 2005; ID., *Nascita della biopolitica. Corso al Collège de France 1978-1979*, Feltrinelli, Milano 2012.

[28] Sul paradosso di questa opzione regressiva, così come, più diffusamente sulle nuove frontiere della privacy nell'età informazionale si veda A. PUNZI, *Dialogica del diritto. Studi per una filosofia della giurisprudenza*, Giappichelli, Torino 2009, pp. 263-280; nonché *Diritto in.formazione*, Giappichelli, Torino 2014, spec. pp. 16-24.

introduce anche l'altro dei punti sollevati dall'editorialista: «What if my thoughts cease to be my property?» ci si chiedeva. E ugualmente al lessico proprietario ricorre il titolo della relazione diffusa dal *Committee on Science and Law*, «Are Your Thoughts Your Own?».

3. I nostri pensieri ci appertengono? Privacy mentale e *lie detection*.

Che i pensieri siano assimilabili a un bene oggetto di proprietà, sia pure in via metaforica, riferisce senz'altro delle origini storiche del diritto alla *privacy*[29], che nasce come diritto borghese, come proiezione di quel diritto di proprietà di cui riproduce le medesime logiche oppositive. È un diritto cioè da opporre *erga omnes*, nella forma che il pensiero costituzionalistico ha individuato come libertà negativa. È, del resto, quella della matrice proprietaria la provenienza 'genetica' di tutti i diritti di libertà, nella teorizzazione del liberalismo classico così come restituito da Macpherson[30]: ogni libertà si costruiva su quell'individualismo possessivo che considerava il soggetto di diritto dell'età liberale anzitutto come proprietario. La logica dominicale si estende tanto ai beni oggetto dello slancio appropriativo dell'individuo moderno, quanto – e prima ancora – al corpo proprio, la cui proprietà originaria fonda, nella celebre pagina lockiana, la proprietà privata. E sono altrettanto note le evoluzioni successive del diritto alla *privacy*, che si è ben presto disancorato da quella matrice proprietaria per diventare strumento di attuazione di libertà positive, rappresentando, in una delle efficaci definizioni di Stefano Rodotà, «il modo in cui percepiamo noi stessi, organizziamo le relazioni con gli altri, ci collochiamo in una comunità»[31]. La definitiva liberazione della categoria di *privacy* da suo originario *pedigree* di diritto borghese-liberale è attestata, del resto, dal primo riconoscimento che

[29] W.S.D. WARREN, L.D. BRANDEIS, *The right to privacy*, in *Harvard Law Review*, Vol. 4, No. 5, 1890, pp. 193-220

[30] C. B. MACPHERSON, *Libertà e proprietà alle origini del pensiero borghese. La teoria dell'individualismo possessivo da Hobbes a Locke*, Isedi, Milano 1973,

[31] S. RODOTÀ, *Intervista su privacy e libertà* a cura di P. Conti, Laterza, Roma-Bari 2005, p. 15.

l'ordinamento giuridico italiano ha accordato a questo diritto: lo statuto dei lavoratori[32].

Insistere sul motivo proprietario, al di là delle vicende evolutive del diritto alla privacy, è però utile per provare a leggere una delle più invocate e controverse applicazioni delle scansioni cerebrali al processo, le tecniche di *lie detection*. Tra gli ultimi ritrovati della diagnostica per immagini applicata al cervello vi sarebbe, infatti, la possibilità di attestare la veracità di un ricordo, così come la mendacità di una dichiarazione[33]. E se la giurisprudenza americana e italiana, seppur in sporadiche pronunce, è compatta nella opposizione a ogni forma di 'macchina della verità'[34], una recente pronuncia italiana apre alla possibilità di utilizzare una sorta di 'macchina della memoria'. Questi brevemente i fatti. Il Tribunale di Cremona (giudice dott. Guido Salvini, 24 febbraio 2012, sent. n. 823), ha reso una sentenza in cui il caso di molestie sessuali subito da una minore è stato deciso con la condanna del commercialista presso cui la ragazza svolgeva uno stage formativo. Nel corso del processo il giudice ha

[32] Lo statuto dei lavoratori aveva, infatti, previsto una norma presidiasse la riservatezza delle informazioni sui lavoratori per scongiurare il ripetersi delle schedature Fiat.

[33] Nel 2004, nel corso del convegno annuale della *Radiological Society of North America*, il dr. Faro presentò per la prima volta uno studio volto a dimostrare che quando si mente si attiva una parte del cervello diversa da quella usata quando si dice la verità. Il resoconto dell'esperimento è in F.B. MOHAMED, S.H. FARO, N.J. GORDON, S.M. PLATEK, H. AHMAD, MD, J.M. WILLIAMS, *Brain Mapping of Deception and Truth Telling about an Ecologically Valid Situation: Functional MR Imaging and Polygraph Investigation—Initial Experience*, in *Radiology*, 238, 2006, pp. 679-688. Sulle applicazioni della fMRI in questo specifico settore del diritto si veda L. SAMMICHELI, A. FORZA, L. DE CATALDO, *Libertà morale e ricerca processuale di verità: metodiche neuroscientifiche* in A. BIANCHI, G. GULOTTA, G. SARTORI (a cura di), *Manuale di Neuroscienze forensi*, Giuffrè, Milano 2010, pp. 231-246.

[34] Stante, in Italia, il divieto contenuto dall'art. 188 del c.p.p., che statuisce: «Non possono essere utilizzati, neppure con il consenso della persona interessata, metodi o tecniche idonei a influire sulla libertà di autodeterminazione o ad alterare la capacità di ricordare e di valutare i fatti». La giurisprudenza italiana sarà oggetto di analisi nel prosieguo. Qui basti segnalare i due casi recentemente decisi dalle Corti americane, che hanno negato l'ammissibilità della prova neuroscientifica in quanto non dotata del sufficiente grado di affidabilità scientifica. I casi sono: *Wilson v. Corestaff Services*, e *United States v. Semrau*.

sottoposto al perito, il Prof. Sartori – già autore delle perizie dei celebri casi Como e Trieste – il seguente quesito: «Dica il Perito, valutato preliminarmente il ricordo dell'evento come potenziale causa di disturbo clinicamente significativo, se la persona offesa, anche in considerazione della sua minore età e dello stato emotivo al momento del fatto, abbia subito un danno post-traumatico da stress o qualunque altro danno psichico riconducibile al reato denunciato. In questo caso ne chiarisca la natura, grado, durata e permanenza nel tempo». Per accertare il danno il Prof. Sartori ha fatto ricorso al test a-IAT (*Autobiographical Implicit Association Test*), che si basa, nelle parole del giudice, «su una valutazione del contenuto della memoria fondata sui tempi di reazione in risposta a frasi che descrivono l'evento autobiografico oggetto della verifica». Il *test* avrebbe verificato l'esistenza di tracce mnestiche della molestia nella vittima, consentendo all'esito di una indagine invero più articolata, di condannare l'imputato per il reato ascrittogli e liquidare a titolo di risarcimento del danno 25.000 euro alla vittima. Nonostante il test sia prevalentemente considerato altro dalle tecniche di *lie detection*[35], è chiaro come uno degli argomenti ricorsivamente addotti nel dibattito circa l'ammissibilità di tale tecnica sia presente anche in questo caso. Il punto, cioè, è se sia possibile per un individuo rinunciare alla sua riservatezza mentale volontariamente. Qui la rilevanza della trama proprietaria si palesa con evidenza: se i miei pensieri mi appartengono posso legittimamente disporne fino ad abdicare del tutto all'esercizio del diritto? Era questo, infatti, uno degli argomenti avanzati da Carnelutti nel corso di un dibattito su statuto della confessione e macchina della verità, che vide il giurista friulano e Piero Calamandrei su opposti fronti di discussione. In commento a una sentenza che aveva rifiutato la richiesta dell'imputato di sottomettersi al poligrafo[36], Carnelutti individuò criticamente le ragioni a fondamento della decisione (che a tutt'oggi marcano i confini del dibattito). Il problema dell'affidabilità scientifica della tecnica del poligrafo – al centro della

[35] Questo test non comporta una vera e propria scansione cerebrale, bensì valuta i tempi di reazione nell'associazione di concetti veri e falsi del periziando, sottoponendogli poi domande oggetto di perizia.
[36] Corte di Assise di Appello di Roma, 27 aprile 1956, in *Riv. dir. proc.*, 2, 1956, pp. 270 ss.

discussione contemporanea per la variante aggiornata dello stesso, la risonanza magnetica funzionale – era risolto sostenendo che le prove non vanno assunte solo in quanto idonee a garantire la certezza[37]. È il secondo argomento, tuttavia, a iscriversi nella complessa trama del rapporto tra libertà e proprietà. Quella libertà invocata come fondamento del diritto al segreto cela, per Carnelutti, una paradossale trappola per l'imputato:

> questi, anche se potesse fornire con certi esperimenti sul suo corpo, le prove della sua innocenza, dovrebbe essere condannato in omaggio alla sua libertà! (…) La libertà, veramente è *dominium sui*, (…) diritto sul proprio corpo (…). Naturalmente il *dominium sui* ha i suoi limiti come, del resto, la proprietà delle cose, nell'interesse degli altri o, secondo la formula tomistica, per il bene comune[38].

La libertà come *dominium sui*, dunque, come «diritto sul proprio corpo», che significa facoltà di disporre anche dei propri pensieri. Il problema è però legato soprattutto alla possibilità che l'inviolabilità dei pensieri vada sacrificata contro la volontà dell'imputato, al fine di conseguire la 'verità' dei fatti. La somministrazione forzata di tecniche volte ad aggirare la reticenza dell'imputato non può non rievocare gli orrori della tortura, funzionale ad un sistema che poneva la verità, e il conseguente obbligo di dire la verità, come finalità del processo. In questo senso si comprendono le perplessità avanzate da Calamandrei[39] rispetto alla posizione di Carnelutti, che proprio sull'obbligo di dire la verità per l'imputato fondava la sua iniziale apertura verso strumenti quali «macchina della verità, siero della verità, ipnosi, suggestioni»[40].

---

[37] F. CARNELUTTI, *Diritto dell'imputato agli esperimenti sul suo corpo*, in *Riv. dir. proc*., 2, 1956, p. 273.
[38] *Ivi*, pp. 273-274.
[39] P. CALAMANDREI, *Postilla a Francesco Carnelutti. A proposito di tortura*, in *Riv. dir. proc.*, 1, 1952, p. 239.
[40] Di qui una controversa affermazione di Carnelutti, che diede adito a numerose polemiche: «la tortura deve essere respinta perché non offre alcuna garanzia di verità della risposta del torturato, non perché lo costringe a palesare un segreto. Perciò se vi fosse un mezzo di coercizione, il quale fornisca tali garanzie senza cagionare

A nulla valse nemmeno la successiva sconfessione di tali tecniche, operata per il fatto che queste aggirerebbero la finalità prima della confessione, da considerarsi non più il raggiungimento della verità, bensì – da una prospettiva cristiana – il pentimento[41]. Molto chiara la censura mossa da Calamandrei a entrambe le argomentazioni di Carnelutti:

> io ritengo che quando si parte dalla premessa che vi sia nell'imputato un vero e proprio obbligo giuridico di dire la verità, e si nega che vi sia a suo favore un diritto al segreto o un diritto al silenzio, riconducibile tra i diritti di libertà, questa negazione porti a fil di logica a legittimare la tortura: e che allo stesso punto si arrivi anche (come purtroppo si arrivò in altri tempi; e il Beccaria ben lo sapeva, anche se per prudenza non lo scrisse *apertis verbis*) quando si dà alla confessione, e quindi alla tortura, una finalità religiosa di pentimento[42].

Il problema, in termini di bilanciamento tra diritti costituzionali, è chiaro. E tuttavia, ciò che sta al fondo della pretesa di accedere senza mediazioni ai pensieri altrui, connotandoli in termini di verità o falsità, è il disconoscimento di una ermeneutica del sé, cioè una comprensione dell'agire umano che assuma quale oggetto della riflessione il *chi*, l'uomo che agisce, non il *cosa* o il *perché*. Su questo punto è forte il richiamo a Paul Ricoeur, che iscrive il valore della testimonianza, impossibile da qualificare come 'vera', in quel percorso ermeneutico di comprensione del soggetto che passa per la sostituzione del sapere autofondante – la scienza – con l'attestazione

---

notevoli danni al corpo dell'inquisito, non vi sarebbe alcuna ragione perché non fosse adottato» (F. CARNELUTTI, *Lezioni sul processo penale*, vol. II, Roma 1947, p. 168).

[41] Sulla funzione della confessione si veda Foucault. «La confessione è un atto verbale attraverso cui il soggetto fa un'affermazione su ciò che egli è, si lega a questa verità, si colloca in un rapporto di dipendenza nei confronti di altri, e modifica allo stesso tempo il rapporto che ha con se stesso». M. FOUCAULT, *Mal fare, dir vero. Funzione della confessione nella giustizia. Corso di Lovanio (1981)*, Einaudi, Torino 2013, p. 9.

[42] P. CALAMANDREI, *Postilla a Francesco Carnelutti*, cit., p. 239.

(«io credo in»[43]). La testimonianza, infatti, più che vera può essere considerata verace, nella misura in cui si è disposti a credere nella parola del testimone[44]. E questi potrà anche essere «falso», ma – come avverte Ricoeur – «non c'è altro rimedio contro la falsa testimonianza che un'altra testimonianza più credibile»[45].

Le riflessioni del filosofo francese, dunque, apportano un ulteriore elemento per pensare criticamente al possibile uso delle nuove tecnologie – il *brain imaging* in special modo – nel processo. Ad un primo ordine di obiezioni, legate allo statuto epistemologico di tali tecniche, ad oggi non oggetto di condivisione assoluta nella comunità scientifica, si è aggiunto il profilo della problematica rilevanza della *privacy*, nell'ipotesi di somministrazione forzata di scansioni cerebrali che pretendano di decodificare la veracità di un'affermazione.

La questione è ben lungi dall'essere chiarita, ed è prevedibile che la scienza giuridica sarà in futuro chiamata a fornire risposte a interrogativi inediti, che coinvolgono – prima ancora che la corretta individuazione della forma di tutela – l'immagine dell'uomo che si intenda tutelare, e la sua identità personale.

---

[43] Scrive Ricoeur: «L'attestazione, in effetti, si presenta innanzi tutto come una forma di credenza. Ma non si tratta di una credenza dossica, nel senso in cui la *doxa* – l'opinione – possiede meno titoli di validità rispetto alla *épisteme* – la scienza, o meglio il sapere. Laddove la credenza dossica si iscrive nella grammatica dell''io credo che', l'attestazione scaturisce da quella dell''io credo in'». P. RICOEUR, *Soi-même comme un autre*, Seuil, Paris 1990, trad. it. a cura di D. Iannotta, *Sé come un altro*, Jaca Book, Milano 1993, p. 98.

[44] Ibidem.

[45] *Ivi*, p. 99.

Problematiche nella tutela dei dati personali e riflessi nei servizi cloud computing

di LUIGI PRINZI [*]

SOMMARIO: 1 Introduzione. – 2. Cloud Computing. – 2.1 Modelli originari. –2.2 Definizione. – 2.3 Modelli di erogazione dei servizi Cloud. – 2.5 Vantaggi del Cloud. – 3. Sicurezza informatica nel Cloud Computing – 4. Quadro giuridico comunitario vigente in materia di protezione dei dati – 4.1. Direttiva 95/46/CE – 4.1.1. Norme generali – 4.1.2. Funzioni e oneri in capo al responsabile del trattamento dei dati. – 4.1.3 Funzioni ed oneri in capo all'incaricato del trattamento dei dati – 4.1.4. Trasferimento verso Paesi terzi: art. 25 e 26. – 4.1.4.1. Concetti generali – 4.1.4.2. *Safe Harbor* – 4.1.4.3. Clausole contrattuali tipo (standard) – 4.1.5. Riflessi della direttiva 95/46/CE sul Cloud Computing. – 5. Evoluzione della normativa comunitaria sulla protezione dei dati personali – 5.1. Proposta di Regolamentazione generale della protezione dei dati del Parlamento europeo e del Consiglio – 5.1.1 Confronto con la normativa base vigente – 5.1.2 Strumenti di regolazione del trasferimento dei dati all'estero- 5.1.2.1 Norme basilari – 5.1.2.2 Norme vincolanti d'impresa (Binding Corporate Rules). – 5.1.3 Diritto all'oblio. – 6. Conclusioni.

1. Introduzione.

Sono dati personali tutte le informazioni associabili ad una persona, alla sua vita privata, o pubblica. Un nome, una foto, l'indirizzo e-mail, l'indirizzo IP, le coordinate bancarie, i *post* nei siti di social network, i dati relativi alla salute, e così via possono costituire un dato personale, ossia un dato che riguarda la persona in tutti gli ambiti della propria esistenza: a casa, al lavoro, quando fa acquisti oppure segue una cura medica, o naviga su Internet. Nell'era digitale poter raccogliere e conservare dati personali è fondamentale. Tutte le imprese ne fanno uso: dalle assicurazioni alle banche passando per i siti dei media sociali e i motori di ricerca. In un mondo globalizzato, il trasferimento

[*] Consulente per il settore delle reti e dei servizi di comunicazioni elettroniche.

di dati a paesi terzi è diventato un fattore importante della vita quotidiana. Non esistono frontiere nel web e il Cloud Computing è per l'appunto la tecnologia che permette di inviare dati da Berlino per trattarli a Boston e conservarli a Bangalore[1]. I dati raccolti, analizzati e trasferiti da una parte all'altra del mondo hanno acquistato un valore economico enorme e, come ha affermato Viviane Reding, vicepresidente della Commissione Europea presieduta da José Manuel Durão Barroso, sono divenuti "*la moneta corrente dell'economia digitale*"[2]. Secondo la Società di consulenza Boston Consulting Group, il valore economico dei dati dei cittadini dell'Unione Europea è pari a 315 M.di € nel 2011 e potrà crescere fino a 1.000 M.di € per il 2020[3]. Il diritto alla protezione dei dati di carattere personale è sancito dall'articolo 8 della Carta dei diritti fondamentali dell'Unione europea e la sua base giuridica figura all'articolo 16 del trattato sul funzionamento dell'Unione europea. Oggi gli strumenti per la raccolta di informazioni personali sono divenuti sempre più sofisticati e meno facili da rilevare. Basti pensare agli spyware installati nei PC da siti web cui essi si siano collegati, che raccolgono informazioni sulle abitudini di navigazione degli utenti, spesso per cederle a terzi. Non meraviglia quindi che sette europei su 10 temano l'uso improprio che le imprese possano fare delle informazioni da loro divulgate[4].

Occorre, pertanto, che la tutela della persona relativamente ai suoi dati personali, sia efficacemente protetta da una normativa che, riconoscendo i suoi diritti fondamentali, sia costantemente allineata all'evoluzione tecnica nella raccolta dei dati e nel loro trattamento. Ciò anche in considerazione del fatto che i dati, atteso il valore economico ad essi associato, costituiscono anche un'opportunità di business. La Privacy riguarda dunque la raccolta e, nel corso del trattamento, la riservatezza (accesso riservato a persone autorizzate), l'integrità, la conservazione e la disponibilità dei dati garantita a specifici soggetti, tra cui i clienti di una impresa, le persone od altre

[1] REDING V. Data Protection Day 2014: *Vice-President Reding calls for a new data protection compact for Europe*, PRESS RELEASE Brussels, 28 January 2014.
[2] EUROPEAN COMMISSION, Memo/14/60 "*Data protection day 2014:Full Speed on EU data Protection Reform"*, 27 January 2014
[3] Ibidem
[4] Ibidem.

entità i cui dati identificativi ed informativi siano processati in una procedura aziendale nell'ambito ad esempio di un sistema informatico o di servizi di comunicazione elettronica. Essa è sottoposta in ambito comunitario, e conseguentemente in ambito nazionale, ad una regolamentazione legislativa che copre tutti gli aspetti del trattamento, dall'archiviazione dei dati personali ad opera dell'impresa o della PA, a seguito del consenso rilasciato dall'interessato, o dalla loro immissione diretta nelle reti informatiche (E-mail, social network) da parte dell'interessato, al loro trattamento automatizzato o non, con implicazione o meno di un loro trasferimento oltre la frontiera nazionale. L'articolo 6 della Direttiva 95/46/CE dispone che i dati siano rilevati per finalità determinate esplicite e legittime, e successivamente trattati in modo non incompatibile od eccedente riguardo a dette finalità. Così, ad esempio, in un servizio che consista nell'archiviazione di record di dati personali medicali non si può farne uso per scopi diversi[5]. La protezione dei dati dovrebbe essere considerata non solo come una problematica dagli aspetti legali ed etici che ruotano attorno alla difesa della sfera privata dell'individuo, al cui rispetto vanno sempre prioritariamente conformate le policies aziendali in materia di tutela dei dati, meglio se secondo l'impostazione "*privacy by default*"[6] o "*privacy by design*"[7], ma anche come il superamento di una sfida tecnica, che si dispiega su due versanti, sicurezza ("security") e resilienza del sistema ICT che supporta con le sue infrastrutture e rende operativo con i suoi strumenti e risorse il trattamento dei dati personali.

La direttiva 95/46/CE stabilisce nell'art. 17 che gli Stati membri dispongano che l'incaricato al trattamento ("processor"), su indicazioni ed istruzioni del responsabile del trattamento

---

[5] HUSTINX P. *"Data Protection and Cloud Computing under EU law"* Third European Cyber Security Awareness Day BSA, European Parliament, 13 April 2010.

[6] Come nella previsione della COMMISSIONE EUROPEA, *Proposta di Regolamento del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (regolamento generale sulla protezione dei dati)*, COM(2012) 11, 25 gennaio 2012, art. 23.

[7] *ibidem*

("controller"), adotti ogni strumento appropriato atto a scongiurare la distruzione accidentale o illecita, la perdita accidentale o l'alterazione, la diffusione e l'accesso non autorizzato dei dati personali. Le suddette misure, compatibilmente con le conoscenze in materia ed i relativi costi di implementazione, devono garantire, secondo il legislatore comunitario, un livello di sicurezza appropriato ai rischi presentati dal trattamento ed alla natura dei dati da proteggere. La stessa norma con formulazione lievemente differente si ritrova nell'art. 30 della Proposta di Regolamento sulla protezione dei dati del 25 gennaio 2012, che, peraltro, a differenza della Direttiva, conferisce alla Commissione determinati poteri circa la fissazione dei criteri e delle condizioni concernenti le misure tecniche e organizzative di cui sopra. La scelta e l'affidamento dei servizi di trattamento dei dati da parte di un'impresa o PA che ne sia responsabile, che ne abbia quindi la titolarità, non può, pertanto, prescindere, né dall'adeguatezza dei livelli di sicurezza e resilienza[8] atti ad assicurare il conseguimento degli standard tecnici di tutela, né dall'osservanza delle disposizioni normative a tal uopo previste. L'E-Government Act degli USA definisce la sicurezza come la capacità di proteggere le informazioni e il sistema da accessi, utilizzi, comunicazioni, modifiche o distruzioni non autorizzati e di gestire la risposta e il recupero in caso di guasti o incidenti.

In ambito comunitario L'ENISA (European Network and Information Security Agency), l'organismo comunitario istituito nel 2004, la cui *mission* è di contribuire ad assicurare un elevato ed efficiente livello di sicurezza di rete e di informazione, ossia rafforzare la NIS (Network and Information Security) all'interno della Comunità europea, in maniera similare definisce la sicurezza: "*Security is the*

[8] NATIONAL INFRASTRUCTURE ADVISORY COUNCIL, "*Critical Infrastructure Resilience Final Report and Recommendations:* "The ability to reduce the magnitude and/or duration of disruptive events to critical infrastructure. The effectiveness of a resilient infrastructure or enterprise depends upon its ability to anticipate, absorb, adapt to, and/or rapidly recover from a potentially disruptive event" September 8, 2009. ENISA, **"***Benefits, risks and recommendations for information security"* "The ability of a system to provide and maintain an acceptable level of service in the face of faults (unintentional, intentional, or naturally caused)", novembre 2009.

ability to protect information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction and to respond and recover in case of a fault or incident"[9].

Nell'ambito del Cloud Computing – non una nuova tecnologia, bensì un nuovo modo di erogare servizi IT con modalità *web based* – la sfida di cui sopra, volta a garantire la sicurezza dei sistemi ICT e dell'informazione, appare ancora più complessa a causa della natura distribuita delle risorse informatiche, allocate in Data Center che possono essere ubicati in zone estremamente remote rispetto al paese di residenza degli utenti che usufruiscono dei servizi. Per tale ragione, in ambiente Cloud risulta più complicata la tutela normativa della persona interessata dalla privacy, essendo innanzitutto spesso controversa la fissazione della legislazione competente e l'accertamento del ruolo di "controller" o di "processor" ai sensi dell'art. 2 della direttiva 95/46/CE. Conseguentemente risultano più difficile l'adempimento degli obblighi che la direttiva e, nel nostro ordinamento, il Codice della protezione dei dati pone in capo al responsabile del trattamento dei dati, e più complessa la verifica che questo ultimo è in grado di effettuare nei confronti delle misure tecniche, legali e contrattuali che l'incaricato del trattamento ha rispettivamente messo in atto ed osserva. Basti pensare alla mancanza di conoscenza del cliente del Cloud circa i server dove sono memorizzati i suoi dati e circa i soggetti abilitati al loro accesso. Un'altra incertezza per il cliente è che la fornitura dei servizi di Cloud Computing è articolata, spesso, su una catena di fornitori e di altri operatori, tra cui i provider dei servizi di comunicazioni elettroniche, i quali si avvarranno sempre più di reti a banda ultra larga[10], che promettono di essere un fattore abilitante per il consolidamento del Cloud.

Sembra allora quanto mai opportuna la posizione della Commissione europea che, nella propria comunicazione del settembre

[9] ENISA, "*Security & Resilience in Governmental Clouds",* January 2011.
[10] 4G LTE (> 100 Mb/s); 3G HSPA (>10 Mb/s); FTTx GPON (> 100 Mb/s) e FTTx VDSL Vectoring (80 Mb/s).

2012[11], sottolinea la necessità di un quadro specifico per la 'nuvola', sia per le norme e la certificazione dell'adeguatezza delle misure di security, sia per le condizioni contrattuali che dovrebbero essere sicure ed eque. A loro volta le autorità pubbliche sono chiamate a contribuire alla creazione di un contesto affidabile per il Cloud in Europa.

2. Cloud computing.

2.1. Modelli originari.

Il Cloud Computing è, dal punto di vista tecnologico, l'evoluzione di concetti e tecnologie sviluppati in progetti di aggregazione di centri di supercalcolo con accesso tramite tecnologie web ed uso di tecniche di virtualizzazione (modello *Grid Computing*) e, dal punto di vista dell'accessibilità per gli utilizzatori alle risorse di calcolo e di memoria, è il modello di business che risponde alle loro istanze rendendo disponibili dette risorse informatiche in modo distribuito come *commodities*, alla stregua delle *utilities* telefonica, elettrica e così via (modello detto *Utility Computing*). Tradizionalmente le imprese private e pubbliche hanno sempre affidato a server ubicati nei loro stabilimenti, o a Data center dedicati, le applicazioni informatiche richieste dal business intrapreso, ma da alcuni anni, nei più vari settori (commerciale, finanziario, amministrativo), esse in misura crescente, valutabile ad oggi intorno ad 80%, le hanno in parte esternalizzate – estendendo l'*outsourcing* finanche alle applicazioni *core* – secondo vari livelli di utilizzo e varie tipologie delle risorse informatiche e di rete necessarie per le loro attività. Ciò in virtù dei progressi nell'accesso broadband ad Internet, nelle crescenti velocità dei circuiti elettronici dei processori negli elaboratori elettronici, della memorizzazione dei dati, nella virtualizzazione[12] e nelle tecnologie di

[11] COMMISSIONE EUROPEA, Com (212) 529 def., *Dispiegare il potenziale del Cloud Computing in Europa*.

[12] La virtualizzazione consiste nell'uso macchine virtuali, VM, ossia di server, computer virtuali, che eseguono programmi come se fossero server, computer fisici, in virtù dell'implementazione di un software (ipervisore, hipervisor) unico per una molteplicità di esse. Ogni VM include il proprio sistema operativo, librerie di

mobile computing che hanno reso più efficiente ed anche conveniente sotto l'aspetto dei costi trasferire ad un provider esterno i costi connessi con l'implementazione e relativa gestione dei componenti di un Data Center.

Gli *outsourcee*, ai quali le imprese e la PA si rivolgono, sono fornitori che si avvalgono di un limitato numero di Data Center, ma di ampia capacità, in cui c'è una concentrazione di risorse IT[13], accessibili via Internet (od Intranet nel caso di Private Cloud), che costituiscono quel paradigma di erogazione di servizi ICT universalmente denominato Cloud. Il nuovo modello di acquisizione di risorse informatiche è sintetizzata dalla succitata figura, in cui i rettangoli si riferiscono ad organizzazioni od operatori, interconnessi tra loro nel modello *in house*, e connessi direttamente a risorse IT in quello *cloud*. La flessibilità e la semplicità con cui è possibile configurare i sistemi in *cloud* ne rende possibile un dimensionamento 'elastico', ossia adeguato alle esigenze specifiche secondo un approccio basato sull'utilizzo. Gli utenti non devono curarsi della gestione dei sistemi informatici che, essendo utilizzati sulla base di accordi di esternalizzazione (outsourcing), sono completamente gestiti dai soggetti terzi nel cui *cloud* sono conservati i dati.

2.2. Definizione

Da quanto detto sopra si deduce che il "Cloud Computing" non è un concetto tecnologico radicalmente nuovo, bensì piuttosto un nuovo paradigma di acquisizione sul mercato di servizi di un Data Center decentrato rispetto all'acquisitore, in modo simile ai servizi pubblici elettrico o del gas. In breve il Cloud Computing si riferisce all'uso delle risorse computazionali (ossia hardware e software), che sono

---

supporto ed applicazioni. Il disaccoppiamento della VM, ossia l'astrazione dall'hardware sottostante consente alla stessa VM di iniziare il funzionamento su differenti macchine fisiche. Pertanto la virtualizzazione è un fattore abilitante fondamentale del Cloud Computing, in quanto consente al provider del Cloud Computing la necessaria flessibilità per spostare ed allocare le risorse del computer richieste dall'utente, dovunque le risorse fisiche siano disponibili.

[13] Cfr. ENISA, "*Critical Cloud Computing. A CIIP perspective on Cloud Computing services*" Version 1.0, December 2012.

veicolate attraverso una rete, tipicamente Internet, e rese disponibili nel punto in cui viene fatta la richiesta alla stregua di un qualunque servizio a rete. Secondo il Nist (Sep. 2011) *"Il Cloud Computing è un modello di abilitazione dell'accesso, conveniente e su richiesta, dovunque essa sia messa in atto, a un insieme condiviso di risorse computazionali variamente configurabili (ad esempio reti, server, memoria di massa, applicazioni e servizi), che possono essere rapidamente rese disponibili e rilasciate con un minimo sforzo di gestione e interazione con il fornitore del servizio"*.

2.3. Modelli di erogazione dei servizi cloud

Esistono vari modelli di erogazione del servizio Cloud richiesto da un utilizzatore. Il modello Private Cloud è un'infrastruttura ITC dedicata ai servizi richiesti da una singola organizzazione, dislocata all'interno della medesima, che può essere o no assegnata in outsourcing ad un terzo, nei confronti del quale il responsabile del trattamento esercita un controllo puntuale. Si tratta quindi in sostanza di un tradizionale centro di elaborazione dati (data center), nel quale però grazie a tecniche di virtualizzazione si consegue l'ottimizzazione in fatto di uso delle risorse disponibili.

Nel caso dei Public Cloud, invece, l'infrastruttura è di proprietà di un *provider* il quale mette a disposizione le proprie risorse informatiche a singoli utenti, imprese o pubbliche amministrazioni in forma condivisa. La veicolazione di tali servizi avviene tramite la rete Internet e implica il trasferimento delle operazioni di trattamento dei dati ai sistemi del fornitore del servizio, il quale assume pertanto un ruolo importante in ordine all'efficacia della protezione dei dati che gli sono stati affidati. Insieme ai dati, l'utente cede una parte importante del controllo esercitabile su di essi.

Accanto ai private e public Cloud sono da menzionare i cosiddetti Cloud 'ibridi', vale a dire combinazioni di Cloud in cui viè la compresenza di servizi erogati da infrastrutture private e servizi acquisiti da Cloud pubblici. Vanno citati anche i community Cloud (o Cloud di comunità) in cui l'infrastruttura informatica è condivisa da

diverse organizzazioni a beneficio di una specifica comunità di utenti[14].

2.4. Vantaggi del Cloud

La seguente tabella mostra un confronto tra soluzioni ITC tradizionali e soluzioni Cloud nelle varie combinazioni di modelli di servizio (*Iaas*, *Paas*, *Saas*) e di erogazione (Private, Public, Hybrid Cloud)

Sistemi ICT tradizionali	***Soluzioni CLOUD (ICT as Service)***
Consistenti investimenti HW/SW	Riduzione dei costi di investimento di start-up del sistema.
Accesso locale	*Broad Network Access* e distribuito. Le risorse telematiche (di calcolo, di storage, di software, di rete) sono accessibili via rete attraverso meccanismi standard che promuovono l'uso di piattaforme client eterogenee (ad esempio smartphone, laptop, PDA, ecc.)[15].
Risorse dedicate	Pool di risorse computazionali, di archiviazione e di capacità di rete, rese condivisibili per servire molteplici utenti, usando uno schema multi-cliente, che gestisce risorse fisiche e virtuali dinamicamente allocate e riallocate, in accordo con le indicazioni dei clienti Cloud. I clienti, salvo alcuni casi, non sono in grado di individuare la locazione fisica delle risorse, se non a un elevato livello di astrazione (ad esempio Stato o Data Center)[16].
Rigidità nel modulare il servizio.	Servizio acquisito on demand con caratteristiche di elevata disponibilità (probabilità in ogni istante di fruire del servizio richiesto dal cliente Cloud) e di

[14] Cfr. GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Parere 05/2012 sul cloud computing*, 1 luglio 2012.
[15] Cfr. CAVALLINI M. *Cloud Security: una sfida per il futuro*, Università Roma Tre, 15 marzo 2012.
[16] *ibidem*

	rapida elasticità tra richiesta al fornitore Cloud e suo soddisfacimento. Ciò grazie alla virtualizzazione dei server ed alla gestione dei picchi di carico di lavoro (*workload*), messi in atto dal fornitore Cloud, conferendo così alle infrastrutture messe in campo una capacità scalare. Il cliente Cloud consegue, pertanto, un rapido ed efficiente provisoning e deprovisioning delle risorse[17]. Il modello Cloud eredita la caratteristica del modello time sharing[18] -di accesso al Data Center- dell'apparente fruibilità senza limiti di quantità di risorsa utilizzata e della sua disponibilità in ogni momento.
"Time to market"	Drastica riduzione dei tempi di realizzazione e di messa in esercizio di nuovi servizi da lanciare sul mercato.
Energia Consumata	ottimizzazione dei consumi energetici sia nell'utilizzo delle risorse computazionali che nella refrigerazione dei Datacenter (Centri di elaborazione).
TCO	L'ottimizzazione dei costi sia in termini di risorse computazionali, sia in termini di risorse umane di gestione consentono al fornitore Cloud una riduzione anche oltre il 20% dei costi TCO ("Total Cost of Ownership") rispetto a Legacy ITC.
Costi fissi (da ammortizzare)	Tariffazione a consumo ("pay as you go") in base a parametri di misurazione del livello di servizio fornito. L'utilizzo delle risorse può essere monitorato, controllato ed elaborato, in piena trasparenza sia per il provider sia per l'utente del servizio[19].

Il Cloud Computing è oggi considerato sempre più come il futuro per la gestione delle risorse informatiche, dati i vantaggi che esso

[17] *ibidem*

[18] E' stato John McCarthy a predire, in un discorso del 1961, che l'accesso alle risorse del computer con modalità time-sharing si sarebbe tradotta un giorno nella messa a disposizione di risorse ed applicazioni informatiche tramite computer allo stesso modo di una utility pubblica.

[19] ibidem

presenta rispetto ai tradizionali sistemi IT, in particolare ai data Center aziendali, come mostra la tabella di cui sopra, dalla quale si evince come siano contenuti i costi sostenuti dal cliente Cloud, risultando essi di natura incrementale a fronte delle risorse informatiche utilizzate, con conversione da costi CAPEX[20] (CAPital EXpenditure) a OPEX (OPerating EXpenditure) per effetto del modello di pagamento *pay per use*. Peraltro, si rileva ancora una certa resistenza da parte di grandi aziende nel settore bancario, governativo o municipale, che pure abbiano deciso di acquisire le risorse informatiche necessarie dalla Nuvola, ad adottare un sistema Cloud interamente pubblico, nel senso di non ibrido, perché esse, oltre ai costi della transizione al nuovo modello di acquisizione di dette risorse, vedono dei rischi nel trattamento lasciato ai provider esterni del Cloud di informazioni particolarmente preziose o delicate per il loro core business.

Il ricorso al Cloud privato, quando non si dimostrino più efficienti soluzioni *in house*, è anche dovuto al fatto che i fornitori di Cloud publico spesso non sono in grado di garantire una qualità del servizio (sulla base di accordi sul livello del servizio) compatibile con la natura delicata del servizio che deve erogare il responsabile del trattamento, perché, ad esempio, larghezza di banda e affidabilità della rete non sono sufficienti o adeguate in una data area[21]. Se è vero che il Cloud privato è preferibile inizialmente in ottica protezione dei dati, nel lungo termine può risultare meno conveniente del pubblico per ragioni di costo.

3. Sicurezza informatica nel Cloud Computing

Nel nuovo modello di erogazione di risorse informatiche *as a service*, basato sulla concentrazione di risorse IT nei Data Centers con

[20] Le spese di capitale (capital expenditures) sono quelle connesse all'acquisto di capitali fissi (beni strumentali, impianti), inscritte nel conto patrimoniale del bilancio ed ammortizzate (depreciated) lungo la durata economica del relativo asset, mentre le spese operative (operating expenses) sono registrate nel conto profitti e perdite del bilancio e si riferiscono a spese correnti, tipicamente di esercizio e manutenzione.

[21] GRUPPO DI LAVORO PER LA TUTELA DEI DATI EX ART. 29, *Parere 05/2012 sul Cloud Computing*, adottato nel luglio 2012.

le relative infrastrutture di interconnessione, tra cui fondamentalmente Internet, si vengono così a costituire delle infrastrutture critiche di trasporto dell'informazione CII (Critical Information Infrastructure), che, se da un lato procurano innumerevoli benefici tecnici ed economici in sede di utilizzo, dall'altro pongono nuove sfide alla garanzia della sicurezza del sistema ICT ove risiedono o vengono veicolati i dati vitali per gli interessi di business e di servizi erogati al pubblico di imprese private e pubbliche che ricorrono ai servizi Cloud, e, conseguentemente, al mantenimento della disponibilità ed integrità di tali informazioni.

In sede comunitaria la Direttiva 2008/114/CE del Consiglio, con riferimento specifico ai settori energia e trasporto, definisce "*«infrastruttura critica» IC un elemento, un sistema o parte di questo ubicato negli Stati membri che è essenziale per il mantenimento delle funzioni vitali della società, della salute, della sicurezza e del benessere economico e sociale dei cittadini ed il cui danneggiamento o la cui distruzione avrebbe un impatto significativo in uno Stato membro a causa della impossibilità di mantenere tali funzioni*". La Direttiva in parola rappresenta il primo passo di approccio graduale inteso a designare la procedura europea per l'individuazione delle CII e dovrebbe essere rivista per includere nel suo campo di applicazione il settore ICT. Inoltre in una Comunicazione del 2009 la Commissione europea ha definito[22] come "*Critical Information Infrastructures*" tutti i sistemi ICT che sono o infrastrutture critiche di per sé o essenziali per l'operatività di altre infrastrutture critiche. La Comunicazione in parola individua tre tipi di minaccia alla sicurezza delle CII: (i) cyber attacchi (v. attacchi DDoS –Distributed Denial of Service – in Estonia nel 2008), (ii) disastri naturali; (iii) cyber disruptions (guasti tecnici su vasta scala), che comportano una perdita temporanea o permanente del servizio, con impatto sugli utenti del servizio Cloud che si affidano alla sua continuità (es. taglio del cavo sottomarino transatlantico nel 2008).

Il pacchetto di riforma del 2009 del quadro regolatorio delle reti e servizi di comunicazioni elettroniche contiene norme sulla security ed

[22] COMMISSIONE EUROPEA, COM(2009) 149 final, *Communication on critical Information Infrastructure Protection*, Brussels, 30 marzo 2009.

integrità, rafforzando gli obblighi degli operatori ad assicurare appropriate misure per l'identificazione dei rischi, la garanzia della continuità di fornitura del servizio e la notifica delle violazioni della security. Internet è certamente una CII e si richiede quindi particolare attenzione alla sua resilienza e stabilità, costituendo essa un ecosistema che supporta una quantità innumerevole e crescente di servizi della SI che vanno da quelli bancari ai servizi per la salute. Internet grazie al suo progetto di architettura distribuita e ridondata si è dimostrata una infrastruttura molto robusta, nella sua complessità fisica e logica, ma data anche la varietà del suo utilizzo e le nuove applicazioni che se ne avvalgono, il numero di *disruptions* e di attacchi cyber che essa subisce è in continuo aumento.

Nella definizione di CII – sistemi ICT vitali per l'economia della Società o del Paese – rientrano senz'altro i servizi offerti dal Cloud, non fosse altro che per il loro imprescindibile impiego di Internet. La nuvola informatica, infatti, in tutte le sue possibili implementazioni servirà nell'immediato futuro una gran parte dei cittadini europei, nonché moltissime PMI e PA e pertanto le infrastrutture di cui essa si avvale per la fornitura dei servizi richiesti dagli utilizzatori, spesso di vitale importanza o comunque di grande impatto sulla vita economica e sociale, devono essere protette dai rischi sopra illustrati. Se è vero, infatti, da un lato che i grossi Cloud provider sono in grado di mettere in atto misure di security e di resilienza allineate allo stato dell'arte, distribuendo tra i loro utenti Cloud i relativi costi, dall'altro lato nei casi, peraltro infrequenti, di interruzioni o violazioni nei sistemi di security, è stata compromessa un'enorme quantità di dati, che ha interessato molte organizzazioni quali utilizzatrici dei servizi Cloud e milioni di utenti nella veste di data subjects. Si citano i casi seguenti di guasti localizzati, che hanno interessato infrastrutture Cloud[23].

Nel corso di una tempesta l'otto agosto 2011 un fulmine colpì non solo i trasformatori, ma anche i generatori di backup dei Data Center di Amazon e Microsoft ubicati nella zona di Dublino, provocando l'interruzione di ogni forma di alimentazione elettrica e mandando quindi in tilt i servizi Cloud forniti a molti loro clienti, EC2 (Elastic

[23] ENISA, *Critical Cloud Computing: A CIIP perspective on Cloud Computing services*, Version 1,0, December 2012

Compute Cloud) ed EBS (Elastic Block Storage) nel caso di Amazon, e soltanto due giorni dopo essi furono ripristinati.

Nell'estate del 2011 un difetto di software in un servizio SaaS, che forniva backup ed archiviazione di documenti, mise in crisi la sicurezza dei dati, dal momento che ciascun utente Cloud fu in grado di vedere I documenti di milioni di altri utenti per almeno 8 ore.

Peraltro anche in questi casi eccezionali, ma di potenziale tremendo impatto su infrastrutture critiche dell'informazione, è venuta in soccorso la ben più elevata resilienza delle soluzioni Cloud rispetto ai tradizionali sistemi IT, che permette la sopravvivenza dei servizi Cloud, a fronte di disastri naturali (es. terremoto in Giappone del 2011) che mettono in ginocchio le tradizionali reti ed impianti di TLC, grazie ai propri specifici servizi di emergenza e reti fisse e mobili di cui è dotata una soluzione Cloud[24]. Diversamente sarebbe assai più difficoltoso mitigare l'impatto di questi eventi di calamità naturale (inondazioni, tempeste, terremoti) sulla continuità di servizio di un singolo Data Center, o di infrastrutture ITC tradizionali. Un rischio non meno temibile che richiede la predisposizione di mezzi di difesa ancor più sofisticati nelle soluzioni di Cloud Computing è costituito dagli attacchi Cyber che cercano di individuare le falle del software per mettere in atto pesanti violazioni dei dati che colpiscono in maniera diretta milioni di utenti. L'effetto moltiplicativo dell'impatto di questi attacchi è causato dalla concentrazione di risorse che, come già evidenziato, è un risultato dell'introduzione del Cloud Computing. I modelli Cloud di maggiore criticità sono quelli IaaS e PaaS, che forniscono servizi ad altri venditori IT, come difatti è anche il Cloud provider, che a loro volta servono milioni di utenti ed organizzazioni. Anche a fronte di attacchi cyber i Cloud provider dispongono delle risorse per prevenirli o mitigarli in un modo più professionale della maggior parte delle altre organizzazioni, ad esempio creando delle ridondanze logiche, ossia l'impiego di differenti livelli di difesa e di sistemi separati con una differente struttura logica, al fine di effettuare un controllo incrociato delle transazioni per scoprire gli attacchi. L'elasticità è un beneficio chiave del Cloud Computing, contribuendo all'allocazione dei carichi di lavoro e mitigando così il rischio di

[24] *ibidem*

sovraccarichi o di attacchi cyber. Sarebbe, invece, difficile fronteggiare l'impatto dei picchi di utilizzazione o di un attacco cyber avendo a disposizione risorse computazionali limitate.

Il problema della sicurezza di origine tecnologica, sopra delineato, è un freno alla diffusione dei servizi Cloud, essendo considerato cruciale da molti potenziali acquirenti, atteso che i servizi offerti da un Cloud Provider (CP) comportano il trattamento di un intenso flusso di dati di natura personale, relativi non solo a dipendenti del CP ma anche a fornitori, partner commerciali, Cloud Customer collegati al cliente Cloud. A questo riguardo, occorre tener presente che i rischi relativi al trattamento dei dati dipendono, nella loro tipologia ed entità, dal modello di erogazione prescelto (Private Cloud, Community Cloud e Public Cloud). Il Public Cloud, oltre ad essere la soluzione più efficiente dal punto di vista dei costi, offre un'elevata resilienza e potenzialmente il più alto grado di disponibilità del servizio d'accesso ai dati, ma la complessità regolatoria che sottende il trasferimento dei dati oltre il confine nazionale, sia verso Stati in ambito UE che extra-Ue, suggerirebbe di limitarne l'utilizzo a dati non sensibili o ad applicazioni non–core per l'utente e di prevedere delle *exit-strategies* per questo ultimo. Le maggiori preoccupazioni per l'adozione dei servizi di Cloud Computing, specialmente per quanto riguarda i modelli di erogazione di Public o Hybrid Cloud, nutrite dalle PMI, riguardano gli aspetti della sicurezza, che si possono sintetizzare in (i) perdita di riservatezza, (ii) disponibilità dei dati, (iii) integrità dei dati, (iv) perdita di controllo sui dati, nonché quelli legati alla disomogeneità dei requisiti legali imposti dalla normativa della privacy comunitaria ed extra-europea. Invero la distribuzione delle risorse informatiche in ambiente Cloud su più siti e la loro allocazione dinamica a seconda delle richieste dei clienti Cloud che le condividono[25] e dei conseguenti carichi di lavoro, genera problemi di security nuovi rispetto a quelli che comportano i tradizionali sistemi informativi. E' pur vero che il Cloud Provider può garantire standard

[25] Si parla "multi-tenant model" per i servizi Cloud, basato sulla condivisione di dati tra diversi Cloud Consumer, che rendendo non fisica, bensì virtuale la separazione dei rispettivi ambienti può dar luogo a criticità circa la riservatezza dei dati di ciascuno di loro.

di sicurezza superiori grazie ad investimenti ingenti, rispetto ai tradizionali Data Center, con ricorso ad architetture ridondate e geograficamente distribuite e più sofisticati sistemi di monitoraggio automatizzati della regolarità e disponibilità degli accessi alle risorse rese disponibili agli utenti, ma paradossalmente la collocazione da parte sua in pochi luoghi di enormi quantità di dati può rappresentare un obiettivo ancora più attraente per gli attacchi informatici. Disincentivante per l'adozione di servizi Cloud è poi la sostituzione del controllo diretto sulle risorse di calcolo e/o storage, la cui perdita si rifletterebbe negativamente sulla sicurezza di rete e di informazione, con un controllo fondato su clausole contrattuali (contratto di servizio, indicatori di prestazioni) o su strumenti software, che comunque è più debole ed indiretto. In linea generale, il modello di servizio SaaS è chiaramente la soluzione che offre al cliente Cloud un minor controllo diretto sui parametri di sicurezza e resilienza, lasciando più controllo e responsabilità nelle mani del Cloud provider, mentre il modello IaaS è quello che garantisce un maggior controllo diretto al cliente rendendolo quindi pienamente responsabile per l'implementazione delle misure tecniche e procedurali in ordine al mantenimento dei livelli prescritti di tali parametri.

All'insufficiente *governance* dei processi si aggiunge il rischio di *lock-in*, ossia di "imprigionamento della domanda", generato dalla difficoltà, tanto di natura contrattuale unita al sostenimento di costi eccessivi insita nell'eventuale scelta di abbandonare l'ambiente Cloud e tornare ai servizi *in house* o cambiare fornitore Cloud, quanto di natura tecnica dettata dalla significativa concentrazione del mercato già in atto – caso degli *over the top* – tendente alla creazione di limiti all'interoperabilità, ossia alla capacità di sistemi computazionali diversi di interagire fra loro attraverso anche lo scambio di dati. L'interoperabilità è una condizione necessaria per l'instaurarsi di un mercato concorrenziale nei servizi Cloud, eliminando le barriere tecniche al cambiamento lato domanda e riducendo la frammentazione del mercato unico[26].

[26] In tal senso, G. CREA, *Il settore pubblico e la tutela degli utenti nella prospettiva della cloud economy*, in *questa rivista*, n. 2, 2012, 279-312.

4. Quadro giuridico comunitario vigente in materia di protezione dei dati.

Il quadro giuridico relativo alla tutela dei dati è costituito da due direttive, quella sulla protezione dei dati 95/46/CE (*Data Protection Directive)*, del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, che si applica a tutti i casi di trattamento di dati personali, quindi anche nell'ambito di servizi di *Cloud Computing*, e l'altra *e-privacy* 2002/58/CE (modificata dalla direttiva 2009/136/CE). La direttiva *e-privacy*, che concerne il trattamento di dati personali e alla tutela della vita privata nel settore delle comunicazioni, si applica ai fornitori di servizi di comunicazione elettronica accessibili al pubblico e impone loro di garantire il rispetto degli obblighi relativi alla segretezza della comunicazione e alla protezione dei dati personali, nonché i diritti e gli obblighi concernenti le reti e i servizi di comunicazione elettronica. La direttiva stabilisce un legame più stringente ed esplicito tra la *data protection* e la sicurezza delle reti e dell'informazione da esse veicolata.

4.1. Direttiva 95/46/CE.

4.1.1. Norme generali.

La direttiva 95/46/CE si prefigge il completamento di un mercato interno (in questo caso, la libera circolazione delle informazioni personali) e la tutela dei diritti e delle libertà fondamentali dei cittadini. La direttiva in parola (in appresso "la direttiva") si riferisce esplicitamente al concetto di "responsabile del trattamento" e di "incaricato del trattamento" in diverse disposizioni, fornendone le definizioni, di cui all'articolo 2, lettere d) ed e)[27]. La stessa direttiva

[27] "responsabile del trattamento" ("controller", "controller of the file" , ossia "responsabile del casellario", termine adoperato dalla Convenzione 108 stipulata dal Consiglio d'Europa nel 1981) : *la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che, da solo o insieme ad altri, determina le finalità e gli strumenti del trattamento di dati personali*.

ha adottato una nozione di "trattamento di dati personali" piuttosto ampia, definendolo all'articolo 2, lettera b) della direttiva come "*qualsiasi operazione o insieme di operazioni compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali, come la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione o la modifica, l'estrazione, la consultazione, l'impiego, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, nonché il congelamento, la cancellazione o la distruzione*."

4.1.2. Funzioni e oneri in capo al responsabile del trattamento dei dati[28].

Il concetto di responsabile (*controller*), non è stato quindi più riferito dalla direttiva a un oggetto statico ("il casellario"), bensì ricollegato a attività rispecchianti il ciclo di vita delle informazioni, dalla raccolta alla distruzione. Inoltre l'articolo 6, paragrafo 2 della Direttiva stabilisce esplicitamente che "il responsabile del trattamento è tenuto a garantire il rispetto delle disposizioni del paragrafo 1" – ossia dei principi fondamentali relativi alla qualità dei dati, fra cui quello, sancito all'articolo 6, paragrafo 1, lettera a), secondo cui "*i dati personali devono essere trattati lealmente e lecitamente*". Da ciò si evince che tutte le disposizioni relative alle condizioni per il trattamento lecito dei dati si rivolgono al responsabile del trattamento. Anche le disposizioni sui diritti dell'interessato (informazione, accesso, rettifica, cancellazione, congelamento e opposizione al trattamento dei dati personali (articoli 10-12 e 14)) sono state formulate in modo tale da creare obblighi per il responsabile del trattamento, la cui figura è inoltre centrale nelle disposizioni sulla notificazione e il controllo preliminare (articoli 18-21). Non sorprende, infine, il fatto che il responsabile del trattamento debba

"incaricato del trattamento": la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che elabora dati personali per conto del responsabile del trattamento.

[28] Cfr. GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Parere 1/2010 sui concetti di "responsabile del trattamento" e "incaricato del trattamento"*, 16 febbraio 2010.

anche rispondere, in linea di principio, per eventuali danni cagionati da un trattamento illecito (articolo 23). L'articolo 17, paragrafo 1 della direttiva stabilisce che il responsabile del trattamento "*deve attuare misure tecniche ed organizzative appropriate al fine di garantire la protezione dei dati personali dalla distruzione accidentale o illecita, dalla perdita accidentale o dall'alterazione, dalla diffusione o dall'accesso non autorizzati, segnatamente quando il trattamento comporta trasmissioni di dati all'interno di una rete, o da qualsiasi altra forma illecita di trattamento di dati personali*".

Il concetto di responsabile del trattamento è inoltre un elemento fondamentale per stabilire la giurisprudenza competente applicabile a un trattamento dei dati. La principale disposizione relativa al diritto applicabile, di cui all'articolo 4, paragrafo 1, lettera a) della direttiva, prevede che ciascuno Stato membro applichi le proprie disposizioni nazionali "*al trattamento di dati personali* [...] *effettuato nel contesto delle attività di uno stabilimento del responsabile del trattamento nel territorio dello Stato membro*". E la disposizione continua nel modo seguente: "*qualora uno stesso responsabile del trattamento sia stabilito nel territorio di più Stati membri, esso deve adottare le misure necessarie per assicurare l'osservanza, da parte di ciascuno di detti stabilimenti, degli obblighi stabiliti dal diritto nazionale applicabile*".

In altri termini, se il responsabile del trattamento ha sede in vari Stati membri e il trattamento di dati rientra nelle attività svolte in tali paesi, il diritto applicabile sarà quello di ciascuno degli Stati membri in cui viene effettuato il trattamento. Ciò significa che gli stabilimenti del responsabile del trattamento, uno o più, determinano anche i diritti nazionali applicabili, ed eventualmente una serie di leggi nazionali competenti e il modo in cui sono collegate fra di loro. L'articolo 4, paragrafo 1, lettera c) estende l'applicazione del diritto nazionale della privacy nello Stato membro al caso dei responsabili del trattamento, che non siano stabiliti nel SEE (Spazio Economico Europeo), ma ricorrano a strumenti automatizzati o non automatizzati situati nel territorio dello Stato membro (ad esempio Data Center per l'archiviazione e l'elaborazione in remoto di dati personali, elaboratori, terminali, server), a meno che questi non siano utilizzati ai

soli fini di transito nel territorio comunitario. Dall'analisi dell'art. 4 della Direttiva segue che:
a) l'ubicazione geografica dello stabilimento del controller impatta sulla sua applicazione;
b) ciò che invece non rileva a tale riguardo è il posto in cui ha luogo il trattamento dei dati, salvo nel caso che il controller sia stabilito al di fuori del SEE;
c) in tutti i casi non è assolutamente rilevante la residenza del soggetto interessato (*data subject*).

Le norme del suddetto articolo sono state tra le più criticate nel corso del processo di revisione della normativa comunitaria sulla privacy. Alcuni hanno sostenuto la necessità dell'applicazione della norma del paese d'origine che consentirebbe alle organizzazioni multinazionali di operare rispettando una sola serie di norme in tutta l'Unione. Molti hanno anche affermato che il ricorso "a strumenti" non costituisce un criterio appropriato o pratico per determinare l'applicazione del diritto dell'UE ai responsabili del trattamento non stabiliti nel territorio della Comunità. Per quanto riguarda la norma del paese d'origine la direttiva già consente l'organizzazione del trattamento facente capo a un unico responsabile, il che comporta l'ottemperanza soltanto alla normativa in materia di tutela dei dati del paese in cui il responsabile è stabilito. Per quanto concerne il ricorso "a strumenti" la Commissione è consapevole che tale criterio potrebbe risultare di difficile applicazione nella pratica e che esso richiede un ulteriore chiarimento. Tenuto conto, pertanto, anche degli sviluppi tecnologici, la Commissione ha disposto una proposta di modifica, peraltro non limitatamente all'articolo 4, bensì estesa all'intero testo della direttiva, alla luce anche dell'evoluzione tecnica.

4.1.3 Funzioni e oneri in capo all'incaricato del trattamento dei dati[29].

Il concetto di "incaricato del trattamento" riveste un ruolo importante nel contesto della riservatezza e sicurezza dei trattamenti (articoli 16-17), poiché serve ad individuare le responsabilità di coloro

[29] Cfr. GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Parere 1/2010*, cit.

che si occupano più da vicino dell'elaborazione dei dati personali, sotto l'autorità diretta del responsabile del trattamento o per suo conto. La distinzione fra i due concetti "responsabile" ed "incaricato" serve per lo più a differenziare fra la persona che ha l'effettiva responsabilità in qualità di "responsabile del trattamento", e la persona che agisce semplicemente per conto di quest'ultimo. Nel caso dell'incaricato del trattamento vi è comunque un'ulteriore conseguenza che interessa anche il responsabile del trattamento: ai sensi dell'articolo 17 della direttiva, il diritto applicabile alla sicurezza dei trattamenti è quello dello Stato membro nel quale è stabilito l'incaricato del trattamento. Per poter agire come incaricato del trattamento occorrono due requisiti: essere una persona giuridica distinta dal responsabile del trattamento ed elaborare i dati personali per conto di quest'ultimo. Questa attività di trattamento può essere limitata a un compito o a un contesto molto specifici o può essere più generale ed ampia. Ad esempio, un *provider* di servizi Internet (ISP) che fornisce servizi di *hosting* è in linea di principio un incaricato del trattamento per i dati personali pubblicati on-line dai suoi clienti, che si rivolgono a lui per l'hosting e la manutenzione del loro sito web. Se tuttavia l'ISP tratta ulteriormente, per scopi propri, i dati contenuti nei siti web, diventa responsabile per tale specifico trattamento. L'analisi sarebbe diversa per un ISP che fornisce servizi di posta elettronica o di accesso a Internet. In tale ottica, la liceità dell'attività di trattamento dei dati da parte dell'incaricato è determinata dal mandato ricevuto dal responsabile del trattamento. Se va al di là del proprio mandato e se acquisisce un ruolo rilevante nella determinazione delle finalità o degli aspetti fondamentali dei mezzi del trattamento, l'incaricato diventa (cor)responsabile.

L'articolo 17, in relazione alla sicurezza dei trattamenti, stabilisce la necessità di un contratto o di un atto giuridico vincolante che disciplini le relazioni fra il responsabile e l'incaricato del trattamento. Deve trattarsi, a fini di conservazione delle prove, di un contratto stipulato per iscritto che deve avere un contenuto minimo, e che deve prevedere segnatamente che l'incaricato del trattamento dei dati operi soltanto su istruzioni del responsabile del trattamento, e che attui misure tecniche e organizzative per proteggere adeguatamente i dati

personali. Il contratto deve includere una descrizione sufficientemente dettagliata del mandato dell'incaricato del trattamento.

4.1.4. Trasferimenti verso paesi terzi: articoli 25 e 26.

4.1.4.1 Concetti generali.

L'art. 25 della Direttiva stabilisce le condizioni di liceità del trasferimento di dati in un Paese esterno all'UE o al SEE (Spazio Europeo Economico) e le procedure messe in atto dallo stato Membro o dalla Commissione ai sensi dei poteri conferitile dall'art. 31, paragrafo 2, in base alle quali viene sancita detta liceità o la sua negazione e corrispondentemente presa un'autorizzazione od una decisione, rispettivamente dallo Stato membro e dalla Commissione. Il criterio di giudizio è costituito dall'adeguatezza del livello di protezione dei dati personali garantito dal Paese estero, valutata in base a vari parametri, tra cui la natura dei dati oggetto del trasferimento, la finalità del trattamento prevista, il Paese d'origine ed il Paese di destinazione finale, le norme di diritto in tema di trattamento dei dati personali dati vigenti nel Paese terzo di cui trattasi, gli impegni internazionali da questo eventualmente sottoscritti -per quanto riguarda la vita privata o le libertà e i diritti fondamentali della persona- a seguito di constatazione di inadeguatezza della tutela dei dati constatata dalla Commissione, nonché le regole professionali e le misure di sicurezza ivi osservate. Gli Stati membri hanno l'obbligo di notifica vicendevole tra loro ed alla Commissione dei casi in cui, a loro parere, un Paese terzo non garantisce un livello di protezione adeguato. Con valore immediatamente esecutivo, la Commissione europea può prendere la decisione ai sensi del paragrafo 6 art. 26 (decisione di adeguatezza)[30], sulla base di un procedimento che prevede, fra l'altro, il parere favorevole del Gruppo di Lavoro ex Articolo 29 della Direttiva 95/46/CE, che il livello di protezione

[30] Le decisioni di adeguatezza della Commissione sinora pubblicate riguardano i seguenti Paesi: Andorra, Argentina, Australia-PNR (trattamento dati nelle procedure di imbarco aereo dei passeggeri ed alle dogane), Canada, Faer Oer, Guernsey, Isola di Man, Israele, Nuova Zelanda, Svizzera, Uruguay, Usa Safe-Harbor, USA –PNR.

offerto in un determinato Paese è adeguato, e che pertanto è lecito trasferire in esso dati personali. Lo stesso procedimento segue la Commissione nelle decisioni di inadeguatezza, che notificherà agli Stati membri. Gli Stati membri adottano le misure necessarie per conformarsi alla decisione della Commissione nell'uno e nell'altro caso.

L'art. 26 fissa le deroghe alla norma di cui sopra, nel caso in cui il Paese terzo non garantisca una tutela dei dati adeguata ai sensi dell'art. 25, prescrivendo che lo Stato membro può lo stesso autorizzare il trasferimento, sempreché si verifichino determinati casi, tra cui fondamentalmente la manifestazione del consenso al trasferimento da parte della persona interessata, la necessità del trasferimento per ragioni contrattuali che riguardano quest'ultima o in forza di prescrizioni di legge per la salvaguardia di un interesse pubblico rilevante, o della medesima persona interessata. In base al paragrafo 2 dell'articolo 26, se il Paese terzo non garantisce l'adeguatezza del livello di protezione, ma il responsabile del trattamento presenta garanzie sufficienti, ad esempio sottoscrivendo clausole contrattuali appropriate, per quanto riguarda la tutela della vita privata e dei diritti e delle libertà fondamentali delle persone, nonché per l'esercizio dei diritti connessi, lo Stato membro può autorizzare, ancora in deroga all'articolo 25, il trasferimento verso il Paese terzo e deve notificare alla Commissione e agli altri Stati membri le autorizzazioni concesse.

Il Gruppo di lavoro ex art. 29, che ha tra i propri compiti quello di fornire interpretazioni e pareri al fine di garantire una omogenea applicazione dei principi della direttiva all'interno dell'Unione europea, ha ritenuto che le BCR (Binding Corporate Rules) possano costituire uno strumento di trasferimento di dati personali verso paesi terzi astrattamente idoneo ad assicurare un livello adeguato di protezione dei diritti degli interessati e, dunque, compatibile con la disciplina dell'art. 26, par. 2[31]. Le BCR sono uno strumento volto a

[31] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Autorizzazione al trasferimento dei dati personali all'estero mediante BCR da parte di Intel corporation Italia SpA* - 21 novembre 2013, in particolare al Preambolo alla autorizzazione.

consentire il trasferimento di dati personali dal territorio dello Stato verso Paesi terzi (extra-UE) tra società appartenenti allo stesso gruppo d'impresa. Si tratta in concreto di una serie di clausole (*rules*) che stabiliscono i principi vincolanti (*binding*), che tutte le società appartenenti ad uno stesso gruppo (*corporate*) sono obbligate a rispettare. Le BCR costituiscono un meccanismo in grado di semplificare gli oneri amministrativi a carico delle società di carattere multinazionale con riferimento ai flussi intra-gruppo di dati personali.

Un altro strumento che rende legalmente possibile il trasferimento, pure in una situazione di protezione inadeguata, è costituito dalle clausole contrattuali tipo. In questo caso è la Commissione (art. 26 paragrafo 4) che a sua volta può autonomamente decidere con la solita immediatezza esecutiva, che la l'incorporazione di clausole contrattuali tipo (nel senso di standard) in un contratto di trasferimento stipulato tra il responsabile del trattamento e l'esportatore, offra garanzie sufficienti ai sensi di cui sopra, nel qual caso gli Stati membri adottano le misure necessarie per conformarsi alla decisione della Commissione. Sinora la Commissione ha adottato quattro decisioni in materia[32].

Si riscontra una disparità di recepimento delle disposizioni degli artt. 25 e 26 nelle normative degli Stati membri, alcune delle quali attribuiscono al responsabile del trattamento l'onere primario della valutazione circa l'adeguatezza del livello di protezione garantito dal destinatario dei dati, prevedendo un controllo piuttosto lasco dei flussi di dati da parte dello Stato o dell'autorità nazionale di controllo. Viceversa, altri Stati membri condizionano ogni trasferimento verso

[32] Le Decisioni della Commissione di liceità del trasferimento in base alle condizioni contrattuali tipo finora sono le seguenti:
1. Decisione 5 febbraio 2010, 2010/87/UE "Clausole contrattuali tipo per il trasferimento di dati personali a incaricati del trattamento in un Paese terzo".
2. Decisione 27 dicembre 2004 "Introduzione di un insieme alternativo di clausole contrattuali tipo per il trasferimento di dati personali a Paesi terzi"
3. Decisione 5 giugno 2001 "Clausole contrattuali tipo per il trasferimento di dati a carattere personale in Paesi terzi"
4. Decisione 27 dicembre 2001 "Clausole contrattuali tipo per il trasferimento di dati personali a incaricati del trattamento residenti in un Paese terzo".

paesi terzi a un'autorizzazione amministrativa che non sembra rispondere allo spirito delle norme del capo IV della direttiva volto a garantire sì una tutela adeguata, ma anche un trasferimento di dati verso paesi terzi senza oneri inutili.

4.1.4.2. *Safe harbor*

Il quadro normativo-regolamentare applicato negli USA in fatto di protezione dei dati personali non è stato riconosciuto dalla Commissione della UE come uno che assicuri una protezione "adeguata". Ciò deriva dal fatto che il suddetto quadro è tradizionalmente fondato su una combinazione di norme specifiche della privacy e di codici di autoregolamentazione, piuttosto che una regolamentazione unitaria e generale in materia di dati personali secondo le linee della Direttiva o le leggi di recepimento dei vari Stati. Nonostante gli USA vantino una solida tradizione culturale in fatto di diritto alla privacy e quindi di *"informational privacy"*, hanno preferito interventi settoriali federali, cui si sono talora affiancati interventi specifici di fonte statuale[33]. Inoltre nel campo soprattutto del commercio, la tutela dei dati, affidata prevalentemente all'autoregolamentazione, si è dimostrata carente, sia per quanto riguarda l'informativa al consumatore, spesso incomprensibile per lui, circa le policies adottate dal fornitore in materia di privacy, sia con riferimento al diritto d'accesso, come ammette la stessa Federal Trade Commission (FTC) fautrice del principio "*notice and choice model*" basato sostanzialmente sul consenso implicito (regime dell'*opt-out*[34]), con riflessi inevitabilmente negativi sulla sicurezza dei dati[35].

Al fine di colmare questo *gap* tra regolamentazione della privacy nel campo dei dati personali in USA e nell'Unione, particolarmente evidente alla fine degli anni Novanta, il Dipartimento del Commercio degli USA e la Commissione europea hanno sviluppato l'Accordo

[33] Cfr. A. MANTELERO, *Data Protection ed attività d'impresa. Verso dove guardano gli USA?*, in *Dir. Inf. Inf*, n. 3, 2011, 457-476.
[34] *Opt-out*: presunzione di consenso dell'interessato, salvo il caso di affermazione da parte sua del proprio diniego. Invece per *opt-in* s'intende una dichiarazione esplicita di consenso espressa dall'interessato.
[35] ibidem

quadro U.S.-EU Safe Harbor (Approdo sicuro) in materia di tutela dei dati negli scambi commerciali tra mercato comunitario ed imprese statunitensi. Più precisamente il suddetto Accordo è sancito dalla Decisione della Commissione dell'Unione n. 2000/520/CE del 26 luglio 2000, presa ai sensi dell'art. 26(4) della 95/46/CE, che stabilisce l'adeguatezza alla normativa comunitaria (direttiva 95/46/CE) del trattamento dei dati personali di cittadini europei trasferiti negli USA da parte di organizzazioni statunitensi che aderiscono al suddetto Accordo. La suddetta Decisione fornisce una base legale per il trasferimento di dati personali dall'Unione Europea a compagnie stabilite negli USA che siano dotate della certificazione Safe Harbor, ossia che si siano impegnate formalmente all'osservanza dei principi di privacy in essa contemplati.

Il Garante italiano della Privacy, preso atto della suddetta decisione comunitaria, ha concesso l'autorizzazione il 10 ottobre 2001 alle Organizzazioni aventi sede negli USA ed aderenti all'accordo "Safe Harbor", a trasferire i dati personali dall'Italia verso gli USA. L'accordo "Safe Harbor" è una politica di compromesso per il superamento delle difficoltà incontrate dalle compagnie USA che operano sul mercato comunitario ad attenersi alle norme di protezione dei dati personali dei cittadini europei verso i quali sono fornitori di beni/servizi, fissate dalla direttiva di cui sopra, dal momento che esse risultano più stringenti della normativa e delle procedure attualmente vigenti negli USA[36]. Il suddetto accordo richiede che le compagnie statunitensi che sono abilitate a sottoscriverlo[37] secondo quanto prevede la legislazione Americana e che desiderano aderirvi, si

[36] Gli USA adottano un approccio settoriale basato su di un mix di norme giuridiche, regolamentazione ed autoregolamentazione. L'Unione Europea, invece, si basa su di una legislazione esauriente, che richiede, tra l'altro, la creazione di Autorità di tutela dei dati indipendenti, registrazione dei database presso dette Autorità e in alcuni casi una loro preventiva autorizzazione prima che il trattamento dei dati possa aver luogo.

[37] Solo le organizzazioni statunitensi soggette alla giurisdizione del Federal Trade Commission (FTC) o quelle soggette alla giurisdizione del Department of Transportation (DoT), tra cui compagnie aeree statunitensi, possono partecipare al programma Safe Harbor. Le organizzazioni generalmente non soggette alla giurisdizione FTC includono alcune istituzioni finanziarie (ad esempio banche), gestori di TLC, associazioni , organizzazioni no-profit.

impegnino, sottoscrivendo una procedura di autocertificazione, al rispetto di 7 principi in materia di trattamento dei dati personali, da applicare in conformità agli orientamenti forniti da talune FAQ, che fanno parte integrante della succitata Decisione. I suddetti principi impongono alle compagnie di:

- informare gli interessati circa le finalità della raccolta di dati atti ad identificarli, le modalità di contatto per la ricezione di eventuali quesiti o reclami espressi dagli stessi e chi siano i terzi ai quali vengono rivelati questi dati informativi (I principio, di notifica).
- di consentire agli interessati di esprimere il rifiuto (modalità di scelta *opt out*) che i loro dati – non sensibili – siano trasmessi a terzi o siano usati in modo incompatibile con lo scopo per il quale furono raccolti o con quello successivamente autorizzato (II principio, di scelta).
- di chiedere il consenso degli interessati circa la trasmissione dei dati ad un terzo nell'osservanza dei primi due principi (III principio, di trasferimento successivo).
- di garantire la *security*, ossia la protezione da rischi di perdita, abuso, uso non autorizzato, distruzione dei dati (IV principio, di sicurezza).
- di garantire l'integrità dei dati, ossia l'affidabilità in relazione all'uso previsto e l'accuratezza (V principio, di integrità dei dati).
- di consentire agli interessati di accedere ai dati raccolti, di richiederne la modifica se inaccurati o la cancellazione (VI principio, di accesso).
- infine di predisporre i mezzi atti a garantire l'osservanza dei principi Safe Harbor e la possibilità di ricorso degli interessati i cui legittimi interessi siano stati lesi da una loro violazione (VII principio, delle garanzie di applicazione, ossia "*Enforcement Principle*").

L'impresa che aderisce all'Accordo Safe Harbor deve inviare annualmente una autocertificazione al Dipartimento del Commercio USA in cui dichiara di ottemperare alle clausole previste da questo Accordo traducentisi nei principi suesposti. Inoltre deve anche specificare nel suo statement della policy della privacy, riportato sul proprio sito web, che aderisce all'Accordo in parola. Ad esempio, sul

proprio sito, la Microsoft, in veste di Cloud provider, riporta le condizioni della privacy alle quali si attiene, ossia il Privacy Term Windows Azure nei termini "*salvo ove diversamente specificato all'interno di un Servizio, le informazioni raccolte da o inviate a Microsoft potranno essere archiviate ed elaborate negli Stati Uniti o in qualsiasi altro Paese in cui siano presenti Microsoft, le sue consociate, le sue filiali o i provider di servizi. Microsoft rispetta la convenzione Safe Harbor stabilita dal Ministero del Commercio degli Stati Uniti relativamente alla raccolta, al trattamento e alla detenzione di dati di utenti dei Paesi dell'Unione europea, dell'Area Economica Europea e in Svizzera"*.

Le organizzazioni devono inoltre rendere note pubblicamente le loro politiche in materia di riservatezza e sono sottoposte all'autorità della Commissione federale per il commercio (FTC) ai sensi della sezione 5 del Federal Trade Commission Act, che vieta attività o pratiche sleali o ingannevoli in materia commerciale o collegata al commercio, oppure di altri organismi istituiti con legge in grado di assicurare efficacemente il rispetto dei principi applicati in conformità alle FAQ. Affinché le organizzazioni che aderiscono ai principi ed alle FAQ possano essere riconosciute dalle parti interessate, quali le persone che sono oggetto dei dati, gli esportatori di dati e le autorità per la protezione dei dati, il Dipartimento del commercio degli Stati Uniti, o l'ente da esso designato, deve assumersi il compito di compilare e rendere disponibile al pubblico un elenco delle organizzazioni che autocertificano la loro adesione ai principi applicati in conformità alle FAQ e sono sottoposte all'autorità di almeno uno degli enti governativi di cui all'allegato VII della presente decisione.

Considerato quanto sopra detto, si può confermare la convergenza dei principi "Safe Harbor" alle disposizioni normative EU in materia di Privacy, pur dovendo riconoscere che il livello di garanzia della protezione dei dati da essi offerto è necessariamente minore di quello derivante dall'osservanza della direttiva comunitaria. Ciò in quanto detti principi sono frutto di una negoziazione, -rispecchiata nella Decisione della Commissione europea 2000/520/CE del 26 luglio 2000-, in cui il peso della controparte statunitense è stato evidentemente rilevante. Pertanto, il fatto che un Cloud Provider sia

fornito di una certificazione "Safe Harbor", se per un verso renderebbe più sicuro l'affidamento di dati personali ad soggetto terzo, proprio per il fatto che egli dispone di risorse hardware e software distribuite in remoto e virtualizzate in Rete per la conservazione e la trasmissione dei dati personali all'estero, in questo caso verso l'America, dall'altro verso non risolve tutti i problemi attinenti alla sicurezza dei dati, specialmente quando si richiedono servizi ICT *as service*. Ciò per varie ragioni, tra cui la non elevata affidabilità in termini di riservatezza oltreoceano e la discussa validità della suddetta certificazione per il trasferimento di dati in Paesi diversi dagli USA, una questione alla quale non sembra sia stato messo finora un punto fermo, di cui si parlerà diffusamente nel punto successivo.
Le stesse Autorità di controllo europee nutrono qualche dubbio circa l'adeguatezza alla normativa comunitaria dei certificati di cui sopra. Si segnala a tale riguardo che l´Autorità Garante tedesca ha stabilito – con una delibera del 18 giugno 2010 – che i principi sanciti dal Safe Harbor non sarebbero idonei ad offrire adeguate garanzie di protezione dei dati nel contesto dei servizi Cloud.

4.1.4.3. Clausole contrattuali tipo (standard).

La Decisione della Commissione dell'UE 2010/87/UE del 5 febbraio 2010, che abroga e sostituisce una precedente Decisione 2002/16/CE sulla medesima materia, si applica al trasferimento dei dati personali effettuato da responsabili del trattamento stabiliti nell'UE (esportatori dei dati) a destinatari che lo siano al di fuori dell'UE (importatori di dati) – in un Paese la cui normativa sulla privacy a norma della Direttiva 95/46/CE sia 'inadeguata' – che agiscano esclusivamente in veste di incaricati del trattamento. Essa fissa clausole contrattuali tipo alle quali riconosce l'adeguatezza della tutela nei riguardi dei dati personali trattati e che gli Stati membri devono accettare come garanzie sufficienti, specificando che dette clausole indicano le misure tecniche ed organizzative di sicurezza da riportare nel contratto, necessarie affinché, tenuto conto della normativa sulla protezione dei dati, delle più recenti tecnologie e dei costi di attuazione, siano garantiti i diritti e le libertà fondamentali della persona in tema di privacy e quindi la sicurezza dei dati

personali in tutti i suoi aspetti, ossia il mantenimento dei dati contro ogni distruzione accidentale od illecita, l'integrità, la protezione da diffusione ed accesso non autorizzato e così via. E' opportuno, secondo la suddetta Decisione, che nel contratto siano presenti anche clausole standard sul subcontratto eventualmente stipulato da incaricati del trattamento (sub-incaricati) stabiliti nei Paesi terzi (importatori di dati) con altri incaricati del trattamento (sub-incaricati) ivi stabiliti. La Decisione lascia agli Stati membri la facoltà di concedere autorizzazioni, indipendentemente da quanto in essa previsto, al trasferimento internazionale dei dati in base a disposizioni nazionali adottate in attuazione dell'art. 26(2) della Direttiva 95/46/CE. Analizzando in maggior dettaglio il testo del documento in esame, si rileva innanzitutto (V. art. 4) che la stipula delle clausole contrattuali tipo non esenta le Autorità competenti dello Stato membro dal vietare o sospendere il flusso di dati verso un Paese terzo in determinate circostanze, quando ad esempio la legge di questo Paese applicabile all'importatore o al subincaricato comporti deroghe alla normativa sulla protezione dei dati oppure non vengono rispettate le clausole contrattuali. L'articolo 5 dispone una durata triennale della Decisione, al cui termine la Commissione procederà a valutare nuovamente l'adeguatezza delle clausole contrattuali tipo. Queste ultime figurano nell'Allegato alla Decisione, di cui si illustrano di seguito quelle più significative.

La clausola tipo n. 3, definita clausola del terzo beneficiario, definisce i casi in cui l'interessato può far valere i suoi diritti nei confronti dell'esportatore, per quanto riguarda ad esempio gli obblighi in nome dell'interessato che questi è tenuto ad assolvere ai sensi della clausola tipo n. 4 o a far assolvere all'importatore secondo la clausola n.5, nonché dell'importatore con riferimento ai suoi obblighi secondo la clausola n. 5, quando l'esportatore sia scomparso di fatto o abbia giuridicamente cessato di esistere senza trasferire i suoi obblighi ad un successore, ed infine nei confronti del sub-incaricato, quando la cessazione di ruolo riguardi sia l'esportatore che l'importatore. La medesima casistica ai sensi sempre della clausola 3 si applica anche ai fini dell'ottenimento da parte dell'interessato del risarcimento di un danno sofferto per violazione degli obblighi di protezione dei propri dati.

La clausola tipo n. 4 fissa i vari obblighi in capo all'esportatore, ossia al responsabile del trattamento, tra cui fondamentalmente:

- svolgimento del trattamento, compreso il trasferimento, dei dati personali conforme alla normativa sulla protezione dei dati vigente nel Paese in cui è stabilito.
- prescrizioni all'importatore circa il rispetto della suddetta normativa
- sufficienti garanzie richieste all'importatore circa le misure tecniche ed organizzative di sicurezza da lui poste in atto.
- garanzie sull'adeguatezza delle suddette misure tenuto conto della più recente tecnologia e dei costi di attuazione.
- impegno ad informare gli interessati che i dati che li riguardano, nel caso essi siano compresi nelle categorie di dati oggetto del trasferimento o categorie particolari elencate nell'Appendice 1 della Decisione, potrebbero essere oggetto di trasferimento in un Paese terzo che non garantisce una protezione adeguata ai sensi della Direttiva 95/46/CE. A sua volta l'importatore è obbligato ai sensi della clausola n.5 a:
- trattare i dati personali esclusivamente per conto e secondo le istruzioni dell'esportatore, nonché a norma delle clausole tipo.
- comunicare all'esportatore qualsiasi modificazione della normativa a lui applicabile, ossia l'insieme delle norme vincolanti della legislazione nazionale, che prevedono, tra l'altro, obblighi di informazione in materia fiscale o contro il riciclaggio del capitale, che possa pregiudicare le garanzie e gli obblighi cui è tenuto in forza delle clausole tipo. Nel caso la suddetta modificazione abbia luogo, l'esportatore ha facoltà di sospendere il trasferimento e/o risolvere il contratto.
- avere applicato le misure tecniche ed organizzative di sicurezza sottoscritte, in conformità a quanto previsto dalle clausole 4 e 5, nell'Appendice 2 della Decisione, che come la n. 1 è parte integrante delle clausole contrattuali, prima di procedere al trattamento dei dati personali trasferiti.
- comunicare prontamente all'esportatore:

a) qualunque richiesta vincolante presentata da un'autorità giudiziaria o di polizia ai fini della comunicazione dei dati personali, salvo il divieto imposto da norme specifiche.
b) qualsiasi accesso accidentale o non autorizzato ai dati
c) qualunque richiesta ricevuta dall'interessato direttamente cui non abbia risposto nonostante vi sia obbligato.

- conformarsi al parere dell'Autorità di controllo per quanto riguarda il trattamento dei dati trasferiti.
- sottoporre i propri impianti di trattamento dei dati al controllo dell'esportatore su sua richiesta o di un organo ispettivo composto da soggetti indipendenti in possesso delle necessarie qualificazioni professionali, vincolati da obblighi di riservatezza e selezionati dall'esportatore, eventualmente di concerto con l'autorità di controllo.

La clausola tipo n. 9 prevede che tutte le clausole tipo sono soggette alla normativa di legge dello Stato membro in cui è stabilito l'esportatore, mentre quella n. 11 (subcontratto) stabilisce che l'importatore rimane pienamente responsabile nei confronti dell'esportatore dell'inadempimento da parte del sub-incaricato degli obblighi di protezione dei dati previsti dall'accordo scritto.

4.1.5. Riflessi della direttiva 95/46/CE sul Cloud Computing.

Il *Cloud Computing* coinvolge una serie di diversi operatori, ognuno dei quali ha specifici obblighi da valutare attentamente, perché non sempre di facile attribuzione, imposti dall'attuale legislazione in materia di protezione dei dati[38]. In linea di principio il cliente Cloud determinando la finalità ultima del trattamento e decidendo in merito all'esternalizzazione (con ciò delegando ad un *outsourcee* le attività di trattamento), riveste il ruolo di responsabile del trattamento dei dati, secondo la definizione che ne dà la direttiva 95/46/CE, ed è tenuto, pertanto, a osservare e a far osservare tutte le norme sulla tutela dei dati, essendo direttamente responsabile di ogni violazione dei requisiti regolatori applicabili al servizio fornito dal suo provider. Pertanto il rispetto di tutti gli adempimenti amministrativi – controlli preliminari,

[38] GRUPPO DI LAVORO EX ART. 29 Opinione 1/2010, cit.

autorizzazioni, notifiche all'autorità di tutela dei dati – previsti dagli ordinamenti nazionali sulla privacy di recepimento della direttiva 95/46/CE è vincolante per il cliente Cloud. A sua volta, il fornitore dei servizi Cloud incaricato per il trattamento ha facoltà di scelta dei metodi e delle misure tecniche e organizzative da impiegare al fine del conseguimento degli scopi del responsabile del trattamento e quindi risponde esclusivamente al cliente Cloud per ogni inadempienza che li pregiudica**.** In altri termini, elaborando dati personali per conto del responsabile del trattamento, è , secondo la direttiva 95/46/CE, da considerare alla stregua di un incaricato del trattamento. Nell'ambito del Cloud Computing, i criteri dell'articolo 4 della direttiva 95/46/CE per stabilire la legislazione applicabile alla tutela dei dati considerano, con riferimento alla dislocazione dello stabilimento del responsabile dei dati, due casi; il primo che la ipotizza in una o più sedi all'interno del SEE, il secondo al di fuori del SEE ma con l'utilizzo di impianti situati all'interno del SEE per il trattamento dei dati personali.

Nel primo caso è determinante, mentre la tipologia del modello di servizio *Cloud* è irrilevante, l'ubicazione della sede e delle attività svolte dal responsabile del trattamento, ossia in questo modello tipico di assegnazione di ruoli si applica la normativa del Paese dov'è stabilito il responsabile del trattamento -o dei singoli Paesi in cui figura un suo stabilimento-, che appalta servizi di *Cloud Computing* e che è il controller, piuttosto che quella dei Paesi dove sono situati i fornitori di tali servizi.

Nel secondo caso, in cui un cliente *Cloud* è stabilito al di fuori del SEE ma incarica un fornitore *Cloud* con sede nel SEE, non si applica il diritto del Paese nel quale è stabilito il cliente Cloud, esportando il fornitore la legislazione sulla protezione dei dati del proprio Paese in quello del cliente.

L'individuazione del diritto applicabile così come dei compiti e delle responsabilità spettanti al singolo soggetto presuppongono una distinzione dei ruoli di controller e di processor chiara ed evidente. Ma, a seconda delle circostanze reali, ci possono essere casi in cui un fornitore di servizi *Cloud* di fatto condivide con il cliente la responsabilità del rispetto delle norme di tutela dei dati, o addirittura può essere considerato responsabile a pieno titolo. Ciò si verifica, ad esempio, nel caso in cui il fornitore procede al trattamento di dati per

scopi propri. In generale, la valutazione della qualificazione giuridica dei soggetti coinvolti nel flusso dei dati, cliente e provider Cloud, non va ancorata tanto a norme contrattuali che definiscano i rapporti intersoggettivi tra le due figure, per effetto di norme contrattuali, e tanto meno a vincoli economici tra loro sussistenti, quanto piuttosto alle differenti posizioni da loro assunte in concreto, singolarmente o congiuntamente in relazione alla gestione dei dati ed ai gradi di autonomia detenuti da ciascuno nell'assolvimento delle relative funzioni ed attività. La finalità è di attribuire correttamente e chiaramente la posizione giuridica a ciascun soggetto, in modo da garantire che congiuntamente, ognuno nel proprio ambito di competenza, garantisca la protezione dei dati, senza che si generino così "conflitti di competenza negativa" o si producano delle falle nel sistema tecnico ed organizzativo di trattamento dei dati.

Il documento del Gruppo di Lavoro ex art. 29 del 1° luglio 2012, Opinion on "Cloud Computing" considera il caso classico e più comune in cui il cliente del Cloud è il responsabile del trattamento (*controller*) ed il *provider* l'incaricato del trattamento (*processor*) e fornisce molti chiarimenti in relazione ad aspetti di security e di rischi associati al trattamento dei dati, che determinano in un certo modo le funzioni e le procedure di controllo a livello tecnico ed organizzativo, che il cliente è tenuto ad esercitare e a mettere in atto per adempiere ai compiti, il cui assolvimento è soggetto in genere a non poche criticità, che il ruolo di responsabile di ogni attentato alla tutela dei dati per le cause più varie gli assegna "in toto". Le difficoltà principali che il cliente Cloud si trova ad affrontare nel quotidiano onorare il suo ruolo, sono ascrivibili primariamente, per ragioni soprattutto tecniche, a mancanza di controllo per quanto attiene a disponibilità, integrità, riservatezza dei dati, capacità di intervento sulla *outsourcing chain* e sul rispetto dell'esercizio dei diritti da parte del soggetto interessato ed infine sull'ottenimento dell'isolamento fisico e/o logico dei propri dati da quelli di altri clienti del medesimo fornitore dei dati e secondariamente a mancanza di informazioni che il cliente può a ragione lamentare in relazione al funzionamento della catena di esternalizzazione costituita da molteplici incaricati al trattamento e subcontraenti ed alle modalità di processamento dei dati dislocati geograficamente in diversi Paesi in ambito EEA o al di fuori. E'

necessario allora che i rapporti tra cliente e provider siano regolati da un contratto[39] in cui oltre alle misure di sicurezza a carico del fornitore Cloud, derivanti da una preventiva analisi dei rischi, siano inserite opportune clausole di salvaguardia delle funzioni di controllo sul trattamento dei dati e che risponda agli effettivi bisogni del cliente declinati in termini di security informatica, analisi dei rischi a questa correlati, continuità di servizio, trasparenza nell'operatività del fornitore Cloud, soprattutto per quanto concerne l'ubicazione dei server in cui sono archiviati i dati del cliente. Il contratto deve anche contenere gli accordi sui livelli di servizio garantiti (SLA)[40], che dovrebbero essere oggettivi e misurabili. Nell'attuale scenario del *Cloud Computing*, i clienti di servizi di *Cloud Computing* potrebbero non avere margine di manovra nel negoziare i termini contrattuali dell'uso dei servizi *Cloud,* che in molti casi sono caratterizzati da offerte standardizzate.

Un'altra criticità, collegata alla precedente e messa in rilievo dal Gruppo di lavoro ex art. 29 nel summenzionato documento è il fatto che il cliente del Cloud ha meno potere contrattuale del provider, dal che deriva di solito che un grosso fornitore di servizi induca il responsabile del trattamento ad accettare clausole e condizioni non conformi alla normativa sulla protezione dei dati. E' fondamentale allora che il responsabile del trattamento scelga un fornitore *Cloud* che garantisca l'osservanza della normativa in materia di protezione dei dati.

Infine, per quanto riguarda il trasferimento dei dati al di fuori dell'ambito EEA, si fa osservare che i casi di deroga dall'art. 25, ossia di autorizzazione al trasferimento nonostante il Paese terzo non garantisca un livello di protezione adeguata, non si verificano generalmente in ambiente Cloud, stante l'instabile ubicazione dei dati all'interno della rete del fornitore ed il loro trasferimento frequente da

[39]come previsto, peraltro, dall'articolo 17, paragrafo 3, della direttiva 95/46/CE, che stabilisce che la relazione tra responsabile e incaricato del trattamento sia disciplinata da un contratto o un altro atto giuridico vincolante.

[40]Gli SLA, ossia Service Level Agreements, sono accordi tra le parti che regolamentano i livelli dei servizi forniti e costituiscono uno strumento/obbligo contrattuale del fornitore nei riguardi del fruitore di mantenere le prestazioni attese all'interno dei valori prestabiliti.

un Paese all'altro nei relativi dispositivi di trattamento, di cui il soggetto interessato non ha quasi mai conoscenza, ed allora occorre che venga posto in essere un approccio predefinito e sistematico al problema dei flussi dei dati all'estero, facendo ricorso alla Decisione di adeguatezza in ambito UE, tra quelle previste dall'articolo 26, che sia più la più idonea alla situazione in esame. In particolare converrà riferirsi alla Decisione della Commissione dell'Unione n. 2000/520/CE del 26 luglio 2000, che valuta adeguato il livello di protezione dei dati garantito dall'Accordo *Safe Harbor,* in tutti quei casi in cui il Cloud Provider, il cui ruolo è quello del "processor", sia stabilito negli USA, nel quale importi i dati provenienti dall'UE, e sia sottoscrittore di detto Accordo. Ora, secondo il Gruppo ex art. 29[41], il cui parete non è vincolante né per la Commissione, né per gli Stati membri, ma riflette il parere autorevole delle Autorità di tutela dei dati europee, "*la sola autocertificazione di conformità al Safe Harbor può non essere considerata sufficiente […] perché in termini di sicurezza dei dati, il Cloud Computing comporta numerosi rischi specifici, quali la perdita di governance, l'insicurezza o incompletezza della cancellazione dei dati, piste di controllo (audit trail) insufficienti o carenze nell'isolamento, che non sono affrontati in misura sufficiente dai principi Safe Harbor esistenti in materia di sicurezza dei dati".* Il Gruppo ex art. 29 conclude che occorre prevedere garanzie aggiuntive per la sicurezza dei dati, ad esempio mediante la valutazione da parte di terzi dell'adeguatezza dei fornitori Cloud statunitensi con l'impiego di vari sistemi di controllo, standardizzazione e certificazione. Alle osservazioni di cui sopra formulate dal Gruppo summenzionato ha controbattuto l'organismo del Dipartimento del Commercio USA, ossia l'ITA, International Trade Administration in un documento[42] in cui fornisce alcune delucidazioni riguardo al Safe Harbor ed alla sua applicazione nel caso del Cloud Computing. L'ITA argomenta che i principi del Safe Harbor in tema di trasferimento di flussi di dati fuori dagli USA prevedono nella sezione "Onward Transfer" che "*Where*

[41] ARTICLE 29 DATA PROTECTION WORKING PARTY, Opinion 5/2012 *on Cloud Computing* of July 1st, 2012.

[42] U.S. DEPARTMENT OF COMMERCE'S INTERNATIONAL TRADE ADMINISTRATION (ITA), "*Clarifications Regarding the U.S.-EU Safe Harbor Framework and Cloud Computing*", april 2013.

an organization wishes to transfer information to a third party that is acting as an agent [...] [ossia agisce come mero incaricato del trattamento] *it may do so if it first either ascertains* [si accerta] *that the third party subscribes to the Principles or is subject to the Directive or another adequacy finding* [clausole tipo, clausole BCR] *or enters into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant Principles* [del Safe Harbor]".

Un modo per adempiere alla succitata norma, la quale non chiama in causa l'esportatore di dati, ossia il cliente Cloud europeo, consiste per il provider aderente al Safe Harbor, nel caso in cui esporti a sua volta i dati dagli USA in un altro Paese che non offra un livello di protezione adeguata, nel condizionare il trasferimento all'osservanza da parte dell'importatore di detto Paese (che si configura quindi come una terza parte) dei principi del Safe Harbor sulla base di un impegno da lui a tal riguardo sottoscritto. Del resto, aggiunge il suddetto organismo, non è giusto che requisiti addizionali, come vorrebbe il Gruppo ex art. 29, siano imposti esclusivamente ai provider USA che processano i dati trasferiti dall'UE negli USA, per il semplice fatto che essi soddisfano i requisiti di adeguatezza in virtù della certificazione Safe Harbor, perché le medesime regole basilari per il trasferimento internazionali di dati si applicano a tutti i Cloud provider, indipendentemente dal fatto che essi siano stabiliti nell'Unione o in un Paese che garantisca misure adeguate di protezione dei dati, o sottoscrivano clausole contrattuali tipo o clausole BCR od infine soddisfi i principi del Safe Harbor con riferimento a Paesi "inadeguati".

Quando, invece, il Cloud provider non sia stabilito negli USA, non è possibile impiegare l'Accordo Safe Harbor e sarà opportuno allora riferirsi alla Decisione della Commissione 2010/87/UE che dispone l'inserimento di clausole contrattuali tipo nel contratto stipulato tra il responsabile del trattamento (nel caso in esame il cliente Cloud dell'UE) e l'incaricato (ossia qui il fornitore statunitense).

5. Evoluzione della normativa comunitaria sulla protezione dei dati personali

Il 25 gennaio 2012 la Commissione europea ha proposto una riforma globale della normativa UE del 1995 in materia di protezione dei dati nell'intento di rafforzare i diritti della privacy on line e stimolare l'economia digitale europea, in considerazione anche del fatto i 28 Stati membri hanno attuato la normativa del 1995 diversamente, con conseguenti divergenze sul piano dell'effettiva applicazione. Le proposte della Commissione aggiornano e modernizzano i principi sanciti dalla direttiva del 1995 sulla protezione dei dati personali e sono contenute nei seguenti documenti:

- una comunicazione strategica in cui la Commissione fissa gli obiettivi e due proposte legislative:
- un regolamento che istituisce un quadro generale dell'Unione per la protezione dei dati e
- una direttiva sulla protezione delle persone fisiche con riguardo al trattamento dei dati a fini di prevenzione, indagine, accertamento o perseguimento dei reati e nell'ambito delle connesse attività giudiziarie.

5.1. Proposta di Regolamento generale sulla protezione dei dati del Parlamento europeo e del Consiglio.

5.1.1. Confronto con la normativa base vigente.

Alla luce dell'importanza della protezione dei dati personali nel quadro degli obiettivi stabiliti dall'Agenda digitale europea, con la Comunicazione COM(2012) 11 final del 25 gennaio 2012 la Commissione europea ha adottato una proposta di regolamento generale sulla protezione dei dati personali, che disegna un nuovo quadro giuridico per il loro trattamento – pur mantenendo in una certa misura l'impianto normativo dell'abroganda vigente normativa 95/46/CE – per la cui approvazione è in corso il previsto iter legislativo, che comporterà l'intervento congiunto di Parlamento europeo e Consiglio UE in base alla procedura detta di 'codecisione' (ora definita dal Trattato di Lisbona "procedura legislativa").

Il 22 ottobre 2013 la Commissione LIBE (Civil Liberties, Justice and Home Affairs) del Parlamento europeo ha approvato, apportando modifiche in una certa misura non sostanziali, il documento suddetto che ora passa all'esame del Consiglio dei Ministri, la seconda Camera dell'UE[43]. Con la Direttiva 95/46/CE se il responsabile del trattamento ha sede in vari Stati membri e il trattamento di dati rientra nelle attività svolte in tali paesi, il diritto applicabile sarà quello di ciascuno degli Stati membri in cui viene effettuato il trattamento, mentre secondo la Proposta di Regolamento tale diritto è costituito dalle norme in esso contenute, che varranno uniformemente in tutti e 28 gli Stati membri. A parere degli esperti le nuove regole della privacy dovrebbero entrare in vigore prima della scadenza naturale del mandato del Parlamento e della Commissione Europea, ossia entro la fine del 2014. Se è vero che lo schema di Regolamento ha non pochi meriti, tra cui quello di estendere l'ambito territoriale di applicazione delle norme di tutela dei dati e di rafforzarne l'*enforcement*, che hanno innescato le reazioni di organismi internazionali OTT (Over the Top) come Google e Faceboox che giudicano il nuovo quadro normativo eccessivamente vincolante, non si può non sottolinearne alcune carenze, tra cui quella di una disciplina apposita per la fornitura di servizi in modalità *Cloud Computing*, che, invece, sarebbe opportuno introdurre[44].

Peraltro occorre riconoscere che il regolamento proposto dalla Commissione affronta alcuni argomenti connessi al Cloud Computing[45]. Al riguardo, meritano rilievo la nozione di titolare e di responsabile e il principio della *accountability* (responsabilità). Per ciò che riguarda il primo argomento, tenuto conto che i fornitori di servizi Cloud spesso non solo determinano i mezzi del trattamento ma

[43] Il 12 marzo 2014 il testo è stato approvato dal Parlamento europeo riunito in assemblea plenaria e per divenire legge dovrà essere approvato dal consiglio dei Ministri.

[44] Confindustria Delegazione di Bruxelles, Lente sull'Europa n. 26, *Data Protection, Proposta di Regolamento*, marzo 2013.

[45] C. COMELLA, *Protezione dei Dati personali e iniziative per lo sviluppo del Cloud Computing in Europa*, Atti del Convegno "Il Cloud Computing nel sistema finanziario. Standard, regolamentazione e controlli, Roma, Banca d'Italia, 28 settembre 2012.

offrono anche prestazioni che interessano in qualche misura le condizioni e le finalità stesse del trattamento, l'articolo 24 unitamente al comma 4 dell'art. 26 dello schema di regolamento introduce una corresponsabilità del trattamento per il fornitore Cloud unitamente al cliente Cloud, dal momento che rafforza gli obblighi e le responsabilità dei processori dei dati. In materia di responsabilità, va segnalato che, rispetto alla direttiva 95/46/CE si passa da un approccio burocratico di notificazione formale dei trattamenti a un regime in cui il titolare deve dar prova di soddisfacimento di tutte le disposizioni previste dal regolamento. titolari stabiliti nell'UE dovranno mantenere documentazione relativa ai trattamenti, eseguire valutazioni di impatto dei trattamenti a rischio, assicurare adeguata protezione dei dati trasferiti all'esterno dell'UE. I Cloud service providers stabiliti in UE saranno sottoposti a questo tipo di misure, che dovrebbero accrescere il livello di protezione dei trattamenti svolti nel territorio dell'Unione.

Una volta entrato in vigore, il Regolamento in esame, in virtù del suo gradimento da parte delle multinazionali per il fatto di costituire un codice normativo unico a livello paneuropeo nel campo della protezione dei dati anche se nel contempo limita fortemente i margini di flessibilità rispetto ai dettami comunitari, riaccenderà la competizione tra la normativa comunitaria e quella corrispondente in vigore negli USA in termini di espansione del rispettivo modello proposto, dopo che le linee guida statunitensi[46] hanno cercato di affermare la leadership degli USA attraverso quello che è sembrato sia stato un riavvicinamento al modello regolamentare europeo dettato dalla direttiva 95/46/CE. A questo riguardo si fa notare come da alcuni anni l'amministrazione statunitense stia già provvedendo a definire, come primo passo, attraverso una serie di atti legislativi, un quadro di tutela dei dati nelle applicazioni commerciali basato sulla co-regolamentazione[47], ossia su di una regolamentazione statuale, che definisce un insieme di principi comuni di base ("*notice, choice, access, security"*), i cosiddetti FIPPS ("*Far Information Practice*

[46] FEDERAL TRADE COMMISSION, *Protecting Consumer Privacy in an Era of Rapid Change. A proposed Framework for Businesses and Policymakers. Preliminary FTC Staff Report,* December 2010.
[47] *ibidem*

Principles"), coniugata con l'autoregolamentazione, ossia con codici di condotta volontari elaborati dai singoli tipi di settori commerciali.

Tornando allo schema di Regolamento comunitario, si fa presente che i regolamenti UE sono immediatamente "self-executing", non dovendo essere recepiti da parte degli Stati membri, a differenza delle direttive e, pertanto, essi possono garantire una maggiore armonizzazione a livello dell'intera UE. Di seguito viene svolta una disamina in maggior dettaglio dei punti salienti del Regolamento, che sostituisce ed abroga la Direttiva 95/46/CE (V. art. 88).

L'art. 3 comma 2 dello schema di Regolamento, rispetto alla Direttiva 95/46/CE, per quanto concerne la *applicable law*, fissa il principio, confermato dal Comitato LIBE del Parlamento il 22 ottobre 2013, che le imprese non europee, nella veste di responsabili o di incaricati[48] del trattamento dei dati di cittadini dell'Unione, quando le loro attività sono rivolte all'offerta a questi ultimi di beni/servizi - indipendentemente dal fatto che sia richiesto un prezzo per la loro fornitura-, o sono volte al monitoraggio di tali soggetti dei dati (es., Internet tracking), devono osservare tutte le norme ed i livelli di protezione fissate da detto Regolamento. L'introduzione di questa norma, come dichiarato dalla stessa Commissione UE[49], è quella di creare un *level-playing field*, attraverso la fissazione delle medesime norme di tutela della privacy dei dati, sia per l'industria digitale europea che per quelle omologhe stabilite in ogni altra parte del mondo che, offrendo beni e servizi nel territorio dell'Unione, sono suoi competitor. Il suddetto comma del Regolamento estende, infatti, l'ampiezza territoriale dell'applicazione del diritto UE al di fuori del territorio comunitario ove sia ubicato lo stabilimento principale

[48] L'art. 3 comma 2 del Regolamento a seguito del voto del Parlamento europeo recita "*This Regulation applies to the processing of personal data of data subjects in the Union by a controller or processor [*"or processor*"*: non figurava nella Proposta originaria di Regolamento] *not established in the Union, where the processing activities are related to:*
(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union [irrespective of whether a payment of the data subject is required*"*: non figurava nella Proposta originaria di Regolamento]*; or (b) the monitoring of such data subjects.*

[49] EUROPEAN COMMISSION, MEMO, *LIBE Committee vote backs new EU data protection rules*, 22 october 2013.

dell'impresa che li fornisce, e quindi costituisce un principio innovativo rispetto alla normativa attualmente in vigore, mirando a rafforzare la tutela della protezione dei dati di interessati nell'UE cui vengono offerti beni e servizi anche per i dati personali trattati all'estero dalle compagnie, sempreché esse se ne avvalgono nell'operare nel mercato comunitario. Infatti, l'articolo 4, paragrafo 1, lettera c)[50] della Direttiva 95/46/CE estende parimente l'applicazione del diritto comunitario al trattamento dei dati personali da parte di un responsabile del trattamento che non sia stabilito nel SEE, ma limitatamente al caso in cui egli faccia ricorso a strumenti automatizzati o non automatizzati situati nel territorio dello Stato membro, che non siano peraltro utilizzati ai soli fini di transito. Nella proposta di regolamento (art. 3), invece, l'estensione dell'applicazione del diritto comunitario è indipendente dall'ubicazione dei suddetti strumenti ed impegna sia il titolare che l'incaricato del trattamento, ma è vincolata a diverse condizioni di applicabilità, ossia che si tratti di:

- fornitura di beni e servizi a interessati nell'Unione o
- del monitoraggio dell'utente europeo, nel senso anche di attività di profilazione, ossia volte ad analizzare o predire gusti personali, comportamenti e attitudini.

Ciò significa che, sussistendo le condizioni suelencate, valgono per imprese con stabilimento (principale)[51] al di fuori del territorio dell'Unione le medesime regole che è tenuto ad osservare un

[50] L'articolo 4, paragrafo 1, lettera c) stabilisce che la legislazione di uno Stato è applicabile quando il responsabile del trattamento "*non stabilito nel territorio della Comunità, ricorre, ai fini del trattamento di dati personali, a strumenti, automatizzati o non automatizzati, situati nel territorio di detto Stato membro, a meno che questi non siano utilizzati ai soli fini di transito nel territorio della Comunità europea*".

[51] E' da intendere "stabilimento principale" definito nell'art. 4 del Regolamento come "…*il luogo di stabilimento nell'Unione in cui sono prese le principali decisioni sulle finalità, le condizioni e i mezzi di trattamento di dati personali; se non sono prese decisioni di questo tipo nell'Unione, il luogo in cui sono condotte le principali attività di trattamento nell'ambito delle attività di uno stabilimento di un responsabile del trattamento nell'Unione. Con riferimento all'incaricato del trattamento, per "stabilimento principale" si intende il luogo in cui ha sede la sua amministrazione centrale nell'Unione*".

responsabile del trattamento od un incaricato del trattamento stabilito nell'Unione secondo quanto fissa il comma 1 del suddetto articolo, anche se il trattamento avviene in realtà su server remoti fuori dal territorio dell'Unione, come può accadere nel caso del modello di business "as a service" del Cloud Computing, di cui fruisca come cliente un'impresa europea. Pertanto, ai sensi del Regolamento ma non della Direttiva 95/46/CE- il fornitore di servizi Cloud, sia esso considerato controller o processor, che allochi in server remoti, al di fuori dello spazio SEE, i dati di cittadini europei cui il cliente Cloud fornisce servizi o di cui controlla il comportamento, è tenuto ad osservare le norme inerenti la security dei dati previste da detto Regolamento. Ma non solo queste, bensì anche quelle relative al trasferimento dei flussi transfrontalieri in un Paese terzo al di fuori del territorio comunitario.

Con le nuove regole l'Europa ribadisce con forza l'importanza della propria normativa prevedendone l'applicazione anche al di fuori del proprio territorio a tutela dei propri cittadini, quando il trattamento dei dati riguarda l'offerta agli stessi di beni e servizi o il controllo dei loro comportamenti (art. 3, 2 della proposta di Regolamento). È evidente, in questa disposizione, la volontà di proteggere i cittadini europei soprattutto rispetto agli aspetti più significativi dei *social network*, dell'uso di *cookies* effettuati a fini di profilazione senza il loro consenso e dei sistemi Cloud Computing. Il trasferimento di dati all'estero, già regolamentato negli artt. 25 e 26 della Direttiva 95/46/CE, sta divenendo un fenomeno in forte ascesa in ragione dell'espansione del commercio internazionale e della cooperazione internazionale, che pone sempre nuove sfide alla protezione dei dati personali se il diritto applicabile non è quello comunitario, bensì quello del paese terzo in cui avviene il trattamento, ossia quando non valgono le condizioni previste dall'art. 3 comma 2 per la sua applicabilità o, quando, pur valendo esse, viene disattesa od elusa la giurisdizione comunitaria e/o l'Autorità di controllo istituita nel paese terzo non svolge correttamente od incisivamente il suo ruolo. Sorgono allora fondate preoccupazioni che venga compromesso il livello di protezione delle persone garantito nell'Unione dal presente Regolamento tutte le volte che abbia luogo il suddetto trasferimento. La proposta di Regolamento, così come la regolamentazione cogente

(Direttiva 95/46/CE), consente i flussi transfrontalieri di dati in altri Paesi solamente se il Paese terzo assicura un adeguato livello di protezione. Nel valutare l'adeguatezza di questo livello la Commissione deve innanzitutto considerare la legislazione in vigore nel Paese terzo, incluse perplessità "*sulla sicurezza pubblica, la difesa, la sicurezza nazionale* e la legge criminale, la garanzia *di diritti effettivi ed azionabili, tra cui il diritto degli interessati a un ricorso effettivo in sede amministrativa e giudiziaria, in particolare quelli che risiedono nell'Unione e i cui dati personali sono oggetto di trasferimento*" (art. 41(2) (a) della Proposta di Regolamento). Deve altresì valutare l'esistenza e l'effettivo funzionamento di una o più autorità di controllo indipendenti nel paese terzo, incaricate di garantire il rispetto delle norme di protezione dei dati, fornire assistenza agli interessati in merito all'esercizio dei loro diritti e cooperare con le autorità di controllo dell'Unione e degli Stati membri, ed infine deve considerare gli impegni internazionali assunti dal paese terzo o dall'organizzazione internazionale in questione (art. 41(2) (b)(c)). In quest'ottica, anche la presenza di organi pubblici investigativi "invasivi" e la mancanza di adeguate garanzie al soggetto dei dati assume rilevanza nella decisione di limitare i flussi di dati transfrontalieri tra "*subsidiaries*" e holding o tra compagnie. Lo schema di Regolamento ribadisce quanto già previsto dalla Direttiva 95/46/CE, ossia la liceità di queste allocazioni di dati in un paese extracomunitario se la Commissione decide che in esso venga garantito un livello adeguato di protezione dei dati o al suo interno o tramite un'organizzazione internazionale che assicuri la certezza del diritto e l'uniformità di applicazione delle norme in tutta l'Unione.

Con decisioni successive nel corso dei primi anni del 2000, in ottemperanza delle disposizioni previste dagli artt. 25 e 26 della Direttiva 95/46/CE, come già richiamato in precedenti note in calce, la Commissione UE ha stabilito che le normative sulla tutela dei dati vigenti in Paesi quali Andorra, Argentina, Australia, Canada, Svizzera, le Isole Faeroe, Guernsey, lo Stato di Israele, l'Isola di Man, Jersey e che i principî Safe Harbor fissati dal US Department of Commerce's Safe per il trasferimento di dati personali di cittadini dell'Unione negli USA forniscono protezione adeguata ed ha definito clausole contrattuali tipo (ossia standard) per il trasferimento di dati in

Paesi al di fuori dell'UE (soprattutto decisioni del 2004 e 2010). L'effetto di tali decisioni è la liceità del trasferimento di dati personali dai 28 Paesi dell'UE e dai tre Paesi membri di EEA (Norvegia, Liechtenstein ed Islanda) in un Paese terzo senza che sia necessaria un'ulteriore salvaguardia. Ora, il comma 2 dell'art. 3 del Regolamento, nei casi in cui valgano le condizioni da esso previsto per la sua applicabilità, rende superate se non addirittura confliggenti con esso le suddette Decisioni, accordando detto comma una protezione dei dati dei cittadini europei ben maggiore del livello minimo giudicato adeguato dalla Commissione, garantito dai suddetti Paesi nei quali i dati personali vengono trasferiti, essendo essa nella sua interezza quella sancita dal diritto comunitario. Con riferimento, ad esempio, ai flussi di dati dall'Unione Europea agli USA, il suddetto articolo impatta profondamente ed in maniera estesa sull'Accordo di Safe Harbour che li regola, dovendosi applicare, allo stato attuale dell'iter normativo del Regolamento, alle imprese statunitensi che offrono servizi nel mercato interno dell'Unione e che lo abbiano sottoscritto. Si tratta di compagnie che offrono servizi su Internet o che operano nei campi più disparati, dai servizi di informazione ed informatici a quelli farmaceutici, del turismo, della salute e di carte di credito (es. MasterCard) o che sono controllate da società europee come Nokia e Bayer. Esse rappresentano ben il 49% delle 3246 compagnie dotate di certificazione ancora valida Safe Harbour alla data del 13 settembre 2013, essendo il 51% di queste ultime costituite da società che effettuano il trattamento di dati di impiegati in Europa società dopo aver trasferito i relativi flussi informativi negli USA, secondo finalità dettate dalla gestione delle risorse umane[52].

Ma, nonostante l'innovazione profonda che lo schema di Regolamento apporta all'attuale disciplina dei trasferimenti di dati al di fuori del territorio comunitario, sorprendentemente lo schema di Regolamento (nella versione del 25 gennaio) nel considerando 79 "*lascia impregiudicate le disposizioni degli accordi internazionali conclusi tra l'Unione ed i paesi terzi che disciplinano il trasferimento*

[52] European Commission, COM(2013) 847, *Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU citizens and Companies Established in the EU*, 2013.

dei dati personali" e, pur essendo abrogata la direttiva 95/46/CE ai sensi del considerando 134 e soprattutto dell'art. 88, ribadisce il mantenimento in vigore delle decisioni adottate dalla Commissione e delle autorizzazioni delle Autorità di controllo basate su detta Direttiva (V. considerando 134[53]). Non si può, pertanto, non convenire con l'indicazione espressa dal Garante Europeo della Protezione dei Dati (GEPD)[54] di cancellare il considerando 79 e di inserire una clausola transitoria che preveda la revisione dei succitati accordi internazionali, tra cui soprattutto il Safe Harbor, entro un determinato periodo di tempo per allinearli al regolamento. La grave incongruenza rilevata è stata sanata successivamente con l'accoglimento di alcuni emendamenti presentati dal Parlamento europeo, in linea con le indicazioni del GEPD. Difatti, nel testo emendato del Regolamento (approvato dal Libe il 22 ottobre 2013) figura una norma transitoria aggiunta al considerando 134[55] che limita ad un periodo di 5 anni dall'entrata in vigore del Regolamento la validità di quelle decisioni della Commissione ed autorizzazioni conseguenti degli Stati membri scaturite dall'applicazione delle norme di cui agli artt. 25(6) e 26(4) della direttiva 95/46/CE, ossia quelle che disciplinano il trasferimento dei dati personali verso Paesi terzi. Si ricorda che le suddette norme danno facoltà alla Commissione di emanare Decisioni in merito alla valutazione positiva da parte della stessa, rispettivamente di adeguatezza del livello di protezione dei dati garantito dal paese terzo in cui vengono importati i dati personali e delle garanzie offerte dal responsabile del trattamento importatore dei dati, benché il paese terzo non garantisca una protezione adeguata, risultanti da clausole contrattuali appropriate, segnatamente le clausole

[53] *"Il presente regolamento dovrebbe abrogare la direttiva 95/46/CE. Ciò nondimeno, è opportuno che rimangano in vigore le decisioni della Commissione e le autorizzazioni delle autorità di controllo basate sulla direttiva 95/46/CE."*.

[54] GARANTE EUROPEO DELLA PROTEZIONE DEI DATI, 2012/C/192/05, *Sintesi del parere del 27 marzo sul pacchetto di riforma della protezione dei dati*, 2012.

[55] *Commission decisions and authorisations by supervisory authorities relating to transfers of personal data to third countries pursuant to Article 41(8) should remain in force for a transition period of five years after the entry into force of this Regulation unless amended, replaced or repealed by the Commission before the end of this period.*

tipo individuate dalla Commissione. In altri termini, se lo schema di Regolamento verrà approvato definitivamente nella versione del 22 ottobre 2013, a partire dalla data della sua entrata in vigore le Decisioni precedentemente richiamate, tra cui ad esempio la Decisione n. 2000/520/CE del 26 luglio 2000 relativa al Safe Harbor, quella del 5 febbraio 2010 n. 2010/87/UE relativa alle clausole contrattuali tipo e le decisioni del 2004, 2010, dopo 5 anni non saranno più da considerare valide, sempreché precedentemente non siano state già modificate, sostituite con altre o abrogate. Con riferimento in particolare all'Accordo Safe Harbor occorre tener presente che, anche dopo l'emanazione della proposta di Regolamento (25 gennaio 2012), che, come si è visto, di fatto, valuta insufficiente il ricorso al criterio di adeguatezza alla normativa comunitaria, imponendo, nell'offerta di servizi commerciali a cittadini europei, l'applicazione delle norme di tutela dei dati previste nel Regolamento, il Dipartimento del Commercio degli USA e la Commissione dell'UE hanno pubblicamente riaffermato in un documento a firma congiunta del marzo 2012[56] il loro impegno a mantenere in vigore l'accordo di cui sopra, in linea con gli obiettivi di accrescere gli scambi commerciali tra UE e USA e l'interoperabilità dei rispettivi regimi normativi della privacy nell'uso dei dati personali per finalità commerciali ed il rafforzamento della cooperazione nell'adozione delle misure esecutive. Ciò alla luce anche di un profondo processo di ridefinizione della privacy pure negli USA a seguito dell'emanazione il 23 febbraio 2012 da parte del Presidente Obama del blueprint sulla tutela dei dati, in cui figura il *Consumer Privacy Bill of Rights*, che è passato all'iter legislativo per l'eventuale approvazione da parte del Congresso ai fini della sua adozione nei settori commerciali, non soggetti alle vigenti leggi federali sulla privacy, attraverso lo sviluppo di codici di condotta di implementazione dei principi in esso contenuti, al termine di un processo che vedrà la partecipazione di una molteplice tipologia di stakeholder (portatori di interesse), compresi i consumatori.

Nel corso del meeting del 10 ottobre 2013 del Comitato interparlamentare europeo in merito alla riforma del quadro della

[56] U.S.-EU *Joint Statement on Privacy from EU Commission Vice-President Viviane Reding and U.S. Commerce Secretary John Bryson*, March 19, 2012.

protezione dei dati, la stessa vice-presidente della Commissione Europea Viviane Reding ha affermato che detta riforma non inciderà sul Safe Harbor, che pertanto sarà mantenuto in vigore. Un'ulteriore prova dell'importanza del mantenimento dell'Accordo Safe Harbor, divenuto un veicolo insostituibile per i flussi di dati UE-US e motore dell'economia digitale, che hanno manifestato una crescita esponenziale -unitamente al numero di imprese importatrici negli USA- sin dalla sua adozione nel 2000 se soltanto si pensa alle centinaia di milioni di clienti in Europa di compagnie web quali Google, Facebook, Microsoft, Apple, Yahoo, è la Comunicazione della Commissione del 27 novembre 2013[57], facente seguito alle due relazioni di valutazione del funzionamento del Safe Harbor del 2002 e 2008 con riferimento agli interessi dei cittadini europei e delle imprese stabilite nell'Unione, che riconosce le funzioni positive che detto Accordo ha svolto in tutto questo tempo nello sviluppo dell'economia digitale, pur non mancando di sottolinearne, con puntuale e rigorosa disamina, non pochi malfunzionamenti intervenuti nel decennio dalla sua validità, al fine di porvi rimedio. Essi concernono la mancanza di trasparenza talora delle imprese partecipanti al Safe Harbor, l'applicazione effettiva dei Principi della privacy previsti dall'Accordo da parte delle compagnie statunitensi aderenti, la necessità di una maggiore efficacia delle misure attuate finora dalle autorità negli USA o di altre ancora per il rispetto dell'osservanza, non poche volte elusa, delle correlative norme di condotta da parte delle medesime. I suddetti rilievi si traducono nella Comunicazione summenzionata in una serie di tredici raccomandazioni rivolte alle Autorità statunitensi responsabili dell'applicazione del Safe Harbor Framework, che sono invitate a trovare gli opportuni rimedi entro l'estate 2014.

Nel discorso del 9 dicembre 2013 "*Mass surveillance is unacceptable- US action to restore trust is needed now"*, l'allora vicepresidente dell'Unione europea Viviane Reding, dopo aver stigmatizzato il comportamento della National Security Agency,

[57] European Commission, COM(2013) 847 final, *Communication from the Commission to the European Commission and the Council on the Functioning of the Safe Harbor from the Perspective of EU Citizens and Companies Established in the EU*, 27.11.2013.

ricollegandosi alle suddette raccomandazioni, ha espresso la necessità che l'Accordo Safe Harbor sia reso più sicuro e che il suo funzionamento venga rivisto successivamente al loro accoglimento. Ha formulato inoltre il forte auspicio che venga accolta la raccomandazione sul reindirizzamento ("*redress*") giudiziario, di cui dovrebbero beneficiare i cittadini europei non residenti negli USA, basato su un link che le imprese americane aderenti al Safe Harbor dovrebbero inserire nella loro policy sulla privacy online di collegamento a un provider alternativo competente nella risoluzione di dispute ("Alternative Dispute Resolution", ADR), tra cui l'EU Data Protection Panel, il provider europeo che svolge il medesimo ruolo, che l'interessato (il "data subject") possa contattare direttamente e trovare prontamente disponibile a trattare il suo reclamo ed a prezzi sostenibili. Si tratta del resto di un diritto dell'interessato il cui riconoscimento è sancito dal principio di "enforcement" del Safe Harbor che prescrive il suo diritto all'accesso ad un meccanismo indipendente di risoluzione della disputa "*readily available and affordable*". In realtà non si può dire che il principio venga osservato nella sua interezza, se è vero che correntemente i prezzi dei provider ADR statunitensi nell'ambito dello schema Safe Harbor per la gestione di reclami sono di circa 200-250 $, mentre in Europa il servizio di risoluzione dello stesso reclamo, rivolgendosi la persona all'European Data Protection Panel, è gratuito[58].

Tornando alla novità più rilevante dello Schema di Regolamento, si può concludere che il mantenimento del comma 2 dell'art. 3 anche nella versione approvata dalla Commissione LIBE (Civil Liberties, Justice and Home Affairs) del Parlamento europeo del 22 ottobre 2013, pone non pochi interrogativi sulla sua compatibilità con le Decisioni di adeguatezza prese in tutti questi anni dalla Commissione ed in particolare con quella relativa al Safe Harbor. Sembra improbabile che le imprese statunitensi che operano nel mercato comunitario per la vendita di beni e servizi, possano essere assoggettate al diritto comunitario sulla privacy, proprio ora che, nell'ipotesi che al Congresso passi il Consumer Privacy Bill of Rights del Presidente Obama, la normativa corrispondente degli USA si

[58] *ibidem*

avvicinerebbe a quella europea o come minimo sarebbe da valutare adeguata ad essa. Vero è che il suddetto Schema è ancora dibattuto nel corso dell'iter legislativo e che l'approvazione definitiva potrebbe portare delle novità non facilmente prevedibili allo stato attuale, che potrebbero ad esempio annullare ogni impatto sull'operatività del Safe Harbor, come sembrerebbe sperare il Dipartimento del Commercio degli USA.

5.1.2. Strumenti di regolamentazione del trasferimento di dati all'estero.

5.1.2.1 Norme basilari.

Nell'ottica della difesa del modello comunitario di tutela dei dati personali anche quando la normativa della privacy competente sia quella di un paese terzo, lo Schema di regolamento mantiene l'indirizzo della direttiva 95/46/CE in materia di flussi internazionali dei dati (art. 40 ss.) al di fuori dello SEE, distinguendo il caso in cui detta normativa garantisca, a giudizio della Commissione, un livello di protezione "adeguato" agli standard comunitari, dagli altri in cui il giudizio sia di "inadeguatezza" o non sia stata emanata alcuna Decisione dalla medesima in merito a tale questione, richiedendosi allora in entrambe le circostanze per la liceità del trasferimento il ricorso, salvo situazioni di esenzione dal relativo obbligo, da parte del responsabile e dell'incaricato del trattamento alle prassi vigenti in materia di misure compensative, che lo schema di Regolamento ripropone approfondendole. Si tratta di strumenti appositi per rendere il trasferimento di dati all'estero conforme ad un livello di "adeguatezza" e quindi consentirlo, tra cui:

- le clausole tipo di protezione approvate dalla Commissione europea
- le Binding Corporate Rules (BCR). Tale strumento, trattato nell'art. 43, viene recepito ed affinato.
- le clausole tipo di protezione dei dati adottate da un'Autorità di controllo.
- le clausole contrattuali tra il responsabile del trattamento o l'incaricato del trattamento e il destinatario dei dati autorizzate da

un'autorità di controllo in conformità del paragrafo 4 dell'articolo 42.
- in caso di importazione di dati personali da parte di compagnie statunitensi l'Accordo *Safe Harbor*. Questo strumento avrà ancora validità per una fase transitoria di 5 anni dall'entrata in vigore del Regolamento, nell'ipotesi, tutt'altro che scontata, che la versione del 22 ottobre 2013 rimanga quella definitiva.

Ad una di esse dovrà ricorrere il responsabile del trattamento e l'incaricato del trattamento, salvi i casi di deroga (ad esempio consenso dell'interessato od esecuzione di un contratto che riguarda l'interessato) dall'impegno di fornire garanzie adeguate, come già previsto nella casistica della direttiva 95/46/CE.

Rispetto alla Direttiva 95/46/CE il Regolamento rafforza gli strumenti sanzionatori del trasferimento illegittimo verso Paesi terzi e della divulgazione non autorizzata. L'importo comminabile come sanzione può arrivare ad un massimo di 100 M.ni di Euro, che per le imprese può essere elevato fino al 5% (2% nella proposta originaria di Regolamento) del fatturato annuale realizzato su scala mondiale.

5.1.2.2 Norme vincolanti d'impresa (Binding Corporate Rules).

Sono norme interne (regole di condotta) adottate da una compagnia multinazionale per il trasferimento dei dati nell'ambito dello stesso gruppo internazionale verso entità del gruppo stabilite in Paesi terzi, nei quali non è fornito un adeguato livello di protezione dei dati. Ai sensi dell'art. 43 del Regolamento le Binding Corporate Rules (BCR) devono contenere in particolare:
- Principi della privacy quali trasparenza, qualità dei dati, sicurezza
- Strumenti di misura di efficienza (certificazione, sistema di trattamento di un reclamo e così via) e
- Una clausola che attesta che le BCR sono vincolanti

Le BCR sono uno strumento validamente utilizzabile anche nell'ambito del Cloud Computing nel caso classico in cui il fornitore del servizio sia un incaricato del trattamento. In effetti, il WP29 attualmente sta lavorando su BCR per incaricati del trattamento, che consentano il trasferimento all'interno del gruppo a vantaggio dei responsabili del trattamento senza richiedere la firma di un contratto

tra incaricato del trattamento e subincaricati per ciascun cliente. Questo tipo di BCR per gli incaricati del trattamento consentirebbero al cliente di affidare i propri dati personali all'incaricato del trattamento con la sicurezza che i dati trasferiti entro la portata dell'attività del fornitore del servizio ricevano un adeguato livello di protezione[59].

5.1.3 Diritto all'oblio.

L'articolo 17 dal titolo "diritto alla cancellazione"[60], approfondendo quanto già previsto in materia dall'articolo 12, lett. b) e lett. c della direttiva 95/46/CE[61], codifica questo diritto degli interessati e istituisce un particolare meccanismo di attuazione (*enforcement*), stabilendo che l'interessato ha il diritto di ottenere dal responsabile del trattamento dei dati la cancellazione dei dati che lo riguardano, l'ulteriore diffusione di tali dati e dai terzi la soppressione di tutti i link verso tali dati, le loro copie o riproduzioni, se sussiste fondamentalmente una delle seguenti condizioni:

- i dati non sono più necessari rispetto alle finalità per le quali erano stati raccolti o trattati;
- l'interessato revoca il consenso al trattamento perché condizionato a specifiche finalità da lui specificate venute meno, oppure perché è scaduto il periodo di trattamento dal medesimo autorizzato e non sussiste motivo legittimo per trattare i dati;
- l'interessato esercita "il diritto di opposizione" al trattamento dei dati personali, per motivi connessi alla sua situazione personale, -e può farlo legittimamente in qualsiasi momento, salvo che il

[59] GRUPPO DI LAVORO PER LA TUTELA DEI DATI EX ART. 29, Parere 05/2012 sul *Cloud Computing*, cit.

[60] Nella versione del 25 gennaio 2012 il titolo dell'articolo era "*Diritto all'oblio ed alla cancellazione*".

[61] Art. 12, lett. b) 95/46/CE: [ogni persona interessata al trattamento ha diritto di ottenere dal responsabile del trattamento] "*a seconda dei casi, la rettifica, la cancellazione e il congelamento dei dati il cui trattamento non è conforme alla presente direttiva, in particolare a causa del carattere incompleto o inesatto dei dati*". Nell'art. 12, lett. c) si prescrive che le operazioni di cui sopra siano comunicate a terzi, salvo il sostenimento di oneri eccessivi, ai quali i dati in questione erano stati comunicati.

responsabile del trattamento non dimostri l'esistenza di motivi preminenti e legittimi per procedere al trattamento che prevalgono sugli interessi o sui diritti e sulle libertà fondamentali dell'interessato – e ha diritto alla cancellazione nei casi in cui detto trattamento non sia necessario, per (i) la salvaguardia degli interessi vitali dell'interessato, (ii) l'esecuzione di un compito di interesse pubblico, (iii) l'esercizio di pubblici poteri di cui è investito il responsabile del trattamento, (iv) il perseguimento del legittimo interesse del responsabile del trattamento;

- il trattamento dei dati non è conforme al presente regolamento per altri motivi.

Il cosiddetto "diritto all'oblio"[62] è una forma di tutela dell'identità personale e morale, che riconosce ad ogni persona il soddisfacimento di una sua richiesta di cancellazione dei dati personali precedentemente archiviati e trattati, quando venga meno la legittimità o le finalità del trattamento ed in particolare in tutte le circostanze in cui i dati suddetti non riflettono la propria attuale dimensione personale, sociale o giuridica. Si tratta, quindi, del diritto di un individuo a non essere più ricordato per fatti che in passato furono registrati dalla cronaca. Fatto salvo il diritto all'informazione per il pubblico, un individuo che abbia commesso un reato in passato ha il pieno diritto di richiedere che quel reato non venga più divulgato dalla stampa e dagli altri canali di informazione. A rendere estremamente attuale il concetto di "diritto all'oblio" – già presente nella letteratura giuridica italiana- è l'esplosione di Internet e l'uso dei motori di ricerca che mettono a disposizione, a seguito di digitazione del nominativo di una persona, pagine di archivi elettronici dei quotidiani nazionali, che non ne rispecchiano, ad esempio, l'attuale posizione giudiziaria procurandole un evidente danno dell'immagine.

Una sentenza del Tribunale di Milano (n. 5820/2013, pubblicata il 26.4.2013)[63] in tema di diritto all'oblio in Internet è perfettamente

---

[62] SARZANA F. " *il diritto all'oblio consiste nel chiedere a un sito web o a un motore di ricerca di cancellare un articolo, un link, un'immagine dove i nostri dati personali sono usati in modo da offendere la nostra reputazione e senza che ci sia il legittimo diritto di cronaca*".

[63] Il Sole24Ore, *Internet e diritto "all'oblio": una recente sentenza del Tribunale di Milano*, 29 luglio 2013.

allineata a quanto disposto dall'articolo delineato del Regolamento e ad una precedente sentenza del Tribunale di Ortona (CH), dal momento che ha riconosciuto all'interessato, che lamentava la facile accessibilità in Rete ad un articolo di giornale del 1985 in cui era descritto come usuraio ed evasore, il diritto all'oblio, nella fattispecie l'accoglimento della sua richiesta di rimozione dell'articolo dal sito dell'editore. Nel gennaio 2013 il Tribunale di Ortona ha condannato la testata online www.PrimaDaNoi.it al pagamento di una multa di oltre 17 mila euro, per un fatto di cronaca giudiziaria avvenuto nel 2008 che aveva coinvolto due ristoratori. Nel 2010 la richiesta di uno dei due interessati, che si appellava al diritto all'oblio, di rimozione dell'articolo che lo riguardava, era stata rifiutata dal direttore del quotidiano. Nel 2011 l'articolo era stato cancellato dai motori di ricerca con tecnica di de-indicizzazione e nel 2013, a seguito della condanna del tribunale, l'articolo è stato addirittura rimosso anche dall'archivio della testata. Secondo il giudice, "*il trattamento dei dati personali si è protratto per un periodo di tempo superiore a quello necessario agli scopi (esercizio del diritto di cronaca giornalistica) per i quali i dati sono stati raccolti e trattati*)". In effetti, già una storica sentenza della Corte di Cassazione n. 5525/2012 in un caso simile aveva riconosciuto ad ogni persona espressamente l'esistenza di un diritto alla tutela della propria (attuale) identità personale e morale riflessa nell'ambito sociale, prevalente nei confronti del diritto di cronaca, in quanto esso era stato esercitato dall'editore con la digitalizzazione dei dati di stampa in grado di identificare la persona alla quale erano riferiti e la loro messa su Internet, con l'attuazione così di una misura eccedente, e quindi oltre le finalità del trattamento di informativa nei riguardi del pubblico e di documentazione storica, rispetto a quella riconosciuta, invece, dal Codice della Privacy della predisposizione e conservazione di un archivio cartaceo. La Corte di Ortona ha posto quindi a carico dell'editore l'obbligo di aggiornare la notizia segnalando la sussistenza di un seguito o di contestualizzarla, considerando solo come "*extrema ratio*" l'operazione di cancellazione dall'archivio digitale, se non più rispondente al vero ("diritto d'oblio").

Ai problemi di cui sopra il Garante dei dati personali aveva dato in precedenza una soluzione diversa consistente nell'imposizione

dell'obbligo in capo all'editore di "de-indicizzazione" dell'articolo dai motori di ricerca esterni al sito del giornale, piuttosto che disporre un intervento diretto sul documento alla fonte. Peraltro, a seguito delle ripercussioni della sentenza summenzionata della Corte di Cassazione, il Garante nell'accogliere vari ricorsi nel 2013 ha imposto all'editore, unico e vero titolare del trattamento, di integrare l'articolo, nonostante fosse stato già de-indicizzato" dai gestori dei motori di ricerca, con un'annotazione a margine circa l'evoluzione della notizia, in modo da contemperare il rispetto del diritto dell'interessato alla protezione della propria attuale identità personale con quello del lettore del giornale a ricevere un'informazione veritiera ed aggiornata. Tuttavia, nel pronunziarsi in merito alle richieste degli interessati di vedersi riconoscere un vero e più radicale "diritto d'oblio" con la procedura della cancellazione dal sito originario, Il Garante continua a darne un'interpretazione soft, ammettendo implicitamente che non si possa andare oltre, ai sensi della vigente Direttiva 95/46/CE.

Questa posizione è coerente con il parere dell'Avvocato generale Jääskinen[64], secondo il quale l'art. 12, lett. b) della Direttiva 95/46/CE, che sancisce il diritto dell'interessato a ottenere la cancellazione e il congelamento dei dati personali, e l'art. 14, lett. a) della medesima, che attribuisce all'interessato il diritto di opposizione al trattamento, non assegnano alcun fondamento normativo al "diritto all'oblio". Non esisterebbe, in altri termini, sulla base delle norme vigenti, un diritto assoluto dell'interessato a ottenere la rimozione dei dati ritenuti dannosi, che solo può aversi quando il trattamento sia difforme dai principi fissati dalla Direttiva[65]. Inoltre, a rendere non del tutto scontata la codifica definitiva del "diritto d'oblio", così come risultante dalla Proposta di Regolamento, è una recente sentenza della Corte europea dei diritti dell'uomo di Strasburgo (sentenza del 16 luglio 2013 sul ricorso n. 33846/07[66]), che stabilisce che la

[64] JÄÄSKINEN, *Conclusioni espresse davanti alla Corte di giustizia dell'Unione europea in merito alla causa C-131/12* (Google Spain SL, Google Inc., v. Agencia Española de Protección de Datos (AEPD),).

[65] IL SOLE24ORE, *Il diritto all'oblio a Lussemburgo*, 27 giugno 2013

[66] EUROPEAN COURT OF HAMAN RIGHTS, *CASE OF WĘGRZYNOWSKI AND SMOLCZEWSKI v. POLAND (Application no. 33846/07)* JUDGMENT STRASBOURG 16 July 2013 FINAL 16/10/2013.

cancellazione di un articolo dall'archivio elettronico di un organo di informazione equivale a una censura, pur prendendo atto nel caso esaminato di una violazione del diritto alla reputazione accertata da un tribunale nazionale[67]. La Corte di Strasburgo afferma che costituisce una violazione dell'articolo 10 della Convenzione, che garantisce la libertà di espressione, la mancata protezione degli archivi web dei giornali per effetto di una rimozione di articoli reperibili online, senza contare il loro valore storico da salvaguardare in una società democratica, in cui il diritto all'informazione è fondamentale per la collettività. Inoltre la rimozione di cui sopra potrebbe produrre "*una riscrittura della storia*". Secondo la Corte di Strasburgo la conservazione nel web di notizie giornalistiche non comporta alcuna violazione della privacy (art. 8 della Convenzione europea dei diritti dell'uomo) ed il diritto della tutela della reputazione nel caso di articoli diffamatori ma obsoleti visualizzati via web, a seguito di indicizzazione del motore di ricerca, può essere garantito semplicemente con l'integrazione dell'articolo con una nota informativa circa l'accertamento dei giudici in merito al carattere lesivo dell'immagine sociale dell'interessato riflessa nell'articolo e la pronuncia dei medesimi.

Fermo restando il diritto di un interessato di ottenere la rettifica o l'aggiornamento delle informazioni contenute in un articolo accessibile via web ritenuto lesivo della propria reputazione, in Italia il "*diritto all'oblio*" non è ancora codificato, ma occorre ricordare che nel Ddl approvato in commissione Giustizia al Senato nell'ottobre del 2012[68] figura per la prima volta una norma che riconosce "*il diritto a richiedere ai siti internet e ai motori di ricerca l'eliminazione dei contenuti diffamatori o dei dati personali trattati in violazione della presente legge*" come si legge nel testo. La norma è stata sollecitata da più parti, ma che nel modo in cui è scritta può limitare, secondo

[67] Si veda <http://www.primadanoi.it/news/mondo/542599/Diritto-all-oblio--Corteeuropea.html>

[68] A. LONGO, *Ddl diffamazione introduce il diritto all'oblio con multe da cinquemila a centomila euro*, La Repubblica, 24 ottobre 2012.

un'autorevole scuola di pensiero, la libertà di espressione e rischiare in nome della privacy di soffocare la libertà di internet[69].

6. Conclusioni.

Con il nuovo regolamento sulla tutela dei dati, che diverrà una legge unica pan-europea sostitutiva dell'inconsistente patchwork attuale di 28 ordinamenti giuridici nazionali, almeno nell'odierna versione l'Unione europea ribadisce con forza il primato della propria normativa, prevedendone l'applicazione anche al di fuori del proprio territorio a tutela dei propri cittadini in maniera incondizionata ed imperativa, allorquando soggetti extracomunitari mettano in atto trattamenti dei loro dati personali volti a controllarne i comportamenti o ad offrire loro beni e/o servizi. Il Garante italiano della Privacy paragona il regolamento di cui sopra, peraltro ancora allo stato di bozza, ad una "*fortezza, che impone le norme Ue anche alle aziende extra europee che operano nel mercato interno, ma è tutto da verificare se queste aziende rispetteranno le regole imposte e soprattutto se l'Ue sarà in grado di farle rispettare*". Questo problema si presenta particolarmente impegnativo con riferimento all'imposizione, ai sensi della Proposta di Regolamento, alle imprese statunitensi delle medesime norme al cui rispetto sono tenute le imprese stabilite nell'Unione Europea, in modo che, secondo l'intenzione del legislatore comunitario, venga stabilito un *level playing field*, espressione traducibile con "campo di gioco livellato", nella protezione dei dati trattati nell'ambito della relazione

[69] Sono in molti a criticare la riforma varata dall'UE ed in particolare l'istituito diritto all'oblio che disconosce l'essenza originaria della Rete, ossia quella di essere un archivio di informazione, unico nel suo genere, divenuto sempre più enorme, in cui tutto si conserva e nulla si dimentica. Secondo Vinton Cerf, uno dei padri fondatori della "Rete", le normative sul diritto all'oblio, al vaglio dell'Unione Europea costituiscono una pericolosa minaccia per la libertà di espressione su cui si fonda il mondo di Internet. Il suo pensiero al riguardo può essere in modo icastico sintetizzato dalla sua espressione: "*Non potete uscire di casa ed andare alla ricerca di contenuti da rimuovere sui computer della gente solo perché volete che il mondo si dimentichi di qualcosa. Non penso che sia praticabile.*"

commerciale col consumatore europeo, che metta fine allo svantaggio competitivo lamentato dalle imprese europee.

L'Accordo *Safe Harbor* risulta superato od insufficiente alla luce del nuovo assetto normativo comunitario, ed è per questo che lo Schema attuale del Regolamento ne estende la validità non oltre cinque anni dalla sua entrata in vigore. Senza contare che nella Comunicazione della Commissione del 27/11/2013[70] vengono enfatizzate la scarsa trasparenza nelle policies di privacy delle imprese statunitensi aderenti all'Accordo e le insufficienti misure di controllo dell'attuazione delle norme da loro sottoscritte da parte delle Autorità di controllo degli USA, ossia Department of Commerce e Federal Trade Commission. Intanto gli USA e la UE hanno riaffermato nel documento sottoscritto il 19 marzo 2012 dal vicepresidente della UE e dal Segretario del commercio USA John Bryson il reciproco impegno a rafforzare l'Accordo Safe Harbor, in piedi fin dal 2000, ritenuto un punto di partenza imprescindibile per una maggiore interoperabilità dei sistemi normativo-regolamentare della privacy applicati nelle due sponde dell'Atlantico. Con riferimento al sistema di tutela dei dati vigente negli USA, Viviane Reding ha ricordato alle Autorità preposte a detta tutela che le regole della privacy devono essere applicate indipendentemente dalla nazionalità dell'interessato ("*data subject*") e che applicare differenti standard a residenti e a non residenti, come difatti sta avvenendo complice anche l'ombrello protettivo per l'industria americana del Safe Harbor, non ha senso, quanto meno alla luce della natura aperta di Internet[71].

La nuova legislazione comunitaria sulla privacy, volta a definire un quadro normativo unitario a livello continentale, pur affrontando i temi sollevati in relazione al Cloud Computing, tra cui il trasferimento di dati personali a paesi situati al di fuori del territorio dell'UE e del SEE garantendo la continuità della protezione delle persone interessate, per molti versi, appare, peraltro, ancora inadeguata nei confronti dei vari modelli di *ICT as a service*. Su tale fronte siamo

[70] EUROPEAN COMMISSION, *Communication on the Functioning of the Safe Harbor from the Perspective of EU citizens and Companies Established in the EU*, 27 November 2013.

[71] REDING V., *Data Protection Day 2014: Vice-President Reding calls for a new data protection compact for Europe European Commission*, IP/14/70, 28/01/2014.

ancora in una fase iniziale della storia di questa nuova messa a disposizione di servizi computazionali, il cui modello di erogazione è simile a quello delle tradizionali utilities (gas, acqua, energia elettrica), ma presenta alcuni aspetti peculiari che attengono alla sicurezza dei dati, fondamentale per lo sviluppo del modello Cloud, tra cui principalmente**:**

- più marcata delocalizzazione dei dati, che possono migrare dai computer locali verso sistemi remoti di proprietà o gestiti da un terzo fornitore del servizio.
- conseguente ridotta capacità di controllo da parte del titolare del trattamento dei dati sulle modalità di tale trattamento e/o sull'infrastruttura per il trattamento dei dati.

Migrando i dati dai sistemi locali sotto il diretto controllo dell'utente ai sistemi remoti del fornitore, questi assume un ruolo centrale in ordine alla sicurezza dei dati e, quindi, all'adozione delle misure necessarie a garantirla, ma non per questo l'esternalizzazione dei servizi esime le imprese e le amministrazioni pubbliche che se ne avvalgono per la gestione del proprio patrimonio informativo dalle responsabilità che vengono loro attribuite, in particolare, dalla disciplina in materia di protezione dei dati personali.

Altre criticità, in fatto rispettivamente di mancanza di trasparenza e di integrità, derivano dall'instaurarsi di una catena di trasformazione di servizi acquisiti presso altri *service provider*, diversi dal fornitore con cui l'utente stipula il contratto di servizio e dalla molteplicità di clienti che condividono la struttura informatica messa a disposizione dal Cloud provider e talora anche gli stessi server per la memorizzazione dei loro dati con conseguenti rischi per la sicurezza del singolo patrimonio informativo ivi residente. A tale riguardo si fa rilevare che è assai difficile fare rientrare il complesso di relazioni che si instaurano fra i numerosi attori coinvolti nel passaggio al Cloud Computing nello schema Titolare-incaricato che esaurisce i ruoli formalmente definiti dalla proposta di Regolamento. La portabilità ed interoperabilità dei dati possono inoltre essere messe a rischio dall'adozione da parte del fornitore del servizio di tecnologie proprie, risultando così difficoltosa per il cliente Cloud la transizione di dati e documenti da un sistema Cloud ad un altro o lo scambio di informazioni con soggetti che utilizzino servizi Cloud di fornitori

differenti[72]. Sapere in quale Stato risiedono i *server* sui quali vengono allocati i dati, è determinante per stabilire la giurisdizione e la legge applicabile nel caso di controversie tra l'utente e il fornitore del servizio. La presenza fisica dei *server* in uno Stato comporterà per l'autorità giudiziaria nazionale, infatti, la possibilità di dare esecuzione ad ordini di esibizione, di accesso o di sequestro, ove sussistano i presupposti giuridici in base al singolo ordinamento nazionale, spesso divergente da quello vigente nell'Unione europea. In ogni caso, l'utente, prima di inserire i dati nella nuvola informatica, dovrebbe assicurarsi che il trasferimento tra i diversi paesi in cui risiedono le Cloud avvenga nel rispetto delle cautele previste dall'Unione europea in materia di protezione dei dati personali, che esigono particolari garanzie in ordine all'adeguatezza del livello di tutela previsto dagli ordinamenti nazionali per tale tipo di informazioni.

[72] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Cloud Computing. Proteggere i dati per non cadere dalle nuvole*, 2012.

GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI

Opinion 9/2014 on the application of Directive 2002/58/EC to device fingerprinting

adopted on 25 November 2014

http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm

THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

Set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995,

Having regard to Articles 29 and 30 thereof,

Having regard to its Rules of Procedure,

HAS ADOPTED THE PRESENT OPINION:

Summary

Device fingerprinting presents serious data protection concerns for individuals. For example, a number of online services have proposed device fingerprinting as an alternative to HTTP cookies for the purpose of providing analytics or for tracking without the need for consent under Article 5(3)[1]. This demonstrates that the risks presented

[1] Wall Street Journal, 2013. Web Giants Threaten End to Cookie Tracking. http://online.wsj.com/news/articles/SB10001424052702304682504579157780178992984

by device fingerprinting are not theoretical and research has shown that device fingerprinting is already being exploited[2].

In this Opinion, the Article 29 Working Party (WP29) addresses the topic of device fingerprinting and the applicability of Article 5(3) of the ePrivacy Directive 2002/58/EC, as amended by Directive 2009/136/EC, without prejudice to the provisions of the Data Protection Directive 95/46/EC. The key message of this Opinion is that Article 5(3) of the ePrivacy Directive is applicable to device fingerprinting.

This Opinion expands upon the earlier Opinion 04/2012 on Cookie Consent Exemption[3] and indicates to third-parties[4] who process device fingerprints which are generated through the gaining of access to or the storing of information on the user's terminal device that they may only do so with the valid consent of the user (unless an exemption applies).

2. Introduction

Article 5(3) of Directive 2002/58/EC as amended by Directive 2009/136/EC[5], (the ePrivacy Directive) stipulates that Member States shall ensure that "the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user" is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information in accordance with Directive 95/46/EC[6] (the Data Protection Directive), inter alia, about the purposes of the processing[7].

---

[2] Nikiforakis, 2013. Cookieless Monster: Exploring the Ecosystem of Web-based Device Fingerprinting. https://lirias.kuleuven.be/bitstream/123456789/393661/1/

[3] Article 29 Working Party, 2012. Opinion 04/2012 on Cookie Consent Exemption. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf

[4] "Third-party" as referred to in Recital 66 of Directive 2009/136/EC.

[5] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri= CELEX:32009L0136:en: NOT

[6] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:

In Opinion 04/2012, WP29 considered Article 5(3) of the ePrivacy Directive in relation to the storage of, or access to, information through the use of cookies. The Opinion stated that Article 5(3) does not exclusively apply to cookies but is also applicable to "similar technologies".

This Opinion addresses growing reports that third-parties are actively exploring alternative technologies to cookies for a range of purposes in an effort to avoid the consent requirement of Article 5(3). In particular, the combination of a set of information elements in order to uniquely identify particular devices or application instances, so-called "device fingerprinting", is examined.

Device fingerprints can also constitute personal data. This Opinion does not provide an analysis of the relevant provisions of the Data Protection Directive, but refers to data protection issues which are particularly relevant in the context of device fingerprinting. For example, when several information elements are combined, especially unique identifiers such as an IP addresses, and the purpose of the processing is to identify users over time, across websites, such as with behavioural advertising. In such cases, processing must also comply with the rules provided in the Data Protection Directive.

The technology of device fingerprinting is not limited to the configuration parameters of a traditional web browser on a desktop PC. Device fingerprinting is not tied to a particular protocol either, but can be used to fingerprint a broad range of internet connected devices, consumer electronics and applications, including those running on mobile devices, smart TVs, gaming consoles, e-book readers, internet radio, in-car systems or smart meters[8].

NOT

[7] This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.

[8] Sometimes referred to as the "Internet of Things".

3. Definition

RFC6973[9] defines a fingerprint as "a set of information elements that identifies a device or application instance". This Opinion uses the term in a broad sense, meaning that it includes a set of information that can be used to single out[10], link[11] or infer[12] a user, user agent or device over time. This includes, but is not limited to, data derived from:

(a) the configuration of a user agent/device; or

(b) data exposed by the use of network communications protocols.

There are many types of data that can form a fingerprint, including the following examples:

(a) CSS information;

(b) JavaScript objects (e.g., document, window, screen, navigator, date and language);

(c) HTTP header information (e.g., the number of bits of information in the User Agent string, HTTP header ordering, HTTP header variation by request type);

(d) clock information (e.g., clock skew and clock error);

(e) TCP stack variation;

(f) installed fonts;

---

[9] Cooper, 2013. Privacy Considerations for Internet Protocols Cooper, 2013. http://tools.ietf.org/html/rfc6973

[10] *Singling out*: the possibility to isolate some or all records which identify an individual in the dataset, Opinion 05/2014 on Anonymisation Techniques, pp 11-12.

[11] *Linkability*: the ability to link, at least, two records concerning the same data subject or a group of data subjects (either in the same database or in two different databases). If an attacker can establish (e.g. by means of correlation analysis) that two records are assigned to a same group of individuals but cannot single out individuals in this group, the technique provides resistance against "singling out" but not against linkability, Opinion 05/2014 on Anonymisation Techniques, pp 11-12.

[12] *Inference*: the possibility to deduce, with significant probability, the value of an attribute from the values of a set of other attributes, Opinion 05/2014 on Anonymisation Techniques, pp 11-12.

(g) installed plugin information (e.g., configuration and version information)[13];

(h) the use of internal Application Programming Interfaces[14] (API) exposed by the user agent/device; or

(i) the use of external API's of Web services the user agent/device is communicating with.

4. Technical background

The internet and the Web have been developed with the needs of a resilient and open architecture network environment in mind[15]. Due to design choices to meet these needs, devices transmit information elements. A number of protocols include a range of mandatory and optional information elements. For example, the HTTP/1.1[16] protocol specifies header fields which allow the server and the client to include additional information regarding the hypertext. Some of these were specifically intended for the server to recognise client types. For example, the User-Agent request-header field includes the description: "*This is for statistical purposes, the tracing of protocol violations, and automated recognition of user agents for the sake of tailoring responses to avoid particular user agent limitations*".

Typical uses of the User Agent String include the optimisation of the layout of content for a particular type of device; to use this information to target content to specific users[17]; or to collect information about the device for security or analytics purposes.

---

[13] Cf. (a) http://www.w3.org/wiki/Fingerprinting, (b) http://w3c.github.io/fingerprinting-guidance/#wsj-orbitz, (c) https://wiki.mozilla.org/Fingerprinting and (d) https://trac.webkit.org/wiki/Fingerprinting for mechanisms.

[14] The API offers a user friendly framework for accessing functions or routines within a software component.

[15] Kahn, 1972. Communications Principles for Operating Systems. Internal BBN memorandum.

[16] Fielding, Reschke, 2014. Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content. http://www.ietf.org/rfc/rfc7231.txt

[17] Wall Street Jorunal, 2012. On Orbitz, Mac Users Steered to Pricier Hotels, http://online.wsj.com/article/SB10001424052702304458604577488822667325882.html

5. Data protection risks

Because an individual HTTP header typically has a non-unique value, users can rarely be individually identified from the information element alone[18]. For example, the media types supported by a browser are often the same amongst many other users utilizing the same browser version. Therefore, when processed in isolation, these non-unique information elements do not generally present a data protection risk.

However, a number of information elements can be combined to provide a set which is sufficiently unique (especially when combined with other identifiers such as the originating IP address) to act as a unique fingerprint for the device or application instance. Such a fingerprint provides the ability to distinguish one device from another and can be used as a covert alternative for cookies to track internet behaviour over time[19,20,21]. As a result, an individual may be associated, and therefore identified, or made identifiable, by that device fingerprint.

The data protection risks of device fingerprinting are increased by the fact that the unique set of information elements is not only available to the website publisher, but also to many other third parties. This is in contrast to the same origin policy of HTTP cookies and exacerbated by the technical nature of the world wide web, where many third parties contribute to the content of a web page.

It is common that a single webpage is dynamically generated in real-time by requesting content from multiple sources. Each of these resources will generate HTTP requests of their own, downloading images, JavaScript and CSS files. Many webpages also contain web-bugs and tracking scripts. They may also issue HTTP requests that

[18] There are cases where a single information element carries information that may uniquely identify a data subject, such as an OAuth access token.
[19] Panopticlick, Electronic Frontier Foundation, 2010. https://panopticlick.eff.org/
[20] Yen, 2012. Host Fingerprinting and Tracking on the Web: Privacy and Security Implications. http://research.microsoft.com/pubs/156901/ndss2012.pdf
[21] Eckersley, 2010. A Primer on Information Theory and Privacy. https://www.eff.org/deeplinks/2010/01/primer-information-theory-and-privacy

record when a user scrolls or clicks on a page, image or advertisement. Therefore, third-parties frequently have the opportunity to collect the information needed to fingerprint the user's device.

The data protection risks are not limited to tracking by third parties. The combination of data obtained through Application Programming Interfaces (API) present in the software on client devices also poses a risk of device fingerprinting. Different software, platforms and APIs will each offer access to different information elements stored in the device. The web browser JavaScript API, for example, can provide information relating to the screen size, colour depth and available system fonts. Other APIs may request access to information elements stored in the firmware (e.g. the CPU type), operating system (e.g. the OS type) or graphics card model[22]. API calls may also reveal the presence of installed software (e.g. browser plug-ins) or even the precise version numbers. Access to such sets of information increases the number of bits of information (entropy) and therefore the risk of recognition of unique individuals through their device[23].

In contrast to HTTP cookies, device fingerprinting can operate covertly[24]. There are no simple means for users to prevent the activity and there are limited opportunities available to reset or modify any information elements being used to generate the fingerprint. As a result, device fingerprints can be used by third-parties to secretly identify or single out users with the potential to target content or otherwise treat them differently.

It has been noted in Opinion 16/2011[25] that advertising companies have argued that the use of unique codes or other values does not

[22] Mowery, 2012. Pixel Perfect: Fingerprinting Canvas in HTML5. http://cseweb.ucsd.edu/~hovav/dist/canvas.pdf

[23] Mozilla, 2014. https://wiki.mozilla.org/Fingerprinting

[24] Only in specific cases, the protocol requires a signal to the user, such as the geolocation HTML5 API specification. See: http://www.w3.org/TR/geolocation-API/#privacy_for_uas.

[25] Article 29 Working Party, 2014. Opinion 16/2011 on EASA/IAB Best Practice Recommendation on Online Behavioural Advertising. http://ec.europa.eu/justice/ data-protection/article-29/documentation/opinion-recommendation/ files/2011/wp 188_en.pdf

involve the processing of personal data. This is in contradiction to the purpose of processing for the delivery of personalised content and advertisements, i.e., to communicate directly with a specific individual. The Working Party has argued on many occasions that such unique identifiers qualify as personal data[26].

6. Legal framework

When a fingerprint is generated through the storage of or access to information stored in the user's terminal device, the ePrivacy Directive applies.

As described in Opinion 04/2012, Article 5(3) allows for processing to be exempt from the requirement of consent, if one of the following criteria is satisfied:

CRITERION A: technical storage or access "for the sole purpose of carrying out the transmission of a communication over an electronic communications network".

CRITERION B: technical storage or access which is "*strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service*".

Furthermore, the website operator must respect the defined meaning of any other signal which indicates the user's preference in this regard - such as the Do-Not-Track[27] header[28].

Although the application of the Data Protection Directive is outside the scope of this Opinion where device fingerprinting constitutes the

[26] Article 29 Working Party, 2014. Opinion 05/2014 on Anonymisation Techniques, pp 11-12. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

[27] W3C, Tracking Preference Expression (DNT). http://www.w3.org/TR/tracking-dnt/

[28] The Do Not Track protocol has potential, under certain circumstances, to become a granular consent mechanism that is in line with Recital 66 of Directive 2009/136/EC Recital allows for users to express consent through their browser settings, but only if the consent complies with the above mentioned requirements for valid consent. http://ec.europa.eu/justice/data-protection/article-29/ documentation/ other-document/files/2014/20140606_wp29_ts_standardisation_letter_to_w3c.pdf

processing of personal data it is important that this is done in accordance with each relevant provision of this Directive.

Article 5(3) of the ePrivacy Directive sets the requirement for consent from the user for any party which intends to store or access information stored in the user's terminal device, even if that information is not yet considered to be personal data. WP29 has discussed consent in a number of opinions both in general[29] and with specific regard to online behavioural advertising[30]. The Working Party has also discussed the consent requirement in the context of Article 5(3) and cookies[31].

It is worthy to recall Opinion 02/2013 on apps on smart devices[32] which noted:

"*the distinction between the consent required to place any information on and read information from the device, and the consent necessary to have a legal ground for the processing of personal data. Though both consent requirements are simultaneously applicable […] the two types of consent can be merged in practice, provided that the user is made unambiguously aware of what he is consenting to.*"

Recital 66 of the ePrivacy Directive refers to "*unwarranted intrusion into the private sphere*" and Article 5 addresses the requirement for the confidentiality of the communications. Article 5(3) can be regarded as extending the confidentiality of information to that which is stored or accessed on the user's device. Therefore any processing which the third-party undertakes which influences the behaviour of that device or otherwise cause it to store or give access to information

[29] Article 29 Working Party, 2011. Opinion 15/2011 on the definition of consent. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf

[30] Article 29 Working Party, 2010. Opinion 2/2010 on online behavioural advertising. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf

[31] Article 29 Working Party, 2013. Working Document 02/2013 providing guidance on obtaining consent for cookies. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp208_en.pdf

[32] Article 29 Working Party, 2013. Opinion 02/2013 on apps on smart devices. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf

on that device, or exposed by that device is within the scope of Article 5(3).

Use of the words "*stored or accessed*" indicates that the storage and access do not need to occur within the same communication and do not need to be performed by the same party. Information that is stored by one party (including information stored by the user or device manufacturer) which is later accessed by another party is therefore within the scope of Article 5(3). An example is a mobile phone app which processes the user's contact list where the contact details are stored by the user himself but the access is performed by the third-party. It is not correct to interpret this as meaning that the third-party does not require consent to access this information simply because he did not store it. The consent requirement also applies when a read-only value is accessed (e.g. requesting the MAC address of a network interface via the OS API).

Thus it is important for a third-party to remember that where device fingerprinting requires the storage of, or access to, (a set of) information on the user's device then consent will be required (unless a valid exemption applies). This will remain the case even if some of those information elements did not require the storage of, or access to, information.

7. Use case scenarios

7.1. Use case: First-party website analytics

A number of online services have proposed device fingerprinting as an alternative to HTTP cookies for the purpose of providing analytics without the need for consent under Article 5(3). In Opinion 04/2012 the Working Party recognised the need for a third exemption for the consent requirement for first party analytics:

"*provided that they are strictly limited to first party aggregated statistical purposes and when they are used by websites that already provide clear information about these cookies in their privacy policy as well as adequate privacy safeguards. Such safeguards are expected to include a user friendly mechanism to opt-out from any data*

collection and comprehensive anonymization mechanisms that are applied to other collected identifiable information such as IP addresses."

However, the Opinion also stated that currently there is no exemption to consent for cookies that are strictly limited to first party anonymised and aggregated statistical purposes[33]. Therefore, first-party website analytics through device fingerprinting do not fall under the exemption defined in CRITERION A or B and consent of the user is required.

7.2. Use case: Tracking for online behavioural advertising

Many websites include third-party web-bugs, pixel tags and JavaScript code to enable advertising services. This results in a number of requests for information elements from the user's device. The requests are transmitted to the third-parties providing the advertising services, and allow them to generate a device fingerprint to follow users across websites and over time, and create an interest profile for targeted advertising, even if the user declines cookies. Such processing can technically be undertaken in a covert manner without the knowledge of the user.

Opinion 04/2012 emphasised that third-party advertising does not fall under the exemption defined in CRITERION A or B. Therefore, device fingerprinting for the purpose of targeted advertising requires the consent of the user.

7.3. Use case: Network provision

The correct management of a network requires the transfer of certain information elements relating to each device on the network. For example, a Wi-Fi access point which manages the connection between wireless devices and a wired network will process unique and non-

[33] Article 29 Working Party, 2012. Opinion 04/2012 on Cookie Consent Exemption, pp. 10-11.

unique information elements such as the MAC address[34] and channel in order to correctly maintain connections and correctly route data packets.

Where the network provisioning requires information elements which store or gain access to information on the user's device then this will fall within scope of Article 5(3). Where this processing is required for the normal functioning of the network, then this would be exempt under CRITERION A.

The secondary use of an information element or device fingerprint for the purpose of tracking is not considered as "*for the sole purpose of carrying out the transmission of a communication over an electronic communications network*" or "*strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service*". When considering multi-purpose cookies in Opinion 04/2012, WP29 noted that "*tracking is very unlikely to meet CRITERION A or B*" thus if a third-party wishes to use a device fingerprint for multiple purposes it will only be "*exempted from consent if all the distinct purposes […] are individually exempted from consent*".

7.4. Use case: User access and control

An online service may intend to use device fingerprinting to support user access and control (i.e. in combination with a username and password). The device fingerprint can be used to ensure that an account is linked to a particular device such that the device acts as a second factor of authentication.

For example, a music subscription service only permits a user to access the service from a limited number of specific devices. If a user has used this device previously, the website operator can choose to perform fewer verification checks before providing access.

If a device fingerprint is comprised of information elements which store or gain access to information on the user's device then this will

[34] The MAC address will likely be unique across devices on the network. The MAC address prefix will refer also to the chip manufacturer.

fall within the scope of Article 5(3). Such purposes would however not be considered as "*strictly necessary*" to provide a functionality explicitly requested by the user and therefore valid user consent is required.

Website operators may need to consider a range of appropriate and proportionate controls or any other authentication method (e.g. a one-time password, secondary email confirmation).

7.5. Use case: User centric security

In Opinion 04/2012, WP29 stated that "*cookies set for the specific task of increasing security of the service that has been explicitly requested by the user*" (e.g. to detect repeated failed login attempts) would be exempt under CRITERION B.

This exemption would also apply to device fingerprinting but, as with cookies, "*not […] cover the use of the technique that relate to the security of websites or third party services that have not been explicitly requested by the user.*"

If data are collected via device fingerprinting to serve a user centric security purpose, in order to qualify for the consent exemption, they may not be used for any secondary purposes. Technical and organisational safeguards must be taken to prevent any secondary use of finger printing data, typically kept in server security logs.

7.6. Use case: Adapting the user interface to the device

Accessing device information such as the screen size can be useful to optimise the layout of content[35]. For example, a media website could switch to a low graphics mode or single column layout for mobile devices. Alternatively a website, or the third-parties serving content through that website, might query the device to ascertain technical capabilities such as which video formats are supported.

[35] Note that other less privacy instructive methods may exist to achieve this same objective such as using the User-Agent string.

Where a third-party requests access to information stored on the user's device for the sole purpose of adapting the content to the characteristics of the device, then CRITERION B is valid. This means that for short-term UI customisation consent is therefore not required.

If this information however is also used for secondary purposes, this exemption no longer applies.

8. Conclusion

This Opinion addresses the topic of device fingerprinting and the applicability of Article 5(3) of the ePrivacy Directive 2002/58/EC, as amended by Directive 2009/136/EC, without prejudice to the provisions of the Data Protection Directive 95/46/EC. This Opinion expands upon the earlier Opinion 04/2012 on Cookie Consent Exemption and confirms that, in a number of circumstances, the technology leads to the gaining of access to, or storing of, information on the user's terminal device. Thus Article 5(3) of the ePrivacy Directive also applies to instances of device fingerprinting.

Therefore, parties who wish to process device fingerprints which are generated through the gaining of access to, or the storing of, information on the user's terminal device must first obtain the valid consent of the user (unless an exemption applies).

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Informazioni sulle convinzioni religiose dei pazienti: i casi in cui possono essere raccolte durante il ricovero - 12 novembre 2014

http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3624070

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, in presenza del dott Antonello Soro, presidente, della dott.ssa Augusta Iannini, vice presidente, della dott.ssa Giovanna Bianchi Clerici e della prof.ssa Licia Califano, componenti e del dott. Giuseppe Busia, segretario generale;

VISTO il Codice in materia di protezione dei dati personali (d. lgs. 30 giugno 2003, n. 196, di seguito "Codice");

ESAMINATE le segnalazioni pervenute all'Autorità in merito alla prassi seguita in alcune strutture sanitarie del Servizio sanitario nazionale (Ssn) relativa alla somministrazione sistematica e preventiva ai pazienti, all'atto del ricovero, di questionari volti ad acquisire informazioni relative anche al credo religioso di appartenenza degli stessi;

VISTE le richieste di informazioni in atti;

VISTO schema tipo aggiornato di regolamento per il trattamento di dati personali sensibili e giudiziari da effettuarsi presso le regioni e le province autonome, le aziende sanitarie, gli enti e agenzie regionali/provinciali, gli enti vigilati dalle regioni e dalle province autonome, predisposto dalla Conferenza delle regioni e delle province autonome, sul quale il Garante ha espresso parere favorevole il 26 luglio 2012 (consultabile sul sito www.gpdp.it, doc. web n. 1915390).

VISTO il provvedimento generale circa il rispetto dei diritti, delle libertà fondamentali e della dignità degli interessati nell'erogazione

delle prestazioni da parte delle strutture sanitarie adottato dal Garante il 9 novembre 2005 (doc. web n. 1191411);

VISTA la normativa relativa ai servizi di assistenza religiosa nelle strutture sanitarie;

VISTO il codice di deontologia medica approvato dalla Federazione nazionale degli ordini dei medici chirurghi e degli odontoiatri il 18 maggio 2014;

VISTO il codice deontologico dell'infermiere approvato dal Comitato centrale della Federazione Ipasvi con deliberazione n.1 del 10 gennaio 2009 e dal Consiglio nazionale dei Collegi Ipasvi il 17 gennaio 2009;

VISTA la documentazione in atti;

VISTE le osservazioni dell'Ufficio, formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante, n. 1/2000;

RELATORE la dott.ssa Augusta Iannini;

PREMESSO

Sono pervenute alcune segnalazioni nelle quali si lamenta una presunta violazione delle disposizioni in materia di protezione dei dati personali in relazione alla prassi seguita da molte strutture del Ssn relativa alla somministrazione sistematica ai pazienti, all'atto del ricovero, di un questionario nel quale è richiesto di rispondere ad alcune domande tra le quali figura la seguente: “Qual è la sua religione?”.

In merito a quanto segnalato, l’Ufficio ha provveduto ad avviare un'istruttoria, al fine di comprendere le motivazioni che renderebbero indispensabile per le strutture sanitarie del Ssn acquisire in modo sistematico e preventivo il dato relativo al credo religioso di appartenenza di tutti i pazienti all'atto del loro ricovero.

Dalle informazioni acquisite, è emerso che la rilevazione di informazioni relative al credo religioso dell’interessato all'atto del ricovero è effettuata dalle strutture sanitarie del Ssn, in modo sistematico e preventivo, per assicurare al paziente un'assistenza

personalizzata con specifico riferimento al regime alimentare, alla possibilità di dedicarsi a momenti di preghiera o di ricevere un conforto da un religioso, nonché al rifiuto a sottoporsi ad alcune pratiche mediche (es. quelle trasfusionali).

Nell'ambito delle attività istruttorie svolte dall'Ufficio è emerso che tale prassi è seguita in molte strutture sanitarie di ricovero appartenenti al Ssn.

OSSERVA

1. Premessa

La struttura sanitaria è titolare del trattamento dei dati personali effettuato durante l'erogazione della prestazione sanitaria (artt. 7 comma 1, lett. f) e 28 del Codice). Nell'ambito dello svolgimento delle attività di cura la struttura sanitaria raccoglie legittimamente numerose informazioni personali, anche di carattere sensibile, dei soggetti dalla stessa assistiti.

Prima ancora di procedere all'attività di cura dell'interessato quest'ultimo deve ricevere una completa informativa sul trattamento dei dati personali che lo riguardano, e -fermi restando i casi di prestazioni d'urgenza- rilasciare il consenso, anche in forma orale, purché documentato per iscritto da parte dell'esercente la professione sanitaria (artt. 13 e 75 e ss. del Codice). Nell'informativa devono essere specificati, tra l'altro, i dati personali il cui conferimento risulti obbligatorio e quali, invece, facoltativo in relazione alle diverse finalità perseguite, avendo cura di precisare anche le conseguenze di un eventuale rifiuto al conferimento degli stessi (art. 13, comma 1, lett. b) e c) del Codice).

In ogni caso, il trattamento dei dati personali deve uniformarsi ai princìpi di pertinenza e non eccedenza in relazione alle finalità legittimamente perseguite; nel rispetto di tali principi occorre, pertanto, circoscrivere il trattamento ai soli dati personali che siano, caso per caso, strettamente necessari (art. 11 del Codice). In particolare, per quanto riguarda le informazioni di carattere sensibile,

assume ancor più rilievo la verifica dell'essenzialità e della indispensabilità dei dati trattati (art. 22 del Codice).

Tra i dati sensibili si annoverano anche quelli idonei a rivelare le convinzioni religiose dell'interessato (art. 4, comma 1, lett. d) del Codice).

Alla luce dei principi suesposti, il Garante ritiene necessario procedere ad un esame delle fattispecie nell'ambito delle quali la raccolta del dato relativo alla religione di appartenenza dell'interessato risulta indispensabile al fine di erogare allo stesso prestazioni in ambito medico aderenti alle sue convinzioni religiose.

2. Libertà di preghiera, assistenza religiosa e spirituale in ospedale e servizi necroscopici

L'ordinamento giuridico riconosce al paziente il diritto a richiedere un'assistenza religiosa e spirituale durante il ricovero (cfr., in particolare, art. 35 del d.P.R. 27 marzo 1969, n.128 "Ordinamento interno dei servizi ospedalieri", art. 6 della legge 11 agosto 1984, n. 449 "Norme per la regolazione dei rapporti tra lo Stato e le Chiese rappresentate dalla Tavola Valdese", art. 11 della legge 25 marzo 1985, n. 121 "Ratifica ed esecuzione accordo con prot. addizionale, firmato a Roma il 18.12.1984 che apporta modificazioni al Concordato Lateranense", art. 8 della legge 22 novembre 1988, n. 516 "Norme per la regolazione dei rapporti tra lo Stato e l'Unione italiana delle Chiese Cristiane avventiste del 7° giorno", art.4 della legge 22 novembre 1988, n.517 "Norme per la regolazione dei rapporti tra lo Stato e le Assemblee di Dio in Italia", art. 9 della legge 8 marzo 1989, n. 101"Norme per la regolazione dei rapporti tra lo Stato e l'Unione delle Comunità ebraiche italiane", art. 6 della legge 12 aprile 1995, n. 116: "Norme per la regolazione dei rapporti tra lo Stato e l'Unione Cristiana Evangelica Battista d'Italia", art. 6 della legge 29 novembre 1995, n. 520 "Norme per la regolazione dei rapporti tra lo Stato e la Chiesa Evangelica Luterana in Italia, art. 5 della legge 30 luglio 2012, n. 126 "Norme per la regolazione dei rapporti tra lo Stato e la Sacra arcidiocesi ortodossa d'Italia ed Esarcato per l'Europa Meridionale, in attuazione dell'articolo 8, terzo comma, della Costituzione", art. 9

della legge 30 luglio 2012, n. 127 "Norme per la regolazione dei rapporti tra lo Stato e la Chiesa di Gesù Cristo dei Santi degli ultimi giorni, in attuazione dell'articolo 8 della Costituzione", art.6 della legge 30 luglio 2012, n. 128 "Norme per la regolazione dei rapporti tra lo Stato e la Chiesa apostolica in Italia, in attuazione dell'articolo 8, terzo comma, della Costituzione", art. 5 della legge 31 dicembre 2012 n. 245 "Norme per la regolazione dei rapporti tra lo Stato e l'Unione Buddhista Italiana, in attuazione dell'articolo 8, terzo comma, della Costituzione", art.5 della legge 31 dicembre 2012 n. 246 "Norme per la regolazione dei rapporti tra lo Stato e l'Unione Induista Italiana, Sanatana Dharma Samgha, in attuazione dell'articolo 8, terzo comma, della Costituzione". Anche nell'elenco dei diritti del paziente da indicare nelle carte dei servizi pubblici sanitari proclamate a livello locale dalle aziende sanitarie si configura il diritto "ad avere il rispetto per la propria fede e alla assistenza religiosa, se richiesta" (allegato 8, punto 44 del d.P.C.M. 19 maggio 1995 "Schema generale di riferimento per la Carta dei servizi pubblici sanitari", cfr. anche art. 4 del codice deontologico dell'infermiere del 10 gennaio 2009).

La valutazione circa l'indispensabilità del dato relativo alla religione di appartenenza dell'interessato ai fini dell'erogazione dell'assistenza religiosa e spirituale in ospedale e della realizzazione dei servizi necroscopici è stata già effettuata dal Garante nell'ambito dell'istruttoria per il rilascio del parere sul citato schema tipo di regolamento per i trattamenti dei dati sensibili e giudiziari di competenza delle regioni e delle province autonome, delle aziende sanitarie, degli enti e agenzie regionali/provinciali, nonché degli enti vigilati dalle regioni e dalle province autonome (cfr. predetto parere del Garante 26 luglio 2012). In tale schema tipo di regolamento è previsto che le strutture sanitarie possano raccogliere i dati relativi alle convinzioni religiose dell'interessato qualora la raccolta di tali informazioni sia finalizzata a garantire ai ricoverati l'assistenza religiosa e spirituale tramite i ministri di culto delle diverse confessioni religiose (bisogno di conforto o di sacramento al letto) (cfr. scheda n. 17 del predetto schema tipo di regolamento). In tal caso, tali informazioni possono essere comunicate verbalmente al personale di reparto dall'interessato stesso o da un suo familiare; detto

personale provvederà a trasmettere alla direzione sanitaria le richieste di assistenza religiosa e spirituale proveniente da infermi di qualunque religione (cfr. art. 35, comma 4 del d.P.R. 27 marzo 1969, n.128 "Ordinamento interno dei servizi ospedalieri").

Il predetto schema tipo di regolamento prevede, inoltre, che i medesimi dati possano essere lecitamente raccolti da parte della struttura sanitaria anche con riferimento ai trattamenti effettuati nell'ambito del servizio necroscopico, ai fini della preparazione della salma (cfr. scheda n. 17 citata; cfr. allegato 1, punto 1.3 del d.P.C.M. 29-11-2001 "Definizione dei livelli essenziali di assistenza").

Le strutture sanitarie possono, pertanto, lecitamente trattare le informazioni idonee a rilevare le convinzioni religiose dell'interessato laddove quest'ultimo richieda di usufruire dell'assistenza religiosa e spirituale durante il ricovero, ovvero nei casi in cui ciò si rilevi indispensabile durante l'esecuzione dei servizi necroscopici per rispettare specifiche volontà espresse in vita dall'interessato. Tale raccolta di dati sensibili non deve avvenire, quindi, in maniera sistematica e preventiva, bensì solo su richiesta dell'interessato o, qualora lo stesso sia impossibilitato, di un terzo legittimato, quale, ad esempio, un familiare, un parente o un convivente.

3. Regimi alimentari, rifiuto di particolari condotte terapeutiche

L'ordinamento giuridico riconosce al paziente il diritto ad "essere assistito e curato con premura ed attenzione, nel rispetto della dignità umana e delle proprie convinzioni filosofiche e religiose" (cfr., fra l’altro, art. 1, all. n. 7, del d.P.C.M. 19 maggio 1995 "Schema generale di riferimento per la Carta dei servizi pubblici sanitari"). Tale diritto si esplicita anche nella facoltà per l'interessato di esprimere durante un ricovero specifiche preferenze alimentari o il rifiuto di sottoporsi a particolari condotte terapeutiche (ad es. rifiuto alla terapia trasfusionale, cfr. art. 7 d.m. 1-9-1995 "Disciplina dei rapporti tra le strutture pubbliche provviste di servizi trasfusionali e quelle pubbliche e private, accreditate e non accreditate, dotate di frigoemoteche"; con riferimento al dovere deontologico del medico di astenersi, nel rispetto delle volontà espresse dal paziente, dall'ostinazione in trattamenti

diagnostici e terapeutici da cui non si possa fondatamente attendere un beneficio per la salute del malato e/o un miglioramento della qualità della vita, cfr. art. 16 del Codice di deontologia medica del 18 maggio 2014).

Sebbene nel citato schema tipo di regolamento per il trattamento dei dati sensibili e giudiziari sia previsto che le strutture sanitarie possano raccogliere i dati relativi alle convinzioni religiose dell'interessato nell'ambito dell'assistenza ospedaliera in regime di ricovero, l'Autorità -durante i lavori preparatori del citato schema tipo- ha ritenuto tale raccolta di dati sensibili indispensabile solo se finalizzata a garantire ai pazienti l'assistenza religiosa e spirituale e, nell'ambito del servizio necroscopico, ai fini della preparazione della salma. Nella citata scheda 17 del predetto schema tipo di regolamento, infatti, il trattamento dei dati idonei a rivelare le convinzioni religiose è previsto solo per l'attività di assistenza spirituale e religiosa e in ambito necroscopico e non anche con riferimento al regime alimentare da offrire al paziente e all'eventuale rifiuto di questo a specifici trattamenti medici (cfr., in particolare, la parte descrittiva della predetta scheda).

La finalità di assicurare un regime alimentare aderente alla volontà espressa dall'interessato, nonché quella di rispettare le scelte terapeutiche espresse in modo consapevole dall'interessato (ad es. rifiuto al trattamento trasfusionale nell'ambito dell'espressione del diritto ad un autodeterminazione terapeutica)- alla luce dei richiamati principi di indispensabilità- possono essere, infatti, utilmente perseguite dalle strutture sanitarie senza raccogliere l'informazione relativa alle religione di appartenenza dell'interessato. Al paziente deve essere, pertanto, consentito di esprimere tali volontà, senza che siano raccolte le eventuali motivazioni religiose che ne sono alla base.

Sotto altro profilo, resta fermo che la struttura sanitaria, nel raccogliere legittimamente il consenso o l'eventuale diniego del paziente ad uno specifico trattamento sanitario (art. 32 della Costituzione), non debba acquisire le informazioni relative al credo religioso sottese a tale scelta.

Il presente provvedimento è pubblicato sul sito Internet del Garante (www.gpdp.it) e, considerata la sua valenza generale, è inviato alle regioni e province autonome affinché provvedano a divulgarlo presso le aziende sanitarie competenti.

TUTTO CIÒ PREMESSO IL GARANTE

1. ai sensi dell'art. 154, comma 1, lett. c) del Codice prescrive alle strutture sanitarie del Ssn, entro 6 mesi dalla data di adozione del presente provvedimento, di adeguare la raccolta delle informazioni relative alla religione di appartenenza dell'interessato a quanto indicato nei punti 2 e 3 del presente provvedimento;

2. ai sensi dell'art. 154, comma 1, lett. h) del Codice dispone che il presente provvedimento sia inviato alle regioni e province autonome affinché provvedano a divulgarlo presso le strutture sanitarie del Servizio sanitario nazionale.
Ai sensi degli artt. 152 del Codice e 10 del d.lgs. n. 150/2011, avverso il presente provvedimento può essere proposta opposizione all'Autorità giudiziaria ordinaria, con ricorso depositato al tribunale ordinario del luogo ove ha la residenza il titolare del trattamento dei dati, entro il termine di trenta giorni dalla data di comunicazione del provvedimento stesso, ovvero di sessanta giorni se il ricorrente risiede all’estero.

Roma, 12 novembre 2014

IL PRESIDENTE
Soro

IL RELATORE
Iannini

IL SEGRETARIO GENERALE
Busia

Provvedimento generale prescrittivo in tema di biometria - 12 novembre 2014

in *G. U.* n. 280 del 2 dicembre 2014

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del dott. Antonello Soro, presidente, della dott.ssa Augusta Iannini, vice presidente, della dott.ssa Giovanna Bianchi Clerici e della prof.ssa Licia Califano, componenti, e del dott. Giuseppe Busia, segretario generale;

VISTO il Codice in materia di protezione dei dati personali (d.lgs. 30 giugno 2003, n. 196, di seguito "Codice");

VISTO il Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE, pubblicato in G.U.U.E. 2014 L 257, p. 73 (cd. Regolamento eIDAS);

RILEVATO l'elevato numero di notificazioni presentate al Garante relative al trattamento di dati biometrici;

CONSIDERATO che l'evoluzione delle tecnologie biometriche ha generato una significativa diffusione della loro applicazione e ne è prevedibile una ulteriore espansione per il perseguimento di diverse finalità nei più svariati ambiti della società;

VISTE le richieste di verifica preliminare presentate ai sensi dell'art. 17 del Codice in ordine al trattamento dei dati personali effettuati tramite l'utilizzo di tecniche biometriche;

RITENUTA l'opportunità di rendere disponibile un quadro unitario di misure e accorgimenti di carattere tecnico, organizzativo e procedurale per conformare i trattamenti di dati biometrici alla vigente disciplina sulla protezione dei dati personali e per accrescerne i livelli di sicurezza;

RITENUTO, in ragione della specificità dei dati biometrici, di dovere assoggettare il loro trattamento a un regime generale di obbligatoria comunicazione delle eventuali violazioni;

RITENUTA inoltre l'esigenza di individuare, ai sensi dell'art. 17 del Codice, opportune cautele da porre a garanzia degli interessati in relazione ad alcune tipologie di trattamenti di dati biometrici, anche alla luce delle attuali conoscenze tecniche, che potranno essere effettuate senza richiesta di verifica preliminare rivolta al Garante;

VISTE le osservazioni dell'Ufficio formulate dal Segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

RELATORE la dott.ssa Augusta Iannini;

1. PREMESSA

L'utilizzo di dispositivi e tecnologie per la raccolta e il trattamento di dati biometrici è soggetto a una crescente diffusione, in particolare per l'accertamento dell'identità personale nell'ambito dell'erogazione di servizi della società dell'informazione e dell'accesso a banche dati informatizzate, per il controllo degli accessi a locali e aree, per l'attivazione di dispositivi elettromeccanici ed elettronici, anche di uso personale, o di macchinari, nonché per la sottoscrizione di documenti informatici.

Tale diffusione ha suscitato la massima attenzione delle autorità di protezione dati, testimoniata anche dall'elaborazione di pareri da parte del Working Party Article 29 (WP29) che costituiscono un significativo punto di riferimento per ogni analisi e studio del fenomeno. I dati biometrici sono infatti dati personali, poiché possono sempre essere considerati come "informazione concernente una persona fisica identificata o identificabile (...)" prendendo in considerazione "l'insieme dei mezzi che possono essere ragionevolmente utilizzati dal responsabile del trattamento o da altri per identificare detta persona". Essi rientrano quindi nell'ambito di applicazione del Codice (art. 4, comma 1, lettera b), e le operazioni su essi compiute con strumenti elettronici sono a tutti gli effetti

trattamenti nel senso delineato dalla disciplina sulla protezione dei dati personali.

Sono considerati dati biometrici nel presente contesto, coerentemente con i pareri del WP29, i campioni biometrici, i modelli biometrici, i riferimenti biometrici e ogni altro dato ricavato con procedimento informatico da caratteristiche biometriche e che possa essere ricondotto, anche tramite interconnessione ad altre banche dati, a un interessato individuato o individuabile.

2. LINEE-GUIDA IN MATERIA DI RICONOSCIMENTO BIOMETRICO E FIRMA GRAFOMETRICA

Il Garante è intervenuto più volte, a seguito di specifiche richieste di verifica preliminare ai sensi dell'art. 17 del Codice, con provvedimenti che hanno in alcuni casi negato e in altri ammesso, nel rispetto di prescrizioni di natura tecnica od organizzativa, i trattamenti sottoposti alla valutazione dell'Autorità.

A fronte della complessità della materia in rapporto alla disciplina sul trattamento dei dati personali, con l'adozione delle "Linee-guida in materia di riconoscimento biometrico e firma grafometrica" (allegato "A"), che formano parte integrante del presente provvedimento, il Garante intende fornire un quadro di riferimento unitario sulla cui base i titolari possano orientare le proprie scelte tecnologiche, conformare i trattamenti ai principi di legittimità stabiliti dal Codice, rispettare elevati standard di sicurezza.

Le linee-guida introducono altresì la terminologia essenziale per la descrizione degli aspetti tecnologici, con il ricorso a standard internazionali, e individuano i principali profili di rischio associati al trattamento di dati biometrici.

3. COMUNICAZIONE DI VIOLAZIONE DEI DATI BIOMETRICI

Le peculiari caratteristiche dei dati biometrici, unitamente ai rischi su di essi incombenti illustrati nelle linee-guida, fanno ritenere necessario assoggettare il loro trattamento, anche in coerenza con le previsioni

del Regolamento europeo eIDAS in tema di identificazione, autenticazione e firma elettronica, all'obbligo di comunicare al Garante il verificarsi di violazioni dei dati (data breach) o incidenti informatici (accessi abusivi, azione di malware…) che, pur non avendo un impatto diretto su di essi, possano comunque esporli a rischi di violazione.

A questo fine, entro ventiquattro ore dalla conoscenza del fatto i titolari comunicano all'Autorità tutte le violazioni dei dati o gli incidenti informatici che possano avere un impatto significativo sui sistemi biometrici o sui dati personali ivi custoditi. Tali comunicazioni devono essere redatte secondo lo schema riportato nell'allegato "B" al presente provvedimento e quindi inviate tramite posta elettronica o posta elettronica certificata all'indirizzo: databreach.biometria@pec.gpdp.it

4. ESONERO DALLA VERIFICA PRELIMINARE DI CUI ALL'ART. 17 DEL CODICE

I dati biometrici sono, per loro natura, direttamente, univocamente e in modo tendenzialmente stabile nel tempo, collegati all'individuo e denotano la profonda relazione tra corpo, comportamento e identità della persona, richiedendo particolari cautele in caso di loro trattamento. L'adozione di sistemi biometrici, in ragione della tecnica prescelta, del contesto di utilizzazione, del numero e della tipologia di potenziali interessati, delle modalità e delle finalità del trattamento, può comportare quindi rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato.

In ragione di ciò, qualora si intenda provvedere al trattamento di dati biometrici, è necessario presentare al Garante una richiesta di verifica preliminare, ai sensi dell'art. 17 del Codice.

Sulla base dell'esperienza maturata, però, il Garante ha ritenuto di individuare, con il presente provvedimento, talune tipologie di trattamento volte a scopi di riconoscimento biometrico (nella forma di identificazione biometrica o di verifica biometrica) o di sottoscrizione di documenti informatici (firma grafometrica) che, in considerazione

delle specifiche finalità perseguite, della tipologia dei dati trattati e delle misure di sicurezza che possono essere concretamente adottate a loro protezione, presentano un livello di rischio ridotto.

In relazione a tali specifiche tipologie di trattamenti non è quindi necessario per i titolari presentare la predetta istanza, a condizione che vengano adottate tutte le misure e gli accorgimenti tecnici idonei a raggiungere gli obiettivi di sicurezza individuati con il presente provvedimento e siano rispettati i presupposti di legittimità contenuti nel Codice e richiamati nel capitolo 4 delle linee-guida (con particolare riferimento ai principi generali di liceità, finalità, necessità e proporzionalità dei trattamenti, e agli adempimenti giuridici quali l'obbligo di informativa agli interessati e di notificazione al Garante).

Il Garante si riserva di prevedere, alla luce dell'esperienza maturata e dell'evoluzione tecnologica, ulteriori ipotesi di esonero.

Le indicazioni relative al trattamento dei dati biometrici contenute nei precedenti provvedimenti del Garante (si vedano, ad esempio, le linee guida in materia di trattamento di dati personali per finalità di gestione del rapporto di lavoro alle dipendenze di datori di lavoro privati e pubblici (doc. web n. 1364939 e n. 1417809) continuano ad applicarsi in quanto compatibili con le previsioni del presente provvedimento.

I provvedimenti specifici di verifica preliminare sui quali il Garante ha già espresso le proprie valutazioni non dovranno essere oggetto di ulteriori istanze.

I titolari dei trattamenti biometrici in relazione ai quali è previsto l'esonero dalla verifica preliminare, che abbiano già presentato istanza ex art. 17 del Codice alla data di pubblicazione del presente provvedimento sulla Gazzetta Ufficiale della Repubblica Italiana, sono tenuti a comunicare al Garante, entro trenta giorni dalla stessa data, la conformità del trattamento alle prescrizioni ivi contenute ovvero la propria intenzione di conformarvisi. La presentazione della comunicazione comporta il non luogo a provvedere sulle relative istanze.

Le istanze di verifica preliminare in relazione alle quali non sia stata presentata la comunicazione di cui al periodo che precede verranno invece valutate dal Garante secondo le ordinarie procedure.

4.1 Autenticazione informatica

Le caratteristiche biometriche possono essere utilizzate come credenziali di autenticazione per l'accesso a banche dati e sistemi informatici, laddove è richiesta maggior certezza nell'identificazione degli utenti per particolari profili di rischio relativi alle informazioni trattate e alla tipologia di risorse informatiche impiegate. Appartengono a tale ambito, ad esempio, le infrastrutture critiche informatiche di cui al D.M. 9 gennaio 2008 del Ministro dell'interno (G.U. n. 101 del 30 aprile 2008).

In questi casi il presupposto di legittimità, che in ambito pubblico è dato dal perseguimento delle finalità istituzionali del titolare, in ambito privato viene individuato nell'istituto del bilanciamento di interessi (art. 24, comma 1, lettera g), del Codice) per cui, in ragione del legittimo interesse perseguito dal titolare, delle prescrizioni imposte dal presente provvedimento, delle finalità connesse a specifiche esigenze di sicurezza commisurate ai rischi incombenti sui dati o sui sistemi informatici che la procedura di autenticazione è destinata a proteggere, anche tenuto conto delle indicazioni normative in materia di misure minime di sicurezza delle banche dati, il trattamento dei dati biometrici può avvenire senza il consenso degli interessati.

Quindi i titolari sono esonerati dall'obbligo di presentare istanza di verifica preliminare se il trattamento è svolto nel rispetto delle seguenti prescrizioni:

a) Le caratteristiche biometriche consistono nell'impronta digitale o nell'emissione vocale.

b) Nel caso di utilizzo dell'impronta digitale, il dispositivo di acquisizione ha la capacità di rilevare la c.d. vivezza.

c) Nel caso di utilizzo dell'emissione vocale, tale caratteristica è utilizzata esclusivamente in combinazione con altri fattori di

autenticazione e con accorgimenti che escludano i rischi di utilizzo fraudolento di eventuali registrazioni della voce (prevedendo, per esempio, la ripetizione da parte dell'interessato di parole o frasi proposte nel corso della procedura di riconoscimento).

d) La cancellazione dei dati biometrici grezzi ha luogo immediatamente dopo la loro trasformazione in campioni o in modelli biometrici.

e) I dispositivi per l'acquisizione iniziale (enrolment) e quelli per l'acquisizione nel corso dell'ordinario funzionamento sono direttamente connessi oppure integrati nei sistemi informatici che li utilizzano, siano essi postazioni di enrolment ovvero postazioni di lavoro o sistemi server protetti con autenticazione biometrica.

f) Le trasmissioni di dati tra i dispositivi di acquisizione e i sistemi informatici sono rese sicure con l'ausilio di tecniche crittografiche caratterizzate dall'utilizzo di chiavi di cifratura di lunghezza adeguata alla dimensione e al ciclo di vita dei dati.

g) Nel caso in cui i riferimenti biometrici siano conservati in modalità sicura su supporti portatili (smart card o analogo dispositivo sicuro) dotati di adeguate capacità crittografiche e certificati per le funzionalità richieste in conformità alla norma tecnica ISO/IEC 15408 o FIPS 140-2 almeno level 3:

i. il supporto è rilasciato in un unico esemplare, è nell'esclusiva disponibilità dell'interessato e, in caso di cessazione dei diritti di accesso ai sistemi informatici, è restituito e distrutto con procedura formalizzata;

ii. l'area di memoria in cui sono conservati i dati biometrici è resa accessibile ai soli lettori autorizzati e protetta da accessi non autorizzati;

iii. i campioni o i riferimenti biometrici sono cifrati con tecniche crittografiche con lunghezza delle chiavi adeguata alla dimensione e al ciclo di vita dei dati.

h) Nel caso di conservazione del campione o del riferimento biometrico sul sistema informatico protetto con autenticazione biometrica:

i. è assicurata, tramite idonei sistemi di raccolta dei log, la registrazione degli accessi da parte degli amministratori di sistema ai sistemi informatici;

ii. sono adottate idonee misure e accorgimenti tecnici per contrastare i rischi di installazione di software e di modifiche della configurazione dei sistemi informatici, se non esplicitamente autorizzati;

iii. i sistemi informatici sono protetti contro l'azione di malware;

iv. sono adottate misure e accorgimenti volti a ridurre i rischi di manomissione e accesso fraudolento al dispositivo di acquisizione;

v. i campioni o i riferimenti biometrici sono cifrati con tecniche crittografiche con lunghezza delle chiavi adeguata alla dimensione e al ciclo di vita dei dati;

vi. i campioni o i riferimenti biometrici sono conservati per il tempo strettamente necessario a realizzare le finalità del sistema biometrico;

vii. i campioni o i riferimenti biometrici sono conservati separatamente dai dati identificativi degli interessati;

viii. sono previsti meccanismi di cancellazione automatica dei dati, cessati gli scopi per i quali sono stati raccolti e trattati.

i) E' esclusa la realizzazione di archivi biometrici centralizzati.

j) E' predisposta una relazione che descrive gli aspetti tecnici e organizzativi delle misure messe in atto dal titolare, fornendo altresì la valutazione della necessità e della proporzionalità del trattamento biometrico. Tale relazione è conservata aggiornata, con verifica di controllo almeno annuale, per tutto il periodo di esercizio del sistema biometrico e mantenuta a disposizione del Garante.

I titolari dotati di certificazione del sistema di gestione per la sicurezza delle informazioni (SGSI) secondo la norma tecnica ISO/IEC 27001

che inseriscono il sistema biometrico nel campo di applicazione della certificazione sono esentati dall'obbligo di redigere la relazione di cui al precedente periodo, potendo utilizzare la documentazione prodotta nell'ambito della certificazione, integrandola con la valutazione della necessità e della proporzionalità del trattamento biometrico.

4.2 Controllo di accesso fisico ad aree "sensibili" dei soggetti addetti e utilizzo di apparati e macchinari pericolosi

L'adozione di sistemi biometrici basati sull'elaborazione dell'impronta digitale o della topografia della mano può essere consentita per limitare l'accesso ad aree e locali ritenuti "sensibili" in cui è necessario assicurare elevati e specifici livelli di sicurezza oppure per consentire l'utilizzo di apparati e macchinari pericolosi ai soli soggetti qualificati e specificamente addetti alle attività.

Appartengono a tale ambito, in particolare:

• le aree destinate allo svolgimento di attività aventi carattere di particolare segretezza, ovvero prestate da personale selezionato e impiegato in specifiche mansioni che comportano la necessità di trattare informazioni riservate e applicazioni critiche;

• le aree in cui sono conservati oggetti di particolare valore o la cui disponibilità è ristretta a un numero circoscritto di addetti;

• le aree preposte alla realizzazione o al controllo di processi produttivi pericolosi che richiedono un accesso selezionato da parte di personale particolarmente esperto e qualificato;

• l'utilizzo di apparati e macchinari pericolosi, laddove sia richiesta una particolare destrezza onde scongiurare infortuni e danni a cose o persone.

In questi casi il presupposto di legittimità, che in ambito pubblico è dato dal perseguimento delle finalità istituzionali del titolare, in ambito privato viene individuato nell'istituto del bilanciamento di interessi (art. 24, comma 1, lettera g), del Codice) per cui, in ragione del legittimo interesse perseguito dal titolare, delle prescrizioni imposte dal presente provvedimento e delle finalità connesse a

specifiche esigenze di sicurezza, il trattamento può avvenire senza il consenso degli interessati.

In relazione a tali finalità, il titolare è esonerato dall'obbligo di presentare istanza di verifica preliminare se il trattamento è svolto nel rispetto delle seguenti prescrizioni:

a) Le caratteristiche biometriche consistono nell'impronta digitale o nella topografia della mano.

b) Nel caso di utilizzo dell'impronta digitale, il dispositivo di acquisizione ha la capacità di rilevare la c.d. vivezza.

c) La cancellazione dei dati biometrici grezzi e dei campioni biometrici ha luogo immediatamente dopo la loro trasformazione in modelli biometrici.

d) I dispositivi per l'acquisizione iniziale e quelli per l'acquisizione nel corso dell'ordinario funzionamento sono direttamente connessi o integrati, rispettivamente, nelle postazioni informatiche di enrolment e nelle postazioni di controllo ai varchi di accesso.

e) Le trasmissioni di dati tra i dispositivi di acquisizione e le postazioni di lavoro o le postazioni di controllo sono rese sicure con l'ausilio di tecniche crittografiche caratterizzate dall'utilizzo di chiavi di cifratura con lunghezza adeguata alla dimensione e al ciclo di vita dei dati.

f) Nel caso di esclusiva conservazione del riferimento biometrico in modalità sicura su supporti portatili (smart card o analogo dispositivo sicuro) dotati di adeguate capacità crittografiche e certificati per le funzionalità richieste in conformità alla norma tecnica ISO/IEC 15408 o FIPS 140-2 almeno level 3:

i. il supporto è rilasciato in un unico esemplare, è nell'esclusiva disponibilità dell'interessato e, in caso di cessazione dei diritti di accesso alle aree sensibili, è restituito e distrutto con procedura formalizzata;

ii. l'area di memoria in cui sono conservati i dati biometrici è accessibile ai soli lettori autorizzati ed è protetta da accessi non autorizzati;

iii. il riferimento biometrico è cifrato con tecniche crittografiche con lunghezza delle chiavi adeguata alla dimensione e al ciclo di vita dei dati.

g) Nel caso di conservazione del riferimento biometrico su un dispositivo-lettore o una postazione informatica dedicata (controller di varco) dotata di misure di sicurezza di cui alla precedente lettera e):

i. è assicurata la registrazione degli accessi alla postazione da parte degli amministratori di sistema, tramite idonei sistemi di raccolta dei log;

ii. sono adottate idonee misure e accorgimenti tecnici per contrastare i rischi di installazione di software e di modifica della configurazione della postazione informatica, se non esplicitamente autorizzati;

iii. i sistemi informatici sono protetti contro l'azione di malware e sono, inoltre, adottati sistemi di firewall per la protezione perimetrale della rete e contro i tentativi di accesso abusivo ai dati;

iv. sono adottate misure e accorgimenti volti a ridurre i rischi di manomissione e accesso fraudolento al dispositivo di acquisizione;

v. il riferimento biometrico è cifrato con tecniche crittografiche con lunghezza delle chiavi adeguata alla dimensione e al ciclo di vita dei dati;

vi. i riferimenti biometrici sono conservati per il tempo strettamente necessario a realizzare le finalità del sistema biometrico;

vii. i riferimenti biometrici sono conservati separatamente dai dati identificativi degli interessati;

viii. sono previsti meccanismi di cancellazione automatica dei dati, cessati gli scopi per i quali sono stati raccolti e trattati.

h) E' esclusa la realizzazione di archivi biometrici centralizzati.

i) E' predisposta una relazione che descrive gli aspetti tecnici e organizzativi delle misure messe in atto dal titolare, fornendo altresì la valutazione della necessità e della proporzionalità del trattamento biometrico. Tale relazione tecnica è conservata aggiornata, con

verifica di controllo almeno annuale, per tutto il periodo di esercizio del sistema biometrico e mantenuta a disposizione del Garante.

I titolari dotati di certificazione del sistema di gestione per la sicurezza delle informazioni (SGSI) secondo la norma tecnica ISO/IEC 27001 che inseriscono il sistema biometrico nel campo di applicazione della certificazione sono esentati dall'obbligo di redigere la relazione di cui al precedente periodo, potendo utilizzare la documentazione prodotta nell'ambito della certificazione, integrandola con la valutazione della necessità e della proporzionalità del trattamento biometrico.

4.3 Uso dell'impronta digitale o della topografia della mano a scopi facilitativi

Le tecniche biometriche possono anche prestarsi a essere utilizzate per consentire, regolare e semplificare l'accesso fisico di utenti ad aree fisiche in ambito pubblico (es. biblioteche) o privato (es. aree aeroportuali riservate) o a servizi.

In questi casi il presupposto di legittimità del trattamento dei dati biometrici è dato dal consenso effettivamente libero degli interessati e dall'utilizzo di sistemi alternativi di accesso non basati su dati biometrici.

Il titolare è esonerato dall'obbligo di presentare istanza di verifica preliminare se il trattamento è svolto nel rispetto delle seguenti prescrizioni:

a) Le caratteristiche biometriche consistono nell'impronta digitale o nella topografia della mano.

b) La cancellazione dei dati biometrici grezzi e dei campioni biometrici ha luogo immediatamente dopo la loro raccolta e trasformazione in modelli biometrici.

c) I dispositivi per l'acquisizione iniziale e quelli per l'acquisizione nel corso dell'ordinario funzionamento sono direttamente connessi o integrati, rispettivamente, nelle postazioni informatiche di enrolment e nelle postazioni di controllo o nei dispositivi di acquisizione.

d) Le trasmissioni di dati tra i dispositivi di acquisizione e le altre componenti del sistema biometrico sono rese sicure con l'ausilio di tecniche crittografiche con lunghezza delle chiavi adeguata alla dimensione e al ciclo di vita dei dati.

e) Nel caso di esclusiva conservazione del riferimento biometrico in modalità sicura su supporti portatili (smart card o analogo dispositivo sicuro) dotati di adeguate capacità crittografiche e certificati per le funzionalità richieste in conformità alla norma tecnica ISO/IEC 15408 o FIPS 140-2 almeno level 3:

i. il supporto è rilasciato in un unico esemplare, è nell'esclusiva disponibilità dell'interessato e, in caso di cessazione dei diritti di accesso, è restituito e distrutto con procedura formalizzata;

ii. l'area di memoria in cui sono conservati i riferimenti biometrici è accessibile ai soli lettori autorizzati ed è protetta da accessi non autorizzati;

iii. il riferimento biometrico è cifrato con tecniche crittografiche con lunghezza delle chiavi adeguata alla dimensione e al ciclo di vita dei dati.

f) Nel caso di conservazione del riferimento biometrico su un dispositivo-lettore o su postazioni informatiche:

i. è assicurata la registrazione degli accessi alla postazione da parte degli amministratori di sistema, tramite idonei sistemi di raccolta dei log;

ii. sono adottate idonee misure e accorgimenti tecnici per contrastare i rischi di installazione di software e di modifica della configurazione dei dispositivi o delle postazioni informatiche, se non esplicitamente autorizzati;

iii. sono adottate misure e accorgimenti volti a ridurre i rischi di manomissione e accesso fraudolento al dispositivo di acquisizione;

iv. il riferimento biometrico è cifrato con tecniche crittografiche con lunghezza delle chiavi adeguata alla dimensione e al ciclo di vita dei dati;

v. i riferimenti biometrici sono conservati per il tempo strettamente necessario a realizzare le finalità del sistema biometrico;

vi. i riferimenti biometrici sono conservati separatamente dai dati identificativi degli interessati.

g) È esclusa la realizzazione di archivi biometrici centralizzati.

h) É predisposta una relazione che descrive gli aspetti tecnici e organizzativi delle misure messe in atto dal titolare, fornendo altresì la valutazione della necessità e della proporzionalità del trattamento biometrico rispetto ai suoi fini facilitativi. Tale relazione tecnica è conservata aggiornata, con verifica di controllo almeno annuale, per tutto il periodo di esercizio del sistema biometrico e mantenuta a disposizione del Garante.

I titolari dotati di certificazione del sistema di gestione per la sicurezza delle informazioni (SGSI) secondo la norma tecnica ISO/IEC 27001 che inseriscono il sistema biometrico nel campo di applicazione della certificazione sono esentati dall'obbligo di redigere la relazione di cui al precedente periodo, potendo utilizzare la documentazione prodotta nell'ambito della certificazione, integrandola con la valutazione della necessità e della proporzionalità del trattamento biometrico.

4.4 Sottoscrizione di documenti informatici

Il trattamento di dati biometrici costituiti da informazioni dinamiche associate all'apposizione a mano libera di una firma autografa avvalendosi di specifici dispositivi hardware è ammesso in assenza di verifica preliminare laddove si utilizzino sistemi di firma grafometrica posti a base di una soluzione di firma elettronica avanzata, così come definita dal Decreto Legislativo 7 marzo 2005, n. 82, recante il “Codice dell'amministrazione digitale” che non prevedono la conservazione centralizzata di dati biometrici.

L’utilizzo di tali sistemi, da un lato, si giustifica al fine di contrastare eventuali tentativi di frode e il fenomeno dei furti di identità e, dall'altro, ha lo scopo di rafforzare le garanzie di autenticità e integrità dei documenti informatici sottoscritti, anche in vista di eventuale

contenzioso legato al disconoscimento della sottoscrizione apposta su atti e documenti di tipo negoziale in sede giudiziaria.

In tali casi, il presupposto di legittimità del trattamento dei dati biometrici è dato dal consenso, effettivamente libero degli interessati ovvero, in ambito pubblico, dal perseguimento delle finalità istituzionali del titolare. Il consenso è espresso dall'interessato all'atto di adesione al servizio di firma grafometrica e ha validità, fino alla sua eventuale revoca, per tutti i documenti da sottoscrivere.

Il titolare è esonerato dall'obbligo di presentare istanza di verifica preliminare se il trattamento è svolto nel rispetto delle seguenti prescrizioni e limitazioni:

a) Il procedimento di firma è abilitato previa identificazione del firmatario.

b) Sono resi disponibili sistemi alternativi (cartacei o digitali) di sottoscrizione, che non comportino l'utilizzo di dati biometrici.

c) La cancellazione dei dati biometrici grezzi e dei campioni biometrici ha luogo immediatamente dopo il completamento della procedura di sottoscrizione, e nessun dato biometrico persiste all'esterno del documento informatico sottoscritto.

d) I dati biometrici e grafometrici non sono conservati, neanche per periodi limitati, sui dispositivi hardware utilizzati per la raccolta, venendo memorizzati all'interno dei documenti informatici sottoscritti in forma cifrata tramite sistemi di crittografia a chiave pubblica con dimensione della chiave adeguata alla dimensione e al ciclo di vita dei dati e certificato digitale emesso da un certificatore accreditato ai sensi dell'art. 29 del Codice dell'amministrazione digitale. La corrispondente chiave privata è nella esclusiva disponibilità di un soggetto terzo fiduciario che fornisca idonee garanzie di indipendenza e sicurezza nella conservazione della medesima chiave. La chiave può essere frazionata tra più soggetti ai fini di sicurezza e integrità del dato. In nessun caso il soggetto che eroga il servizio di firma grafometrica può conservare in modo completo tale chiave privata. Le modalità di generazione, consegna e conservazione delle chiavi sono

dettagliate nell'informativa resa agli interessati e nella relazione di cui alla lettera k) del presente paragrafo, in conformità con quanto previsto all'art. 57, comma 1 lettere e) ed f) del d.P.C.M. 22 febbraio 2013.

e) La trasmissione dei dati biometrici tra sistemi hardware di acquisizione, postazioni informatiche e server avviene esclusivamente tramite canali di comunicazione resi sicuri con l'ausilio di tecniche crittografiche con lunghezza delle chiavi adeguata alla dimensione e al ciclo di vita dei dati.

f) Sono adottate idonee misure e accorgimenti tecnici per contrastare i rischi di installazione di software e di modifica della configurazione delle postazioni informatiche e dei dispositivi, se non esplicitamente autorizzati.

g) I sistemi informatici sono protetti contro l'azione di malware e sono, inoltre, adottati sistemi di firewall per la protezione perimetrale della rete e contro i tentativi di accesso abusivo ai dati.

h) Nel caso di utilizzo di sistemi di firma grafometrica nello scenario mobile o BYOD (Bring Your Own Device), sono adottati idonei sistemi di gestione delle applicazioni o dei dispositivi mobili, con il ricorso a strumenti MDM (Mobile Device Management) o MAM (Mobile Application Management) o altri equivalenti al fine di isolare l'area di memoria dedicata all'applicazione biometrica, ridurre i rischi di installazione abusiva di software anche nel caso di modifica della configurazione dei dispositivi e contrastare l'azione di eventuali agenti malevoli (malware).

i) I sistemi di gestione impiegati nei trattamenti grafometrici adottano certificazioni digitali e policy di sicurezza che disciplinino, sulla base di criteri predeterminati, le condizioni di loro utilizzo sicuro (in particolare, rendendo disponibili funzionalità di remote wiping applicabili nei casi di smarrimento o sottrazione dei dispositivi).

j) L'accesso al modello grafometrico cifrato avviene esclusivamente tramite l'utilizzo della chiave privata detenuta dal soggetto terzo fiduciario, o da più soggetti, in caso di frazionamento della chiave stessa, e nei soli casi in cui si renda indispensabile per l'insorgenza di

un contenzioso sull'autenticità della firma e a seguito di richiesta dell'autorità giudiziaria. Le condizioni e le modalità di accesso alla firma grafometrica da parte del soggetto terzo di fiducia o da parte di tecnici qualificati sono dettagliate nell'informativa resa agli interessati e nella relazione di cui alla lettera k) del presente paragrafo, in conformità con quanto previsto all'art. 57, comma 1, lettere e) ed f) del d.P.C.M. 22 febbraio 2013.

k) E' predisposta una relazione che descrive gli aspetti tecnici e organizzativi delle misure messe in atto dal titolare, fornendo altresì la valutazione della necessità e della proporzionalità del trattamento biometrico rispetto alle finalità. Tale relazione tecnica è conservata aggiornata, con verifica di controllo almeno annuale, per tutto il periodo di esercizio del sistema biometrico e mantenuta a disposizione del Garante.

I titolari dotati di certificazione del sistema di gestione per la sicurezza delle informazioni (SGSI) secondo la norma tecnica ISO/IEC 27001 che inseriscono il sistema biometrico nel campo di applicazione della certificazione sono esentati dall'obbligo di redigere la relazione di cui al precedente periodo, potendo utilizzare la documentazione prodotta nell'ambito della certificazione, integrandola con la valutazione della necessità e della proporzionalità del trattamento biometrico.

TUTTO CIÒ PREMESSO IL GARANTE

1. adotta ai sensi dell'art. 154, comma 1, lettera h) del Codice l'allegato "A", recante le "Linee-guida in materia di riconoscimento biometrico e firma grafometrica", che forma parte integrante della presente deliberazione, al fine di informare i titolari di trattamento, i produttori di tecnologie biometriche, i fornitori di servizi e gli interessati sui diversi aspetti connessi alla protezione dei dati personali, ivi compresi quelli relativi alla sicurezza, e sui presupposti di legittimità dei trattamenti dei dati biometrici;

2. prescrive, ai sensi dell’art. 154, comma 1, lettera c) del Codice, che i titolari di trattamenti biometrici comunichino al Garante, entro

ventiquattro ore dalla conoscenza del fatto, le violazioni dei dati biometrici secondo le modalità di cui al paragrafo 3;

3. individua, nei termini di cui al paragrafo 4, i casi di esonero dalla presentazione di istanza di verifica preliminare, e prescrive ai soggetti che intendano procedere in qualità di titolari a tali trattamenti, ai sensi dell'art. 17 del Codice, di adottare le misure e gli accorgimenti tecnici, organizzativi e procedurali descritti nel medesimo paragrafo, nonché di rispettare i presupposti di legittimità e le indicazioni contenute nelle allegate linee-guida con particolare riferimento al capitolo 4 "Principi generali e adempimenti giuridici";

4. prescrive ai titolari di trattamenti biometrici che non abbiano richiesto la verifica preliminare al Garante:

a. di adottare – entro centottanta giorni dalla pubblicazione del presente provvedimento sulla Gazzetta Ufficiale della Repubblica Italiana – le misure e gli accorgimenti di cui al paragrafo 4, qualora i trattamenti siano compresi nei casi di esonero dall'obbligo di verifica preliminare;

ovvero

b. di sospendere – entro il medesimo termine – i trattamenti e di sottoporre gli stessi a verifica preliminare, con interpello al Garante ai sensi dell'art. 17 del Codice;

5. invita i titolari dei trattamenti biometrici compresi nei casi di esonero dall'obbligo di verifica preliminare, i quali abbiano già presentato istanza, tuttora pendente, ex art. 17 del Codice, a comunicare al Garante – entro trenta giorni dalla pubblicazione del presente provvedimento sulla Gazzetta Ufficiale della Repubblica Italiana – la conformità del trattamento alle prescrizioni ivi contenute ovvero la propria intenzione di conformarvisi. La presentazione della comunicazione comporta il non luogo a provvedere sulle relative istanze. Le istanze di verifica preliminare in relazione alle quali non sia stata presentata la comunicazione di cui al periodo che precede verranno valutate dal Garante secondo le ordinarie procedure;

6. dispone, ai sensi dell'art. 143, comma 2, del Codice, che copia del presente provvedimento sia trasmessa al Ministero della giustizia –

Ufficio pubblicazione leggi e decreti – per la sua pubblicazione sulla Gazzetta Ufficiale della Repubblica Italiana.

Roma, 12 novembre 2014

IL PRESIDENTE

Soro

IL RELATORE

Iannini

IL SEGRETARIO GENERALE

Soro

Giurisprudenza

CORTE DI CASSAZIONE, sez. I civile – sentenza 28 marzo – 7 ottobre 2014, n. 21107.

Condivisa dai giudici la posizione assunta dal Garante della protezione dei dati personali, che ha sanzionato una Provincia per avere raccolto in rete dati riferiti a offerte di prestazioni sessuali a pagamento, pubblicate da un dipendente. Ci si trova di fronte a "dati sensibili", e il fatto che siano disponibili in rete non li rende disponibili per qualsiasi utilizzo, considerando nullo il problema della privacy.

Svolgimento del processo

1. - Con sentenza del 13 giugno 2012, il Tribunale di Verbania ha accolto il ricorso proposto dalla Provincia ____ avverso il provvedimento emesso il 6 dicembre 2011, n. 468, con cui il Garante per la Protezione dei Dati personali aveva fatto divieto alla ricorrente di trattare ulteriormente le informazioni relative alla vita sessuale di ____ Ha premesso il Tribunale che, a seguito di una comunicazione anonima con cui si segnalava l'esercizio dell'attività di escort da parte di un dipendente, l'Amministrazione aveva proceduto a verifica mediante accesso ai siti web indicati, promuovendo successivamente un procedimento disciplinare nei confronti del B.; tale procedimento si era concluso con determinazione del 28 settembre 2011, con cui il dirigente del settore aveva applicato al dipendente la sanzione della destituzione, per aver inserito su siti per escort annunci contenenti l'offerta di prestazioni sessuali a pagamento, in danno dell'immagine della Provincia. Precisato che la sanzione si riferiva esclusivamente agli annunci pubblicati sui predetti siti, e non anche alle inserzioni pubblicate su siti di contenuto sociale rivolti prevalentemente a persone omosessuali e bisessuali, il Tribunale ha escluso che la raccolta delle informazioni in rete fosse avvenuta in difetto delle condizioni richieste dal d.lgs. 30 giugno 2003, n. 196 per il trattamento dei dati sensibili finalizzato alla gestione del rapporto di

lavoro, osservando che nella specie non poteva trovare applicazione la disciplina in materia di tutela della privacy, in quanto, avuto riguardo alle finalità del provvedimento disciplinare, la raccolta dei dati era volta ad acquisire non già elementi relativi all'orientamento sessuale del dipendente, ma la prova della denunciata pubblicizzazione dell'attività di prostituzione, che, per le modalità prescelte, era stata ritenuta lesiva dell'immagine dell'Ente.

2. - Avverso la predetta sentenza il Garante ha proposto ricorso per cassazione, articolato in cinque motivi, illustrati anche con memoria. La Provincia ha resistito con controricorso, anch'esso illustrato con memoria. Il B. non ha svolto attività difensiva.

Motivi della decisione

1. - Con il primo motivo d'impugnazione, il Garante denuncia la contraddittorietà della motivazione circa un punto decisivo della controversia, censurando la sentenza impugnata nella parte in cui ha negato la sussistenza di un trattamento di dati riguardanti la vita sessuale del dipendente, in contrasto con gli atti di causa, dai quali risultava pacificamente che la Provincia aveva raccolto in rete le informazioni poi utilizzate nell'ambito del procedimento disciplinare.
2. - Con il secondo motivo, il ricorrente deduce la violazione e la falsa applicazione dell'art. 4, comma primo, lett. a), del d.lgs. n. 196 del 2003, sostenendo che, nell'escludere l'applicabilità della disciplina in materia di tutela della privacy, il Tribunale non ha considerato che costituisce trattamento di dati personali qualsiasi operazione o complesso di operazioni concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione e l'utilizzo di informazioni.

3. - Con il terzo motivo, il ricorrente lamenta l’insufficienza e la contraddittorietà della motivazione circa un punto decisivo della controversia, osservando che, nonostante l'avvenuto accertamento della raccolta di informazioni inerenti alla vita sessuale, in quanto riguardanti lo svolgimento dell’attività di prostituzione, la sentenza impugnata ha escluso la configurabilità di un trattamento di dati sensibili.

4. - Con il quarto motivo, il ricorrente denuncia la violazione e la falsa applicazione dell’art. 4, comma primo, lett. d), del d.lgs. n. 196 del 2003, rilevando che l'esclusione della configurabilità di un trattamento di dati sensibili ha indotto il Tribunale a negare l'applicabilità della tutela rafforzata prevista dalla predetta disposizione in considerazione della particolare natura di tali dati, che investono la parte più intima della persona nella sua corporeità e nelle sue convinzioni psicologiche più riservate.

5. - Con il quinto motivo, il ricorrente deduce la violazione dell’art. 20, commi primo e secondo, del d.lgs. n. 196 del 2003, come integrato dal regolamento approvato con d.P.C. n. 78 del 2005 e modificato con d.P.C. n. 49 del 2006, sostenendo che l’utilizzazione di dati personali per l'adozione di provvedimenti disciplinari nei confronti di un dipendente costituisce un accadimento tipico della gestione del rapporto di lavoro, tale da giustificare nella specie l'applicazione della disciplina regolamentare adottata dalla Provincia ai sensi dell’art. 20 cit., la quale consente il trattamento dei dati sensibili soltanto in caso di rettifica di attribuzione di sesso.

6. - In ordine all’ammissibilità delle predette censure, va disattesa l'eccezione sollevata dalla difesa della Provincia, secondo cui l'osservanza dell’onere di specificazione dei motivi d’impugnazione avrebbe richiesto l’indicazione e la trascrizione nel ricorso dei documenti che costituiscono oggetto del contenzioso, e segnatamente degli estratti dei siti internet e delle comunicazioni in discussione, oltre che del regolamento adottato dalla Provincia a tutela dei dati sensibili, nonché la formulazione dei quesiti di diritto sottesi alle singole censure.
Il ricorso ha infatti ad oggetto una sentenza pubblicata in data successiva all’entrata in vigore della legge 18 giugno 2009, n. 69, e pertanto, ai sensi dell’art. 58, comma quinto, ad esso si applica l’art. 47, comma primo, lett. d), della medesima legge, il quale, disponendo l’abrogazione dell’art. 366-bis cod. proc. civ., introdotto dall’art. 6 del d.lgs. 2 febbraio 2006, n. 40, ha escluso la necessità della formulazione del quesito di diritto, che la norma abrogata imponeva a corredo dell'illustrazione di ciascun motivo d’impugnazione.

L’indicazione degli atti processuali e dei documenti sui quali si fonda il ricorso è resa invece superflua dall'assenza di contestazioni in ordine alla ricostruzione dei fatti emergente dalla sentenza impugnata e dalla natura prettamente giuridica delle questioni sollevate dal ricorrente, che escludono la necessità di procedere all'esame degli atti, ai fini del riscontro dei relativi presupposti. La verifica della osservanza di quanto prescritto dall'art. 366, primo comma, n. 6), cod. proc. civ. dev'essere infatti compiuta con riguardo al contenuto dei motivi d'impugnazione, potendo condurre alla declaratoria di inammissibilità soltanto quando si tratti di censure rispetto alle quali uno o più specifici atti o documenti ne costituiscano il fondamento, nel senso che, senza l'esame di quell'atto o quel documento, risulterebbero impossibili la comprensione del motivo di doglianza e degl'indispensabili presupposti fattuali sui quali esso si basa, nonché la valutazione della sua decisività (cfr. Cass., Sez. I, 5 luglio 2013, n. 16887).
Quanto al regolamento per il trattamento dei dati sensibili e giudiziari, adottato dall'Amministrazione provinciale con deliberazione consiliare del 22 dicembre 2005, n. 78 e modificato con deliberazione consiliare del 31 luglio 2006, n. 49, il suo richiamo dev'essere ritenuto sufficiente ai fini dell'applicazione delle relative disposizioni, nonostante la mancata trascrizione delle relative disposizioni nel ricorso, trattandosi di un atto normativo secondario integrativo della disciplina legale, e quindi conoscibile anche d'ufficio da parte del giudice, che può farne applicazione indipendentemente dalle prospettazioni delle parti, in ossequio al principio jura novit curia (cfr. ex plurimis, Cass., Sez. II, 15 giugno 2010, n. 1446; 2 febbraio 2009, n. 2563).

7. - I cinque motivi devono essere trattati congiuntamente, avendo ad oggetto profili diversi della medesima questione. Il trattamento di dati personali da parte dei soggetti pubblici è disciplinato dall'art. 18 del d.lgs. n. 196 del 2003 (c.d. codice in materia di protezione dei dati personali), il quale stabilisce, al comma secondo, il principio generale secondo cui tale trattamento è consentito soltanto per lo svolgimento delle funzioni istituzionali dell'ente, precisando al comma terzo che nel trattare i dati il soggetto pubblico deve rispettare i presupposti e i

limiti stabiliti dal medesimo codice, anche in relazione alla diversa natura dei dati, nonché dalla legge e dai regolamenti. Con particolare riferimento ai dati sensibili, comprendenti tra l'altro quelli idonei a rivelare lo stato di salute e la vita sessuale dell'interessato (art. 4, comma primo, lett. e), i predetti limiti sono stabiliti dall'art. 20, il quale consente il trattamento solo se autorizzato da un'espressa disposizione di legge, in cui devono essere specificati i tipi di dati che possono essere trattati ed i tipi di operazioni eseguibili, nonché le finalità di rilevante interesse pubblico perseguite. Tra le predette finalità l'art. 112, comma primo, annovera specificamente quelle inerenti all'instaurazione ed alla gestione di rapporti di lavoro di qualunque tipo da parte di soggetti pubblici, in relazione alle quali il comma secondo della medesima disposizione elenca, a titolo meramente esemplificativo, i tipi di trattamenti consentiti, includendovi, tra l'altro, lo svolgimento di attività dirette all'accertamento della responsabilità civile, disciplinare e contabile e l’esame dei ricorsi amministrativi, in conformità alle norme che regolano le rispettive materie (lett. g). Poiché quest'ultima disposizione si limita ad indicare genericamente le finalità del trattamento, senza specificare i dati che possono essere trattati e le operazioni che possono essere eseguite, trova applicazione il comma secondo dell'art. 20, il quale stabilisce che in siffatti casi il trattamento è consentito solo in riferimento ai tipi di dati e di operazioni identificati e resi pubblici a cura dei soggetti che ne effettuano il trattamento, in relazione alle specifiche finalità perseguite nei singoli casi e nel rispetto dei principi di cui all'art. 22, con atto di natura regolamentare adottato in conformità al parere espresso dal Garante ai sensi dell'art. 154, comma primo, lett. g), anche su schemi tipo.
La predetta disciplina riproduce fedelmente quella dettata dall'abrogata legge 31 dicembre 1996, n. 675, come modificata dal d.lgs. 11 maggio 1999, n. 135, in relazione alla quale questa Corte ha affermato il principio secondo cui il trattamento dei dati sensibili, la cui legittimità è ancorata in linea generale alla contestuale presenza del consenso scritto dell'interessato ed all'autorizzazione del Garante per la protezione dei dati personali, è consentito, da parte dei soggetti pubblici, anche in difetto del predetto consenso e della predetta autorizzazione, a condizione che sussistano a) una rilevante finalità

d’interesse pubblico, b) un'espressa disposizione di legge autorizzatoria e c) una specificazione legislativa dei tipi di dati trattabili e delle operazioni eseguibili. Con particolare riguardo al trattamento di dati effettuato nell'ambito di un rapporto di lavoro per l'accertamento della responsabilità disciplinare, si è quindi precisato che l'espressa inclusione di tale finalità tra quelle d'interesse pubblico non è di per sé sufficiente ad escludere la necessità del consenso e dell'autorizzazione, occorrendo a tal fine anche l'indicazione dei tipi di dati sensibili che possono essere trattati e delle operazioni eseguibili sugli stessi, da parte dello stesso soggetto pubblico o, su sua richiesta, della Autorità garante. Si è infatti osservato che la particolare natura dei dati sensibili, e segnatamente di quelli riguardanti la salute e la vita sessuale delle persone (che appartengono alla categoria dei dati c.d. supersensibili, i quali investono la parte più intima della persona, nella sua corporeità e nelle sue convinzioni psicologiche più riservate), esige, in ragione dei valori costituzionali posti a loro presidio (artt. 2 e 3 Cost.), una protezione rafforzata, la quale trova espressione anche nelle garanzie previste per il trattamento effettuato dai soggetti pubblici, che può quindi aver luogo soltanto nel rispetto del modulo procedimentale previsto dalla legge (cfr. Cass., Sez. I, 8 luglio 2005, n. 14390).

In riferimento alla fattispecie in esame, tale modulo procedimentale ha trovato espressione nel regolamento adottato dall'Amministrazione provinciale con le citate deliberazioni consiliari, il quale, nel disciplinare il trattamento dei dati sensibili e giudiziari, individua alla scheda n. 1 i tipi di dati trattabili e le operazioni eseguibili ai fini dell'instaurazione e della gestione del rapporto di lavoro, ed alla scheda n. 7 quelli consentiti ai fini della gestione del contenzioso, prevedendo un regime differenziato dei dati riguardanti la vita sessuale, il cui trattamento è consentito senza limitazioni nella seconda ipotesi, mentre nella prima ipotesi è permesso soltanto in caso di eventuale rettificazione di attribuzione di sesso.

Alla stregua di tali indicazioni, non possono condividersi le conclusioni cui è pervenuta la sentenza impugnata, la quale ha escluso l'applicabilità della disciplina in esame, in virtù dell'osservazione che l'attività posta in essere dall'Amministrazione non era finalizzata alla raccolta di dati inerenti alla vita sessuale del dipendente, ma alla

verifica dell’avvenuta pubblicizzazione dell'attività di meretricio da quest'ultimo svolta, attraverso l'acquisizione dei documenti informatici attestanti gli annunci da lui pubblicati sul web per l'offerta di prestazioni sessuali a pagamento. Nella parte in cui fa leva sulle finalità della ricerca ai fini dell'esclusione della configurabilità di un trattamento di dati, tale affermazione si pone in contrasto con l'ampia definizione risultante dall'art. 4, comma primo, lett. a), del d.lgs. n. 196 del 2003, che include nella predetta nozione «qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l’elaborazione, la modificazione, la selezione, l’estrazione, il raffronto, l’utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati», conferendo pertanto rilievo alla natura dell'operazione, oggettivamente considerata, senza fare alcun riferimento alle motivazioni o ai fini della stessa, che vengono in considerazione esclusivamente per l'individuazione delle modalità e dei limiti del trattamento. Portata decisiva, in quest'ottica, deve riconoscersi al dato oggettivo dell'acquisizione d'informazioni attinenti alla vita sessuale del dipendente, di per sé sufficiente a rendere configurabile un trattamento di dati sensibili, le cui modalità ed i cui limiti devono essere ricostruiti avendo riguardo alla gestione del rapporto di lavoro, cui è indiscutibilmente preordinata l'adozione di provvedimenti disciplinari: e poiché, come emerge dalla scheda n. 1 allegata al regolamento provinciale, il trattamento di dati relativi alla vita sessuale è consentito soltanto in caso di rettificazione di attribuzione di sesso, deve concludersi per l'illegittimità dell'operazione posta in essere dall’Amministrazione attraverso l'acquisizione dei documenti informatici.

Non merita consenso, al riguardo, la tesi sostenuta dall'Amministrazione, secondo cui il trattamento in questione, in quanto volto all'adozione di un provvedimento suscettibile di dare origine ad un contenzioso, dev'essere ricondotto alle indicazioni contenute nella scheda n. 7 del regolamento, che esclude qualsiasi limitazione all'acquisizione ed all'utilizzazione dei dati relativi alla vita sessuale. Nel definire la gestione del contenzioso come insieme

delle attività relative alla consulenza giuridica, al patrocinio ed alla difesa in giudizio dell'Amministrazione, la predetta scheda attribuisce ai trattamenti ivi contemplati la finalità di consentire l'esercizio del diritto di difesa in sede amministrativa e/o giudiziaria, in tal modo postulando una diretta connessione dell'operazione con una controversia in atto, non ancora configurabile nella fase amministrativa che conduce all'adozione del provvedimento concernente la gestione del rapporto di lavoro. Se è vero, peraltro, che la difesa dell'Amministrazione in sede amministrativa o giurisdizionale può richiedere il trattamento di dati sensibili, soprattutto (ma non solo) nel caso in cui la controversia riguardi la legittimità di un provvedimento che ne presuppone l'utilizzazione, è anche vero, però, che da tale esigenza difensiva non può farsi discendere la legittimità di qualsiasi trattamento dei predetti dati, risultando altrimenti elusi i principi generali di proporzionalità, necessità, pertinenza e non eccedenza allo scopo della raccolta e del trattamento, stabiliti dall'art. 11 del d.lgs. n. 196 del 2003, e dei quali costituiscono espressione le limitazioni imposte dalla disciplina in esame. Quanto al rilievo conclusivo della sentenza impugnata, secondo cui il riconoscimento della tutela assicurata dal codice della privacy deve ritenersi precluso per effetto dello stesso ricorso dell'interessato all'uso della rete, il quale implica la volontà di rivolgersi ad un pubblico potenzialmente indeterminato, con la conseguente impossibilità di garantire la limitata diffusività degli annunci, è sufficiente osservare che l'immissione di alcuni dei propri dati personali in rete, pur lasciando presumere la volontà dell'interessato di permetterne l'utilizzazione in vista degli obiettivi per cui gli stessi sono stati posti a disposizione del pubblico, non consente tuttavia di ritenere che quel consenso sia stato implicitamente prestato anche in funzione di qualsiasi altro trattamento. L’utilizzazione dei dati diffusi per finalità diverse da quella per cui ne è stata consentita la divulgazione costituisce d'altronde un’eventualità già presa in considerazione da questa Corte, la quale ha affermato in proposito che la tutela apprestata dal d.lgs. n. 196 del 2003 si estende anche ai dati già pubblici o pubblicati, dal momento che colui che compie operazioni di trattamento di tali informazioni può ricavare dal loro accostamento, comparazione,

esame, analisi, congiunzione, rapporto od incrocio ulteriori informazioni, e quindi un «valore aggiunto informativo», non estraibile dai dati isolatamente considerati, potenzialmente lesivo della dignità dell'interessato, valore sommo (tutelato dall'art. 3, primo comma, prima parte, e dell'art. 2 Cost.) a cui si ispira la legislazione in materia di trattamento dei dati personali (cfr. Cass., Sez. I, 8 agosto 2013, n. 18981; 25 giugno 2004, n. 11864).

8. - Il ricorso va pertanto accolto, con la conseguente cassazione della sentenza impugnata, e, non risultando necessari ulteriori accertamenti di fatto, la causa può essere decisa nel merito, ai sensi dell'art. 384, secondo comma, cod. proc. civ., con il rigetto della domanda proposta dalla Provincia.

9. - La novità della questione trattata giustifica la dichiarazione dell'integrale compensazione delle spese dei due gradi di giudizio.

P.Q.M.

La Corte accoglie il ricorso, cassa la sentenza impugnata, e, decidendo nel merito, rigetta la domanda proposta dalla Provincia del ____; dichiara interamente compensate tra le parti le spese processuali.

CORTE DI CASSAZIONE, sez. V penale – 16 giugno 2014, n. 25774.

Integra il delitto di sostituzione di persona, previsto e punito dalla fattispecie incriminatrice di cui all'art. 494 c.p., la condotta criminosa consistita nella creazione, su un social network, di un profilo che riproduca l'effige della persona offesa e nel conseguente utilizzo, con tale falsa identità, dei servizi del sito, consistenti essenzialmente nella possibilità di comunicazione in rete con gli altri iscritti, indotti in errore dalla identità dell'interlocutore, e di condivisione di contenuti. In punto di elemento soggettivo, il dolo specifico del delitto, consistente nel fine di procurare a sé o ad altri un vantaggio patrimoniale o non, oppure di recare ad altrui un danno, deve ritenersi integrato nell'ipotesi di utilizzo del profilo al fine di intrattenere rapporti con altre persone (essenzialmente di sesso opposto), ovvero per il soddisfacimento di una propria vanità (costituente vantaggio non patrimoniale), o ancora al fine di ledere la immagine e la dignità della persona offesa, apparentemente titolare del profilo creato dal reo. (Nel caso concreto tale fine è dimostrato dall'aggressione verbale di uno sconosciuto, che accusò l'apparente titolare del profilo di aver insultato la propria fidanzata, minacciandolo di denuncia, nonché dalla rimostranze di una conoscente, che lo accusava di non essere una persona seria).

RITENUTO IN FATTO

1. Con la sentenza resa in data 19 aprile 2012, confermata dalla Corte d'appello di Reggio Calabria il 16 maggio 2013, il Tribunale di Palmi condannava (OMISSIS) alla pena di giustizia per il delitto di sostituzione di persona, poiché al fine di procurarsi un vantaggio o comunque di recare danno a (OMISSIS), si attribuiva la sua identità, pubblicando sul sito (OMISSIS) la sua immagine, associata al nominativo "(OMISSIS)", utilizzando il profilo creato e così inducendo in errore coloro che comunicavano con lui attraverso la "chat".

2. Contro la sentenza propone ricorso per Cassazione l'imputato, con atto del proprio difensore, avv. (OMISSIS), affidato a tre motivi.

2.1 Con il primo motivo si deduce violazione dell'articolo 606 c.p.p., lettera E, in relazione all'articolo 494 cod. pen., con riferimento all'elemento soggettivo del reato richiesto dalla norma penale nella forma del dolo specifico, caratterizzato dal fine di recare a se o ad altri un vantaggio o di recare ad altri un danno. A giudizio del ricorrente tale forma di dolo deve escludersi nella mera pubblicazione di un profilo su Internet, non del tutto riferibile alla persona offesa, della quale viene solo utilizzata una fotografia e non anche il nome.

2.2 Con il secondo motivo si deduce violazione dell'articolo 606, lettera E, in relazione all'articolo 192 cod. proc. pen., con riferimento alla valutazione di attendibilità delle dichiarazioni della persona offesa, la quale riferisce circostanze generiche ed in parte incongruenti, che dovevano condurre ad escludere la sua attendibilità, considerata altresì la costituzione di parte civile.

3. Con il terzo motivo si deduce violazione dell'articolo 606, lettera D ed E, in relazione all'articolo 495 c.p.p., comma 2, con riferimento alla mancata escussione, ai sensi dell'articolo 603 cod. proc. pen., della teste (OMISSIS), alla quale la parte civile aveva fatto riferimento come la persona che lo avrebbe informato dell'esistenza del falso profilo su internet. Il ricorrente censura la valutazione di non necessarietà della prova richiesta, come non adeguatamente motivata e violativa del diritto alla controprova.

4. Con memoria del 9 aprile 2013, la parte civile (OMISSIS) chiede dichiararsi l'inammissibilità del ricorso, poiché nello stesso sono denunciati esclusivamente vizi di merito. In subordine se ne chiede il rigetto, per infondatezza delle doglianze.

4.1 Con riferimento al primo motivo, si sottolinea che il dolo è evidenziato, nella sentenza di primo grado, nel fine di arrecare un danno all'immagine ed alla dignità della vittima.

4.2 Quanto all'attendibilità della persona offesa, si richiama la motivazione della sentenza impugnata, che si ritiene congrua ed

immune da illogicità di sorta e pertanto sottratta ad ogni sindacato di legittimità.

4.3 In ordine, infine, alla mancata assunzione di prova decisiva, si ribadisce la superfluità dei mezzi istruttori richiesti, atteso che la responsabilità dell'imputato è stata provata attraverso le indagini sull'utenza telefonica e sul personal computer del (OMISSIS).

CONSIDERATO IN DIRITTO

1. Il ricorso va rigettato.

1.1 Il primo motivo, riguardante la mancata verificazione del dolo specifico da parte della Corte territoriale, è inammissibile, poiché proposto per la prima volta in sede di legittimità, in contrasto con l'orientamento costante di questa Corte (Sez. 3, n. 21920 del 16/05/2012, Hajmohamed, Rv. 252773) secondo cui la denuncia di violazioni di legge non dedotte con i motivi di appello costituisce causa di inammissibilità originaria dell'impugnazione. Il parametro dei poteri di cognizione del giudice di legittimità è delineato dall'articolo 609 c.p.p., comma 1, il quale ribadisce in forma esplicita un principio già enucleabile dal sistema, e cioè la commisurazione della cognizione di detto giudice ai motivi di ricorso proposti. Detti motivi - contrassegnati dall'inderogabile "indicazione specifica delle ragioni di diritto e degli elementi di fatto" che sorreggono ogni atto d'impugnazione (articolo 581 c.p.p., comma 1, lettera E e articolo 591 c.p.p., comma 1, lettera C) - sono funzionali alla delimitazione dell'oggetto della decisione impugnata ed all'indicazione delle relative questioni, con modalità specifiche al ricorso per cassazione. La disposizione in esame deve infatti essere letta in correlazione con quella dell'articolo 606, comma 3, nella parte in cui prevede la non deducibilità in cassazione delle questioni non prospettate nei motivi di appello. Il combinato disposto delle due norme impedisce la proponibilità in cassazione di qualsiasi questione non prospettata in appello, e, come rileva la più recente dottrina, costituisce un rimedio contro il rischio concreto di un annullamento, in sede di cassazione, del provvedimento impugnato, in relazione ad un punto

intenzionalmente sottratto alla cognizione del giudice di appello: in questo caso, infatti, è facilmente diagnosticabile in anticipo un inevitabile difetto di motivazione della relativa sentenza con riguardo al punto dedotto con il ricorso, proprio perché mai investito della verifica giurisdizionale.

1.2 La doglianza è comunque anche infondata.

L’articolo 494 cod. pen. punisce chiunque, al fine di procurare a sè o ad altri un vantaggio o di recare ad altri un danno, induce taluno in errore, sostituendo illegittimamente la propria all'altrui persona, o attribuendo a sé o ad altri un falso nome, o un falso stato, ovvero una qualità a cui la legge attribuisce effetti giuridici. Oggetto della tutela penale è l'interesse riguardante la pubblica fede, in quanto questa puo' essere sorpresa da inganni relativi alla vera essenza di una persona o alla sua indentita' o ai suoi attributi sociali; siccome si tratta di inganni che possono superare la ristretta cerchia d'un determinato destinatario, il legislatore ha ravvisato in essi una costante insidia alla fede pubblica, e non soltanto alla fede privata e alla tutela civilistica del diritto al nome. In questa prospettiva, è evidente la configurazione, nel caso concreto, di tutti gli elementi costitutivi della contestata fattispecie delittuosa.

1.3 Nella specie, il ricorrente ha creato un profilo sul social network (OMISSIS) denominato "(OMISSIS)", riproducente l'effige della persona offesa, con una descrizione tutt'altro che lusinghiera (ad esempio nelle informazioni personali era riportata la dicitura "Mangio solo cibo spazzatura e bevo birra... quando mi ubriaco vado su di giri") e con tale falsa identità usufruiva dei servizi del sito, consistenti essenzialmente nella possibilità di comunicazione in rete con gli altri iscritti (indotti in errore sulla sua identità) e di condivisione di contenuti (tra cui la stessa foto ritraente il (OMISSIS)).

1.4 Il dolo specifico del delitto di cui all'articolo 494 cod. pen., consiste nel fine di procurare a se o ad altri un vantaggio patrimoniale o non, oppure di recare ad altri un danno (Sez. 5, n. 13296 del 28/01/2013, Marino, Rv. 255344) e sul punto le decisioni di merito danno conto della sussistenza di entrambi i profili: dei vantaggi ritraibili dall'attribuzione di una diversa identità, che il ricorrente

utilizzava per poter intrattenere rapporti con altre persone (essenzialmente ragazze) o per soddisfacimento di una propria vanita' (vantaggio non patrimoniale); della idoneita' della condotta a ledere l'immagine e la dignita' del (OMISSIS) (come dimostrato dall'aggressione verbale dello sconosciuto, che lo accuso' di aver insultato la propria fidanzata, minacciando di denunciarlo nonche' dalle rimostranze della conoscente, che lo aveva accusato di non essere una persona seria).

1.[5] Con riferimento al fenomeno della comunicazione a mezzo internet, questa Corte ha recentemente ritenuto sussistere il delitto di sostituzione di persona nella condotta di colui che crei ed utilizzi un “account” ed una casella di posta elettronica, servendosi dei dati anagrafici di un diverso soggetto, inconsapevole, con il fine di far ricadere su quest'ultimo l’inadempimento delle obbligazioni conseguenti all'avvenuto acquisto di beni mediante la partecipazione ad aste in rete (Sez. 3, n. 12479 del 15/12/2011 - dep. 03/04/2012, Armellini, Rv. 252227), nonché nella condotta di chi inserisca nel sito di una “chat line” a tema erotico il recapito telefonico di altra persona associato ad un “nickname” di fantasia, qualora abbia agito al fine di arrecare danno alla medesima, giacche' in tal modo gli utilizzatori del servizio vengono tratti in inganno sulla disponibilità della persona associata allo pseudonimo a ricevere comunicazioni a sfondo sessuale (Sez. 5, n. 18826 del 28/11/2012 - dep. 29/04/2013, Celotti, Rv. 255086).

1.[6] Più aderente alla fattispecie oggetto di questo giudizio è però quella esaminata da una decisione meno recente di questa Sezione (Sez. 5, n. 46674 del 08/11/2007, Adinolfi, Rv. 238504), della condotta la condotta di colui che crei ed utilizzi un "account" di posta elettronica, attribuendosi falsamente le generalità di un diverso soggetto, inducendo in errore gli utenti della rete internet nei confronti dei quali le false generalità siano declinate e con il fine di arrecare danno al soggetto le cui generalità siano state abusivamente spese (nella specie a seguito dell'iniziativa dell'imputato, la persona offesa si ritrovò a ricevere telefonate da uomini che le chiedevano incontri a scopo sessuale). In questa fattispecie, come in quella, infatti, la descrizione di un profilo poco lusinghiero, come sopra ricordato,

consente di riconoscere, oltre all'intento di conseguire un vantaggio non patrimoniale, quello di recare un danno all'altrui reputazione, intesa come l'immagine di se' presso gli altri.

2. Il secondo motivo è inammissibile.

2.1 Con riferimento alla doglianza di illogicità e contraddittorietà delle motivazioni in ordine all’attendibilità delle dichiarazioni della persona offesa, vanno ricordati i principi espressi sul tema da questa Corte. Il Tribunale di Palmi si è adeguato alla consolidata giurisprudenza di legittimità, secondo la quale le dichiarazioni della persona offesa possono essere assunte anche da sole come prova della responsabilità dell'imputato, purché' siano sottoposte ad un attento controllo circa la loro attendibilità, senza la necessità di applicare le regole probatorie di cui all'articolo 192 cod. proc. pen., commi 3 e 4, che richiedono la presenza di riscontri esterni; fermo restando che, nel caso in cui la persona offesa si sia anche costituita parte civile - e sia, perciò, portatrice di pretese economiche - il controllo di attendibilità deve essere più rigoroso rispetto a quello generico cui si sottopongono le dichiarazioni di qualsiasi testimone e può rendere opportuno procedere al riscontro di tali dichiarazioni con altri elementi (Sez. U, n. 41461 del 19/07/2012, Bell'Arte, Rv. 253214). Detto controllo avviene peraltro nell'ambito di una valutazione di fatto che non può essere rivalutata in sede di legittimità, a meno che il giudice non sia incorso in manifeste contraddizioni (Sez. 2, n. 41505 del 24/09/2013, Terrusa, Rv. 257241).

2.2 La Corte territoriale ha poi confermato la valutazione del Tribunale in ordine all’attendibilità delle dichiarazioni della persona offesa, definendole "coerenti, costanti nel tempo immuni da contraddizioni e scevre da malanimo o risentimento" e idonee a fondare un giudizio di responsabilità dell'imputato, evidenziando che comunque tale giudizio si fonda su molti altri elementi, derivanti dall’attività investigativa della Polizia postale, che ha consentito di associare al profilo del sito (OMISSIS) la famiglia dell'imputato, attraverso l'individuazione dell'indirizzo IP del computer che aveva creato l'account e, nell'ambito del nucleo familiare corrispondente all'utenza telefonica, di risalire all’odierno imputato, grazie all'analisi

dell'hard disk del suo computer portatile. La sentenza di primo grado (la cui motivazione, trattandosi di c.d. "doppia conforme", ben può integrare, come è noto, quella della sentenza d'appello; Sez. 1, n. 8868 del 26/06/2000, Sangiorgi, Rv. 216906; Sez. 2, n. 5606 del 10/01/2007, Conversa, Rv. 236181) sottolinea l'inconferenza di qualsiasi questione sull’attendibilità della persona offesa, dal momento che la circostanza dell'inserimento di un profilo a suo nome emerge obiettivamente e pacificamente da tutto il compendio probatorio acquisito in atti.

3. Il terzo motivo di ricorso, riguardante il diniego di rinnovazione dell'istruttoria, per mancanza di una adeguata motivazione e violazione del diritto alla controprova, è infondato.

3.1 In sede di appello l'imputato aveva richiesto l'escussione delle sorelle (OMISSIS), al fine di verificare l’attendibilità della persona offesa (OMISSIS), la quale aveva dichiarato di aver appreso dell'esistenza del falso profilo sul sito www.badoo.com da una delle due: la donna gli aveva riferito di aver avuto uno spiacevole colloquio in chat con la persona che si celava dietro la sua immagine. La prova era considerata dall'istante una prova "nuova", poiché il nominativo delle (OMISSIS) era emerso solamente nel dibattimento di primo grado; inoltre era stata chiesta una nuova escussione della persona offesa, al fine di approfondire la reale verificazione di un profilo di danno, necessario ai fini della sussistenza del reato.

3.2 Il motivo di doglianza deve ritenersi non accoglibile, costituendo ius receptum, nell'elaborazione giurisprudenziale di questa Suprema Corte, il principio secondo cui la mancata assunzione di una prova decisiva può costituire motivo di ricorso per cassazione, ai sensi dell'articolo 606 c.p.p., lettera D, solo quando si tratti di prove sopravvenute o scoperte dopo la pronuncia di primo grado, che avrebbero dovuto essere ammesse secondo il disposto dell'articolo 603 c.p.p., comma 2; negli altri casi, la decisione istruttoria è ricorribile, ai sensi dell'articolo 606 c.p.p., lettera E, sotto il solo profilo della mancanza o manifesta illogicità della motivazione come risultante dal testo del provvedimento impugnato e sempre che la prova negata, confrontata con le ragioni addotte a sostegno della decisione, sia di

natura tale da poter determinare una diversa conclusione del processo (Sez. 5, n. 34643 del 08/05/2008, De Carlo, Rv. 240995; Sez. 2, n. 44313 del 11/11/2005, Picone, Rv. 232772).

3.3 La prima evenienza deve essere esclusa, poiché' la prova "nuova", che il giudice di appello, in presenza di istanza di parte, è tenuto ad ammettere, con il solo limite costituito dalle ipotesi di richieste concernenti prove vietate dalla legge o manifestamente superflue o irrilevanti (Sez. 1, n. 39663 del 07/10/2010, Cascarino, Rv. 248437) è solo quella "sopravvenuta o scoperta dopo il giudizio di primo grado" e non nel corso di questo, cioè quella con carattere di novità, rinvenibile laddove essa sopraggiunga autonomamente, senza alcuno svolgimento di attività, o quando venga reperita dopo l'espletamento di un'opera di ricerca, la quale dia i suoi risultati in un momento posteriore alla decisione (Sez. 3, n. 11530 del 29/01/2013, A.E., Rv. 254991). In proposito il ricorso si limita a richiamare la deposizione in dibattimento della parte civile, indicando poi nella rubrica del motivo - impropriamente - la lettera D dell'articolo 606 cod. proc. pen..

3.4 Nel caso di specie deve però escludersi anche la seconda ipotesi.

Proprio in ragione del carattere eccezionale della rinnovazione dell'istruzione dibattimentale in appello, infatti, il mancato accoglimento della richiesta in tanto può essere censurato in sede di legittimità, in quanto risulti dimostrata la oggettiva necessità dell'adempimento in questione e, dunque, l'erroneità di quanto esplicitamente o implicitamente ritenuto dal giudice di merito circa la possibilità di "decidere allo stato degli atti", come previsto dall'articolo 603 cod. proc. pen., comma 1; ne discende che il ricorrente deve dimostrare l'esistenza, nell'apparato motivazionale posto a base della decisione impugnata, di lacune o manifeste illogicità, ricavabili dal testo del medesimo provvedimento e concernenti punti di decisiva rilevanza, le quali sarebbero state presumibilmente evitate qualora fosse stato provveduto, come richiesto, all'assunzione o alla riassunzione di determinate prove in sede di appello (Sez. 6, n. 1256 del 28/11/2013 - dep. 14/01/2014, Cozzetto, Rv. 258236). Il ricorrente non ha fornito tale dimostrazione, avendo la Corte d'appello congruamente ed esaustivamente

argomentato, sulla base di una valutazione in fatto non censurabile in sede di legittimità, nel senso della manifesta superfluità dei temi oggetto della richiesta di rinnovazione istruttoria formulata dalla difesa, per la completezza dell'apparato probatorio e le inequivoche ed oggettive risultanze processuali; tale motivazione non può ritenersi di mero stile, laddove si consideri la decisività degli accertamenti operati dalla Polizia postale e la genericità delle richieste istruttorie.

3.5 Per concludere sul punto va ricordato che recentemente si è osservato che mentre la rinnovazione deve essere specificamente motivata, occorrendo dare conto dell'uso del potere discrezionale derivante dalla acquisita consapevolezza di non potere decidere allo stato degli atti, nel caso di rigetto la relativa motivazione può essere anche implicita nella stessa struttura argomentativa posta a base della pronuncia di merito, che evidenzi la sussistenza di elementi sufficienti per una valutazione in senso positivo o negativo sulla responsabilità con la conseguente mancanza di necessità di rinnovare il dibattimento (Sez 5 n. 15320 del 10/12/2009, Pacini, Rv. 246859; Sez. 3, n. 24294 de. 07/04/2010, D. S. B.; Rv. 247872; Sez. 6, n. 30774 del 16/07/2013, Trecca, Rv. 257741) 4. in conclusione il ricorso dell'imputato va rigettato, con conseguente condanna dello stesso al pagamento delle spese processuali ed alla rifusione delle spese sostenute nel grado dalla parte civile, che si liquidano in euro 2000,00, oltre accessori di legge.

P.Q.M.

Rigetta il ricorso e condanna il ricorrente al pagamento delle spese processuali alla rifusione delle spese sostenute nel grado dalla parte civile, liquidate euro 2000,00, oltre accessori di legge.

Editoriale

GIOVANNI CREA
Alcune riflessioni in tema di sicurezza delle ICT in una prospettiva di law and technologies.

Contributi

LUCA BOLOGNINI, GIUSEPPE RAGUSA, CAMILLA BISTOLFI, FRANCESCO COREA, LUCIO SCUDIERO
Effetti dei motori di ricerca sul pluralismo dell'informazione. Aspetti giuridici e di analisi econometrica.

ALESSIA FARANO
Mind detection e protezione dei dati neurogenetici. Alcune riflessioni sulla privacy mentale.

LUIGI PRINZI
Problematiche nella tutela dei dati personali e riflessi nei servizi cloud computing.

Rassegna giuridica

GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI

Opinion 9/2014 on the application of Directive 2002/58/EC to device fingerprinting.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI
Informazioni sulle convinzioni religiose dei pazienti: i casi in cui possono essere raccolte durante il ricovero - 12 novembre 2014.

Provvedimento generale prescrittivo in tema di biometria - 12 novembre 2014.

Giurisprudenza

CORTE DI CASSAZIONE, sez. I civile – sentenza 28 marzo – 7 ottobre 2014, n. 21107.
Offerte di prestazioni sessuali a pagamento "dati sensibili"

CORTE DI CASSAZIONE, sez. V penale – 16 giugno 2014, n. 25774.
Reato di sostituzione di persona

ISTITUTO ITALIANO PRIVACY

ISSN 2239 -7671

Anno V, numero 3, 2014 - Diritto, Economia e Tecnologie della Privacy

€ 25,00