TRATTATO DI DIRITTO COMMERCIALE
E DI DIRITTO PUBBLICO DELL'ECONOMIA
VOLUME QUARANTOTTESIMO

DIRITTO ALL'ANONIMATO

ANONIMATO, NOME E IDENTITÀ PERSONALE

A cura di GIUSELLA FINOCCHIARO

31556 ABen

CASA EDITRICE DOTT. ANTONIO MILANI
CEDAM
CASA EDITRICE DOTT. ANTONIO MILANI
2008

Capitolo II

L'ANONIMATO SU INTERNET
(*Enrico Pelino*)

Sommario: 1. Oggetto del capitolo. – 2. Diritto all'anonimato su Internet. – 3. Contrazione del diritto all'anonimato dinanzi ad altri diritti prevalenti. – 4. Anonimato *online* come condizione giuridica normale. – 5. Limiti specifici all'anonimato su Internet. – 5.1. La direttiva 2006/24/CE. – 5.2. L'art. 132 del d. legisl. 196/2003. – 5.3. Il d.-l. 144/2005. – 5.4. Altre norme che impongono l'identificazione. – 6. Limiti all'anonimato derivanti da posizioni di controllo private. – 6.1. *Cookie* dannosi e meno dannosi. – 6.2. *Third-party cookie* e DoubleClick. – 6.3. Il *cookie* permanente di Google e i *server log*. – 6.4. Contromisure in difesa della privacy. – 6.5. I *web beacon*. – 7. Lo scandalo AOL. – 8. Profili di violazione della normativa sulla protezione dei dati personali. – 9. Combinazione di servizi diversi forniti dallo stesso gestore. – 10. Combinazione di dati provenienti da *database* di soggetti diversi. – 11. Fusioni e acquisizioni aziendali: i pericoli per la privacy. – 12. I pericoli della collaborazione tra multinazionali e governi. – 13. Altre possibilità di identificazione su Internet attraverso la combinazione di informazioni. – 14. Conclusioni.

1. Oggetto del capitolo.

In questo capitolo sono affrontati alcuni aspetti dell'applicazione al contesto di Internet di concetti e categorie analizzati altrove in questo volume con riferimento al mondo fisico, mentre nel successivo si muoverà all'approfondimento di alcuni aspetti di dettaglio, attraverso lo studio di casistica giurisprudenziale. È d'obbligo l'avvertenza che il tema dell'anonimato in Internet si presta ad essere affrontato da una molteplicità di prospettive diverse, tra le quali è necessario operare una scelta. Ad esempio, molto spesso si opta per disamine di taglio pratico dedicate a descrivere tecniche ([1]), strate-

([1]) Quali ad esempio dotarsi di un *firewall* aggiornato, di aggiornati programmi di contrasto a *malware*, e in maniera specifica di programmi di riconoscimento di *spyware, trojan, backdoor, rootkit*, ecc.

gie (2) e strumenti (3) per l'attuazione di forme di anonimato. In altri casi si dà spazio a progetti ed esperienze mirati ad accrescere il livello di anonimato, come Freenet (4), o a stabilire protocolli per una migliore gestione dei dati personali degli utenti, come nel caso del superato P3P. Sotto altra prospettiva, si può considerare l'anonimato su Internet facendo riferimento alla giurisprudenza, anche straniera, sulle richieste di identificazione rivolte agli ISP per condotte ritenute *contra ius* (5). Non si è scelto nessuno di questi approcci, ma si è preferito condurre alcune considerazioni generali sulla garanzia giuridica dell'anonimato in rete, sui suoi limiti e sui soggetti e sulle occasioni che ne determinano una riduzione. Occorre anche richiamare le considerazioni già svolte sulla relatività dell'anonimato, e le definizioni di anonimato positivo/negativo, strumentale/modale, anonimato relativo al rapporto provenienza, di pertinenza, di destinazione già proposte: per tutte si rimanda alla Sez. II, Cap. I di questo volume.

2. Diritto all'anonimato su Internet.

Possono darsi per acquisite al dibattito giuridico le premesse generali sull'architettura, sui protocolli, sul funzionamento e sulle caratteristiche della rete (6), e così pure la tradizionale avvertenza che ogni valutazione in questa materia è inevitabilmente esposta a provvisorietà per via di un contesto estrema-

(2) Si va da quelle più evidenti, quali ad esempio rimozione dei *cookie* (cfr. per un approccio divulgativo, Penenberg, *Cookie Monsters. The innocuous text files that Web surfers love to hate*, in *Slate*, 7 novembre 2005, URL *slate.com/id/2129656*), della cronologia registrata dal *browser*, a quelle meno note, quali per esempio preferire una connessione con IP dinamico, non utilizzare servizi di email e motore di ricerca realizzati dallo stesso soggetto, evitare – ove possibile – di firmare petizioni *online* (data la persistenza dei dati).

(3) Tra i più noti, i classici *anomyser*, *anonymous remailer*, TOR. Su quest'ultimo cfr. Wikipedia, italiano, *Tor*, URL *it.wikipedia.org/wiki/The_Onion_Routing*.

(4) Cfr. URL *freenetproject.org*.

(5) Si pensi ai recenti episodi che hanno visto al centro la casa discografica tedesca Peppermint, relativi a presunte violazioni in materia di diritto d'autore connesse alla riproduzione di file musicali, o ai casi riportati da Solove-Rotenberg, *Information Privacy Law*, New York, 2003, pp. 89-154, oppure infine ai casi Raytheon e Xircom, relativi rispettivamente alla rivelazione di informazioni a proposito di fusioni e acquisizioni e alla pubblicazione di commenti *online* su aziende, per il cui approfondimento si rimanda a Lugaresi, *Internet, privacy e pubblici poteri negli Stati Uniti*, Milano, 2000, pp. 197-199.

(6) Ampie trattazioni tecniche ad uso del giurista si rinvengono da molti anni. Si segnalano, tra i molti, gli ormai classici Borruso – Tiberi, *L'informatica per il giurista*, Milano, 2001 e Cassano (a cura di), *Internet. Nuovi problemi e questioni controverse*, Milano, 2001, volumi ai quali si rimanda per una ricostruzione della storia e del funzionamento generale della rete.

mente mobile (7). Venendo direttamente al tema scelto, sembra necessario, prima di ogni altra considerazione, tenere fermo un punto essenziale: Internet è un mezzo, e, come tale, non sembra in grado di incidere sulle osservazioni generali e sulle idee sviluppate in questo volume a proposito della nozione di anonimato. In particolare, le attività normalmente assistite dalla garanzia giuridica dell'anonimato nel mondo fisico non vedono configurarsi diversamente quest'ultima per il solo fatto di essere effettuate in tutto o in parte con strumenti elettronici collegati alla rete. Si pensi, per fare un esempio immediato, a quei rapporti tra cliente e professionista tradizionalmente garantiti da segreto, come quelli tra paziente e medico o tra cliente e avvocato. Si è notato che in tali casi l'anonimato che deve caratterizzare le eventuali comunicazioni tra professionista e terzi funge di regola da garanzia del segreto. È pertanto strumentale al segreto, perché lo fa salvo pur permettendo la circolazione di informazioni. Occorre tuttavia che l'anonimato risponda alla configurazione più robusta, quella dell'anonimato ragionevole, e che l'oggetto della comunicazione anonima sia sufficientemente generale da escludere qualsiasi inferenza in merito al soggetto tutelato dal segreto.

Stessa cosa deve dirsi per altre ipotesi di anonimato relativo al rapporto di pertinenza individuate in questo volume, quali ad esempio l'anonimato della madre (8), del tossicodipendente, del donatore di sangue, di midollo osseo, di organi. È infatti verosimile il transito di queste informazioni attraverso reti telematiche anche parzialmente collegate ad Internet. È chiaro che anche in tale caso il mezzo (Internet) non incide, né può incidere, sulle garanzie che per legge assistono i dati.

In altri casi l'anonimato è tutelato come modalità di esercizio di un diritto soggettivo da parte di colui che ne è titolare. Ad esempio il diritto alla protezione dei dati personali, il diritto a manifestare il pensiero o il diritto ad associarsi liberamente possono ben esprimersi attraverso comportamenti e osservando forme caratterizzate dalla non identificabilità del titolare dei medesimi (anonimato relativo al rapporto di provenienza) o dell'eventuale destinatario delle comunicazioni (anonimato nel rapporto di destinazione) (9). Si pensi,

---

Tra i volumi di taglio tecnico-giuridico recentemente editi, cfr. MAGGIPINTO – IASELLI, *Sicurezza e anonimato in rete. Profili giuridici e tecnologici della navigazione anonima*, Milano, 2007.

(7) Ampiamente evidenziata già da LUGARESI, *op. cit.*

(8) Cfr. Sez. IV, Cap. I, § 5 e Sez. VI, Cap. III, §§ 1-2.

(9) Cfr. RICCIO, *Diritto all'anonimato e responsabilità civile del provider*, in NIVARRA-RICCIUTO (a cura di), *Internet e il diritto dei privati. Persona e proprietà intellettuale nelle reti telematiche*, Torino 2006, pp. 27-29: "(...L)a dottrina, che ha analizzato la questione solo in rare occasioni, ha considerato l'anonimato come corollario del diritto alla riservatezza o alla libertà

quanto al diritto alla protezione dei dati personali, alla scelta dell'interessato di utilizzare pseudonimi e indirizzi di posta non immediatamente identificativi dinanzi a richieste di conferimento di dati personali come condizioni per la fruizione di un servizio. Può aggiungersi che quando sia possibile sostituire il proprio nome con uno pseudonimo vuol dire che il servizio non ha *realmente* bisogno di identificare l'utente per poter funzionare, e dunque che l'identificazione non può considerarsi a rigore necessaria. L'anonimato si pone allora in tali casi come un mezzo per recuperare, almeno sul piano dell'effettività, il significato normativo dell'art. 3 d. legisl. 196/2003.

Quanto al diritto di associazione, nell'attuale fase di evoluzione della rete, designata come "Web 2.0", e caratterizzata com'è noto dall'attiva partecipazione degli utenti alla creazione di contenuti ([10]), gli esempi di applicazione dell'anonimato positivo sono numerosi. Si pensi anche in queste ipotesi al mascheramento del nome attraverso uno pseudonimo ([11]) in occasione della partecipazione a *forum* di discussione, a *wiki*, a gruppi di lavoro per la promozione di iniziative, a comunità virtuali e ad altre più o meno intense e più o meno spontanee forme di associazione. La riunione dei Garanti europei, il Gruppo *ex* art. 29, osservava già in uno dei suoi documenti seminali sulla privacy in Internet che "(l)a persona interessata deve avere la possibilità di conservare l'anonimato, in particolare quando partecipa ai gruppi di discussione" ([12]).

In maniera analoga, il diritto di manifestare anonimamente il pensiero trova frequente occasione di esercitarsi nella pubblicazione di commenti ad articoli, a *post* (ossia aggiornamenti di *blog*), a filmati, e in generale in relazione a qualsiasi altro contenuto informativo pubblicato in rete. Uno dei più cospicui

---

di manifestare il pensiero. Si è così ritenuto che, proteggendo l'anonimato, si potesse agevolare il completo sviluppo democratico, consentendo ai consociati di esprimere liberamente le proprie opinioni, senza timore di eventuali ripercussioni. (...) La tutela dell'anonimato, connessa alla libertà di manifestazione del pensiero, segna il solco da seguire per realizzare pienamente la *democrazia continua*: l'obiettivo da raggiungere dovrebbe essere, dal lato attivo, quello di rendere i cittadini artefici del processo democratico, attraverso una partecipazione diretta e attiva, che non sia limitata 'al momento estremo di decisione' e, dal lato passivo, quello di aumentare le fonti di informazione". Si consideri anche l'apparato dottrinario citato in nota dall'autore.

([10]) Si va dalla costruzione di *blog*, alle risorse cosiddette di *social software* e *social networking* come Ciao, Youtube, MySpace, Facebook, Meeptup, Flicr; per un elenco più ampio ma non esaustivo, cfr. WIKIPEDIA, *English, List of social networking websites*, URL *en.wikipedia.org/wiki/List_of_social_networking_websites*.

([11]) Sul rapporto tra anonimo e pseudonimo "di mascheramento" si veda Sez. II, Cap. I, nota 15 in questo volume.

([12]) GRUPPO EX ART. 29, *Tutela della vita privata su Internet – Un approccio integrato dell'EU alla protezione dei dati on-line*, 5063/00/IT/DEF, WP 37, p. 42, URL *ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2000/wp37it.pdf*.

esempi di anonimato positivo è in questo senso rappresentato da Wikipedia ([13]), vasta compilazione enciclopedica collettiva continuamente aggiornata da contributori senza nome.

3. Contrazione del diritto all'anonimato dinanzi ad altri diritti prevalenti.

Si deve ricordare che il diritto all'anonimato come modalità di espressione di un diritto protetto in via principale cede soltanto dinanzi all'esito sfavorevole del bilanciamento rispetto ad altra situazione giuridicamente tutelata. È il caso, assai tipico, della diffamazione *online*, dinanzi alla quale il diritto all'anonimato, normalmente connesso con il diritto di manifestare il pensiero e con il diritto alla protezione dei dati personali, soccombe al diritto al rispetto della reputazione e dell'onore altrui. È anche il caso dei reati pedopornografici, il cui accertamento e la cui repressione sono evidentemente preminenti rispetto al mantenimento dell'anonimato.

Si è descritto altrove questo anonimato del reo come anonimato negativo. Altre volte il diritto all'anonimato cede anche nel bilanciamento con diritti patrimoniali, laddove siano poste in essere condotte criminose di particolare gravità. È il caso di attacchi che determinano la temporanea inutilizzabilità di siti *web*, praticati talvolta per sfida, provocazione o contestazione politica (danneggiamento da *defacement* ([14]) o da *Ddos attack* ([15])), e più spesso costituenti invece momenti della realizzazione di condotte estorsive (estorsione attraverso *Ddos attack* ([16])); è anche il caso degli accessi abusivi a sistema informatico o, per fare altro esempio, dei furti di identità.

Altrove il bilanciamento tra diritto alla tutela dei dati personali e diritti patrimoniali confliggenti si risolve a favore del primo. È il caso per esempio dei rapporti con il diritto *economico* d'autore secondo l'assetto disegnato da

---

([13]) Cfr. URL *wikipedia.org*.

([14]) Cfr. Staff Zone-H, *Ahmadinejad's blog hacked and defaced*, 29 agosto 2006, URL *www.zone-h.org/content/view/14106/30*.

([15]) Cfr. Kirk, *Analysis: Russian Gov't Not Behind Estonia DDOS Attacks*, in *Pc World* 1° giugno 2007, URL *www.pcworld.com/article/id,132469-pg,1/article.html*; cfr. anche Staff ZDNet, *Al-Jazeera suffers DoS attack*, 27 marzo 2003, URL *news.zdnet.co.uk/itmanagement/0,1000000308,2132585,00.htm*.

([16]) Cfr. Leyden, *Russian bookmaker hackers jailed for eight years*, in *The Register*, 4 ottobre 2006, URL *www.securitypronews.com/news/securitynews/spn-45-20061006GangJailedinRussiaforDDoSBlackmail.html*; Staff BBC, *UK version*, *Blackmailers target $1m website*, 18 gennaio 2006, URL *news.bbc.co.uk/1/hi/technology/4621158.stm*.

recente decisione del tribunale di Roma, pur in presenza di asserite violazioni da parte di utenti anonimi, che avrebbero potuto integrare profili penali ([17]). La materia appare comunque ben lungi dall'avere trovato una soluzione stabile e, al di là della valutazione giurisprudenziale sulla vicenda citata, senz'altro condivisibile a giudizio di chi scrive, anche tenuto conto delle sue peculiari caratteristiche, occorre infatti riconoscere che il problema del bilanciamento tra la tutela dell'anonimato in Internet e la necessità di identificare gli autori di condotte ritenute ingiustamente pregiudizievoli rispetto a diritti altrui rappresenta questione estremamente problematica e di non immediata soluzione, neppure affrontabile comunque nello spazio di questo breve articolo oltre le linee generali già esposte.

4. Anonimato *online* come condizione giuridica normale.

Se si considera che le relazioni intrattenute in Internet si esprimono in informazioni, e cioè attraverso dati potenzialmente personali ([18]), e se è vero che

([17]) Si tratta di Trib. Roma, ord. 16 luglio 2007 sul già richiamato caso Peppermint. In merito al bilanciamento, il giudice romano ha osservato: "(...D)eve rilevarsi come la questione fondamentale dell'infondatezza di tale pretesa (ci si riferisce alla richiesta di istanza cautelare *ex* art. 156 *bis* l. 633/41, per ottenere dall'ISP l'identificazione degli utenti assegnatari di alcuni numeri IP, *n.d.a.*) sia rappresentata dall'anzidetto limite della segretezza delle comunicazioni elettroniche e telematiche tra privati, quale diretta espressione di tutela di interessi di rilevanza costituzionale (art. 2 e 15 Cost.), che la normativa esistente consente di superare solo in funzione della tutela di valori ed interessi della collettività con eguale e superiore rilevanza costituzionale, e sempre in un'ottica di equilibrio e comparazione. Infatti, l'unica possibilità ammessa di compressione di tali diritti personalissimi è quella strumentale all'accertamento, prevenzione e repressione di illeciti penali di particolare gravità, ossia quelli previsti dall'art. 407, 2° comma lett. a) del c.p.p. (delitti associativi con finalità di terrorismo, di tipo mafioso ecc., e delitti per i quali è previsto l'arresto obbligatorio in flagranza, giacché puniti con pena detentiva superiore, nel minimo, ad anni cinque di reclusione) e quelli in danno di sistemi informatici". Deve anche notarsi che nel caso di specie l'ampiezza, la durata, la segretezza dell'operazione di schedatura, la scelta di non segnalare immediatamente le presunte violazioni all'autorità ma di esercitarne surrettiziamente in via privata alcune prerogative di indagine, le modalità della transazione proposta agli interessati, tutte queste caratteristiche rendevano da un lato particolarmente vasta e intensa la lesione della sfera individuale degli interessati e dall'altro configuravano la pretesa della ricorrente piuttosto come un'occasione di speculazione economica che come l'esercizio di un diritto violato. In definitiva, in aggiunta alle esatte considerazioni svolte dal Tribunale di Roma, sembrano anche affacciarsi nel caso di specie ulteriori profili di illegittimità riconducibili all'esercizio arbitrario delle proprie ragioni o, quantomeno, all'abuso di diritto. Le precedenti decisioni, di segno contrario, dello stesso giudice su vicende del tutto analoghe appaiono peraltro di modesto significato, in quanto fortemente carenti nella stessa individuazione dei diritti da bilanciare.

([18]) Peraltro, come si vedrà meglio in seguito, alcune caratteristiche peculiari di Internet

l'"anonimato modalità" estende all'utente anonimo la tutela giuridica assicurata dal diritto riconosciuto in via principale, in questo caso il diritto alla protezione dei dati personali, non è inesatto concluderne che l'anonimato dell'utente nell'ambiente Internet riceve di regola tutela giuridica, mentre l'identificazione va considerata in diritto come un'eccezione. In proposito il considerando n. 24 della direttiva 2002/58/CE chiarisce espressamente che "(l)e apparecchiature terminali degli utenti di reti di comunicazione elettronica e qualsiasi informazione archiviata in tali apparecchiature fanno parte della sfera privata dell'utente, che deve essere tutelata ai sensi della convenzione europea per la protezione dei diritti dell'uomo e delle libertà fondamentali". L'art. 123 d. legisl. 196/2003, norma con la quale sono state recepite alcune disposizioni della direttiva citata, enuncia il principio generale che l'anonimato delle comunicazioni elettroniche va ripristinato non appena i dati relativi al traffico "non sono più necessari ai fini della trasmissione della comunicazione elettronica", fatte salve le esigenze di fatturazione, di commercializzazione di servizi di comunicazione elettronica o fornitura di servizi a valore aggiunto richiesti dall'abbonato e dall'utente, e fatte salve le ipotesi di cui all'art. 132, che saranno esaminate al successivo par. 5.2. Questa condizione giuridica di anonimato normale e di identificazione eccezionale sembra peraltro direttamente riconducibile al principio di necessità di cui all'art. 3 d. legisl. 196/2003 (oltre che del principio di proporzionalità), di cui veramente occorre segnalare una volta di più la portata generale. Questa lettura ha ricevuto di recente puntuale conferma dall'Autorità Garante per la protezione dei dati personali: "Partendo dal principio secondo il quale i dati non devono essere formati se non sono necessari e proporzionati ai fini della funzionalità della rete o della prestazione del servizio (artt. 3 e 11 del Codice), il legislatore ha stabilito il divieto generale di conservazione dei dati relativi al traffico (art. 123, comma 1° cit.), con le seguenti eccezioni:

– è consentito il trattamento di dati strettamente necessario a fini di fatturazione per l'abbonato, ovvero di pagamenti in caso di interconnessione (nei limiti e con le modalità di cui all'art. 123, comma 2°) o, previo consenso dell'utente, a fini di commercializzazione di servizi di comunicazione elettronica, per la durata a ciò necessaria (art. 123, comma 3°);

---

fanno sì che qualsiasi dato, anche quello apparentemente anonimo, possa per effetto di successivo trattamento che lo collega ad altri dati divenire dato personale. È sufficiente considerare in questo senso caratteristiche peculiari della rete quali la tendenziale permanenza di dati oltre i parametri di obsolescenza naturalmente seguiti nel mondo fisico e la possibilità di incroci tra diverse banche di dati anche a seguito di imprevedibili operazioni di acquisizione e fusione di aziende.

– è prescritta la conservazione dei dati di traffico per esclusive finalità di accertamento e repressione dei reati (art. 132 del Codice)" ([19]). Va ribadito che la ragione di questa riduzione della conservazione dei dati al minimo necessario è in funzione di un più generale principio di riduzione al minimo necessario di qualsiasi trattamento di dati dell'utente, come del resto evidenziato con nettezza nella risoluzione recentemente adottata alla 28ª conferenza internazionale delle Autorità Garanti tenutasi a Londra il 2-3 novembre 2006 ([20]).

Si può anticipare che questo generale diritto all'anonimato *online*, derivante dall'applicazione della normativa sulla protezione dei dati personali oltre che dall'attuazione dei diritti riconosciuti nella CEDU, costituisce, come si vedrà, materia di difficile contenzioso nei confronti di quei motori di ricerca che procedono a macroscopiche raccolte di dati personali in occasione della navigazione degli utenti attraverso i loro siti.

5. Limiti specifici all'anonimato su Internet.

Si è fatto riferimento nei paragrafi precedenti alla contrazione del diritto all'anonimato su Internet per effetto del bilanciamento con diritti prevalenti. Si sono anche indicate le ipotesi in cui l'anonimato subisce per legge una limitazione, peraltro temporanea, in applicazione dell'art. 123, commi 2° e 3° d. legisl. 196/2003. Occorre ora esaminare altre ipotesi eccezionali di limitazione dell'anonimato previste dal legislatore.

5.1. *La direttiva 2006/24/CE.*

Si tratta innanzitutto della recente direttiva 2006/24/CE, che, modificando la precedente 2002/58/CE, armonizza la normativa degli Stati membri in relazione agli obblighi di conservazione dei dati e ai tempi minimi e massimi consentiti per questo trattamento. La direttiva, che avrebbe dovuto già essere attuata nel nostro Paese ([21]), riguarda sia i dati relativi al tradizionale traffico

---

([19]) Cfr. Garante prot. dati pers., delibera, 19 settembre 2007, in *Boll.*, n. 87, doc. web. n. 1442463.

([20]) Cfr. *Risoluzione sulla protezione della privacy e i motori di ricerca*, URL *ec.europa.eu/justice_home/fsj/privacy/news/docs/pr_google_annex_16_05_07_en.pdf*, p. 2.

([21]) La direttiva, a norma dell'art. 15, comma 1°, avrebbe dovuto essere recepita integralmente entro il 15 settembre 2007, non avendo l'Italia scelto di usufruire, come previsto dall'art. 15, comma 3°, del più lungo termine del 15 marzo 2009 per l'applicazione delle sole norme sul

telefonico, argomento che si colloca al di fuori di questo specifico contributo, sia di quelli relativi al traffico su Internet, compreso il VoIP e gli *sms* inviati via *web*. Con questo atto normativo vengono posti specifici obblighi in capo a quei soggetti che realizzano esclusivamente o prevalentemente una trasmissione di segnali su reti di comunicazioni elettroniche, a prescindere dall'assetto proprietario della rete, e che offrono servizi a utenti finali secondo il principio di non discriminazione ([22]), ossia in definitiva, per quanto concerne il traffico telematico, agli ISP. I dati telematici oggetto degli obblighi di conservazione sono quelli relativi sia al mittente o al chiamante via VoIP sia al destinatario della comunicazione. A norma dell'art. 5, comma 1°, lett. a), n. 2 e lett. b), n. 2 della citata direttiva, i dati di cui è richiesta la conservazione rispetto alle due tipologie enunciate di interessati (mittente e destinatario) sono in estrema sintesi i seguenti:

- nome, cognome e indirizzo;
- ID utilizzati;
- numeri VoIP, sempre che i dati viaggino su rete telefonica pubblica;
- numeri per l'accesso via *dial-up* o ADSL;
- giorno, ora e durata della comunicazione (dal *log-in* al *log-off*);
- servizio Internet utilizzato.

Non sono invece registrati i contenuti delle comunicazioni ([23]). Vengono in definitiva perciò ad essere limitati quelli che altrove si sono definiti come l'anonimato relativo al rapporto di provenienza e quello relativo al rapporto di destinazione. Nessuna compressione subisce invece l'anonimato relativo al rapporto di pertinenza, dato che i contenuti delle comunicazioni, come si

---

traffico telematico. Tuttavia, alla data in cui si scrive (ottobre 2007), v. per completezza anche p. 331, nota 24 non si ha alcuna notizia certa circa i tempi del recepimento. Cfr. sul punto CONSIGLIO NAZIONALE FORENSE, *Rassegna quotidiana*, 22 ottobre 2007, URL *www.consiglionazionaleforense.it/visualizzazioni/vedi_dettagli.php?areanumber=40&action=view&idmessaggio=4778*. Non risultano al momento avviate procedure d'infrazione contro il nostro Paese. Il Garante per la protezione dei dati personali ha avviato una pubblica consultazione sulla direttiva (ved. *infra* n. 19) da concludersi il 31 ottobre 2007.

([22]) Cfr. Garante prot. dati pers., *ult. provv. cit.*

([23]) Cfr. *ibidem*: "I dati relativi al traffico telefonico e telematico sono informazioni che dovrebbero riguardare solo alcune caratteristiche esteriori delle conversazioni, delle chiamate e delle comunicazioni, senza permettere di desumerne, almeno direttamente, i contenuti". Particolarmente rilevante l'osservazione che nel caso di comunicazioni telematiche "(n)on di rado, i dati esteriori a tali comunicazioni possono essere infatti anche indirettamente espressivi del contenuto di messaggi, consultazioni in rete di documenti e di dialoghi, sempre in rete, tra soggetti definiti. Taluni dati possono permettere anche di desumere particolari orientamenti, convincimenti e abitudini di ordine politico, sindacale o religioso o attinenti alla sfera della salute o della vita sessuale."

è evidenziato, non sono interessati dalle norme citate. Il periodo di conservazione è individuato in una finestra piuttosto ampia, dai sei mesi ai due anni, il che pone alcuni problemi di compatibilità con l'attuale normativa, almeno quanto alla telefonia fissa e mobile, problemi che peraltro, in attesa di conoscere il contenuto del decreto di attuazione, pare prematuro affrontare.

5.2. *L'art. 132 del d. legisl. 196/2003.*

È necessario ricordare che l'acquisizione e la conservazione di una parte significativa delle informazioni menzionate avviene già nel nostro Paese a norma dell'art. 132 d. legisl. 196/2003 (attuativo anche di alcune disposizioni della direttiva 2002/58/CE), così come modificato dal c.d. "pacchetto Pisanu", vale a dire il decreto legge 27 luglio 2005, n. 144, convertito con legge 31 luglio 2005, n. 155. Va evidenziato che l'utilizzo di queste informazioni è possibile soltanto per l'accertamento e la repressione di reati, secondo un regime graduato in base alla gravità degli stessi. In particolare, nel caso del traffico telematico, per tutti i reati è previsto un tempo di conservazione di sei mesi, ai sensi dell'art. 132, comma 1°, che diventano dodici nel caso delle fattispecie particolarmente gravi di cui all'articolo 407, comma 2°, lett. a) del codice di procedura penale e dei delitti in danno di sistemi informatici o telematici. Esiste in definitiva un chiaro vincolo di finalità che regola l'accesso ai dati conservati, il che porta a ribadire la regola che la condizione giuridica normale nella fruizione dei servizi Internet è quella dell'anonimato. Deve essere chiaro che ci si riferisce qui sempre e comunque, come più volte ribadito in altre parti di questo volume, ad un anonimato relativo, nel senso che esiste sempre un soggetto in relazione al quale l'utente non è anonimo (il fornitore del servizio di comunicazione). Peraltro anche nei confronti di tale soggetto, si noti, la perdita dell'anonimato è soltanto temporanea e quest'ultimo viene ripristinato una volta che sia trascorso il tempo massimo di conservazione dei dati.

È particolarmente interessante riflettere sul significato di questa garanzia all'anonimato *online* assunta quale condizione giuridica originaria, che può subire compressioni, ma che, all'esaurirsi delle stesse, torna elasticamente a recuperare la sua iniziale estensione. In ciò si coglie infatti un rovesciamento della tradizionale impostazione italiana, rispecchiata, tra molti, nell'articolo di Candian più volte citato ([24]), che vede l'identificazione come la condizione giuridica originaria e l'anonimato come l'anomalia.

([24]) CANDIAN, *op. cit.*

5.3. *Il d.-l. 144/2005.*

Il d.-l. 144/2005 ha introdotto una serie di misure volte a porre sotto controllo, tra l'altro, il traffico telematico e a stabilire procedure di identificazione. In applicazione dell'art. 7, comma 4°, i titolari e i gestori di esercizi pubblici (tipicamente, ma non solo, gli Internet *cafe*) e di circoli privati sono tenuti ad identificare chiunque, cliente o socio, utilizzi apparecchi terminali messi a disposizione per comunicazioni telematiche (cfr. anche il decreto ministeriale attuativo di tale previsione, decreto ministeriale 16 agosto 2005). In tal modo la navigazione effettuata può essere associata ad un soggetto individuato. È stata inoltre sospesa l'applicazione di qualunque disposizione che prescriva o consenta la cancellazione dei dati di traffico, anche se non soggetti a fatturazione, fino alla data del 31 dicembre 2007. Sono state anche apportate modifiche all'art. 132 del d. legisl. 196/2003, in parte già ricordate nel precedente paragrafo. Va segnalato che, in seguito alla modifica del comma 3° dell'art. 132, entro il termine dei primi 6 mesi di conservazione del traffico telematico il Pubblico Ministero, con decreto motivato, e senza necessità di provvedimento del giudice (come era in precedenza), può acquisire tali dati dal fornitore del servizio. Non è prevista dal decreto legge in questione la conservazione dei contenuti delle comunicazioni. Il prevalente interesse pubblico alla base di queste limitazioni dell'anonimato starebbe in un'esigenza di sicurezza in relazione a possibili minacce terroristiche e ad altre emergenze criminali.

A riportare parzialmente questo eccezionale pacchetto di misure entro una più equilibrata cornice giuridica, vi è peraltro l'ormai prossima scadenza al 31 dicembre del 2007 (prorogata al 31 dicembre 2008 dall'art. 34 d.-l. 248/2007, in attesa di conversione) dell'accennato termine di sospensione delle norme in materia di conservazione e cancellazione dei dati, con conseguente recupero della disciplina normale. È pure necessario ribadire che i contenuti delle comunicazioni sono fatti salvi, né è impedito l'uso di *remailer* e di *anonymiser*. Inoltre si deve ricordare che la ricostruzione dei percorsi telematici degli utenti è possibile soltanto in presenza di precise condizioni giuridiche e fattuali. Infatti, pur tenendo conto dei notevoli poteri del P.M. nei primi sei mesi di conservazione dei dati, occorre quantomeno che ricorrano ipotesi di reato individuate in un decreto motivato. Peraltro, sotto un profilo meramente pratico, l'incrocio dei *log* degli ISP con i tabulati tenuti dai gestori degli Internet *cafe* si trova comunque esposto all'incertezza derivante dalla corretta tenuta di questi ultimi ([25]).

([25]) Ad esperienza dello scrivente, e nei limiti in ciò può avere valore, l'effettivo rispetto dell'obbligo di registrazione degli utenti non risulta sempre seguito.

Le norme del d. legisl. 196/2003, il pacchetto Pisanu e la direttiva 2006/24/CE, destinata ad attuazione nell'immediato futuro, compongono una disciplina dettagliata e complessa, che introduce una serie di significative riduzioni del generale diritto all'anonimato in Internet. Come già notato, tuttavia, le compressioni vere e proprie emergono solo in corrispondenza della realizzazione di attività criminose in rete, e anche in questo caso possono avvenire non oltre un preciso limite temporale. Si aggiunga l'elemento, assai rilevante, che sono esclusi i contenuti, e dunque è fatto salvo quantomeno l'anonimato relativo al rapporto di pertinenza. Tutto ciò considerato, non sembra di poter dire che l'utente veda erose in maniera irreparabile dalla legislazione vigente le sue possibilità di navigazione anonima ([26]).

5.4. *Altre norme che impongono l'identificazione.*

Altre residuali eccezioni alla regola generale dell'anonimato riguardano i soggetti che svolgono alcune attività in Internet. Si tratta ad esempio di coloro che effettuano pubblicazioni periodiche *online*, qualificabili come "prodotti editoriali" agli effetti del discusso art. 1, comma 1° della legge 7 marzo 2001, n. 62, i quali sono tenuti, a norma del comma 3° dello stesso articolo, a osservare gli obblighi previsti dall'art. 2 della legge 47/48 per gli stampati cartacei, ossia: indicazione del luogo e dell'anno della pubblicazione, del nome e domicilio dello stampatore e, se esiste, dell'editore, e, per i giornali, le agenzie d'informazione e i periodici, il nome del proprietario e del direttore o vice direttore responsabile. Se il "prodotto editoriale" è diffuso al pubblico con periodicità regolare ed è contraddistinto da una testata, costituente elemento identificativo del prodotto, è sottoposto, altresì, agli obblighi di registrazione previsti dall'articolo 5 della medesima legge n. 47/48.

Altri limiti sono posti dal codice del consumo, di cui al d. legisl. 6 settembre 2005, n. 206, che in materia di contratti a distanza all'art. 52, comma 1°, lett. a) dispone che "(i)n tempo utile prima della conclusione di qualsiasi contratto a distanza, il consumatore deve ricevere le seguenti informazioni: a) identità del professionista e, in caso di contratti che prevedono il pagamento anticipato, l'indirizzo del professionista (...)". In definitiva il professionista che

([26]) Naturalmente il discorso è più complesso di quanto sia possibile dare conto in queste brevi note, potendo talvolta attività normalmente lecite non essere considerate tali sotto regimi repressivi (è il caso che si menzionerà più avanti della cessione di dati da parte di Yahoo! al governo cinese). Non può neppure tacersi che i già segnalati poteri attribuiti al P.M. dal pacchetto Pisanu aprono alcuni squarci nelle garanzie giuridiche dell'interessato.

svolga attività commerciale *online* è soggetto all'obbligo di rivelare la propria identità.

Tutti questi limiti specifici, si noti, riguardano essenzialmente l'identificazione del soggetto che immette informazioni, quello che altrove si è definito l'anonimato relativo al rapporto di provenienza, ma non riguardano l'anonimato relativo al rapporto di pertinenza.

6. Limiti all'anonimato derivanti da posizioni di controllo private.

Limiti ben più intensi, seppur meramente fattuali, all'anonimato degli utenti, tali anzi da ridurlo in misura pressoché totale, derivano piuttosto dalla gestione di alcune posizioni di controllo private su settori chiave del traffico in rete. Si tratta soprattutto della posizione dei fornitori di motori di ricerca, articolazioni decisive nella fruizione dei contenuti *online*, e dei fornitori di servizi di posta elettronica, essenziali strumenti di relazione interpersonale. I soggetti che nel panorama mondiale controllano i principali motori di ricerca sono sostanzialmente quattro: Google, Yahoo!, Microsoft e AOL. Una quota molto ridotta è gestita da un quinto motore, che fa capo a Ask. Google, in particolare, occupa un ruolo assolutamente dominante nel settore (27), ed è stato recentemente oggetto di preoccupate prese di posizione da parte del Gruppo *ex* art. 29 dei Garanti europei (28), prese di posizione che da un lato hanno esposto macroviolazioni della normativa sulla protezione dei dati personali, e dall'altro hanno anche messo in luce le particolari difficoltà in cui si trovano le Autorità europee nel gestire il confronto con grandi soggetti econo-

(27) Cfr., solo a titolo di esempio, la statistica aggiornata al 19 ottobre 2007 della Nielsen Online, URL *www.netratings.com/pr/pr_071019.pdf*, in base alla quale Google si trova al primo posto con il 54% del totale delle ricerche effettuate tramite motori, segue Yahoo! con solo il 19,5%, Microsoft con il 12%, AOL con il 6%.

(28) Il 14 marzo 2007 la società, in seguito alle pressioni ricevute, ha annunciato la riduzione del periodo di conservazione dei dati degli utenti a 18-24 mesi, cfr. Fleischer-Wong, *Taking steps to further improve our privacy practices*, in *Official Google blog*, URL *googleblog.blogspot.com/2007/03/taking-steps-to-further-improve-our.html* (*permalink*). Cfr. anche Google, *Google Log Retention Policy FAQ*, URL *64.233.179.110/blog_resources/google_log_retention_policy_faq.pdf*. Successivamente il Gruppo *ex* art. 29 ha chiesto ulteriori chiarimenti, con una pubblica lettera del 6 maggio 2007, URL *ec.europa.eu/justice_home/fsj/privacy/news/docs/pr_google_16_05_07_en.pdf*. Il 16 luglio 2007 Google accettava la riduzione a 18 mesi per l'Europa e la limitazione della validità del proprio *cookie* a due anni, cfr. Fleischer, Cookies: *expiring sooner to improve privacy*, in *Official Google blog*, URL *googleblog.blogspot.com/2007/07/cookies-expiring-sooner-to-improve.html* (*permalink*).

mici posizionati in settori chiave. Essenzialmente, il problema sta in questi termini: Google registra tutte le informazioni relative alle ricerche che vengono effettuate da qualsiasi utente che si serva del suo motore. Si tratta essenzialmente delle parole chiave digitate, delle pagine e dei *link* effettivamente selezionati ([29]), associati all'IP dell'utente e al *cookie* unico di Google, e contrassegnati con una marca temporale ([30]). Il *cookie* unico di Google è un codice permanente associato a ciascuna macchina che si connette a Google.

6.1. Cookie *dannosi e meno dannosi.*

Per inquadrare in maniera più chiara il problema, occorre fare alcune precisazioni di ordine sistematico rispetto ai *cookie*, che, pur oggetto da molto tempo di analisi giuridica, non sono stati sempre distinti con attenzione rispetto alle loro diverse tipologie. Va innanzitutto evidenziato che i *cookie* non sono tutti ugualmente pericolosi in termini di violazione della privacy dell'utente ([31]). Certamente è vero che in generale essi permettono al soggetto che li

---

([29]) Cfr. URL *www.google.com/intl/it/privacy_faq.html#*, punto 5: "Quando cliccate su un *link* visualizzato su Google, il fatto che avete cliccato su tale *link* potrà essere comunicato a Google. In tal modo, Google è in grado di memorizzare informazioni su come utilizzate il nostro sito ed i nostri servizi".

([30]) Cfr. URL *www.google.com/intl/it/privacy_faq.html#*, punto 4: "Come la maggior parte dei siti *web*, i nostri *server* registrano automaticamente le pagine che vengono richieste dagli utenti quando questi visitano i nostri siti. Questi 'log del server' comprendono normalmente quali *web* avete richiesto, l'indirizzo del Protocollo Internet, il tipo di *browser*, il linguaggio del *browser*, la data e l'ora della vostra richiesta ed uno o più *cookie* che possono identificare il vostro *browser* in modo univoco".

([31]) Tecnicamente è opportuno sottolineare che si tratta non di software, cioè di programmi con istruzioni eseguibili, ma soltanto di file di testo, ossia con estensione ".txt", dunque i *cookie* non possono far compiere all'elaboratore operazioni di alcun tipo, come accade tipicamente con il *malware*. La funzione dei *cookie* è in termini generali quella di facilitare la gestione del sito agli utenti, memorizzando informazioni quali ad esempio pagine e sottopagine già visitate, e facilitare in questo modo la navigazione *online* evitando all'utente di inserire nuovamente tali informazioni. Si tratta in un certo senso di segnalibri virtuali. Esistono *cookie* di sessione, che spariscono automaticamente all'uscita dell'utente da un sito, e più problematici *cookie* permamenti. Per un esame della materia, cfr. i seguenti studi giuridici: CARIDI, *La tutela dei dati personali in internet: la questione dei* logs *e dei* cookies *alla luce delle dinamiche economiche dei dati personali*, in *Dir. inf.*, 2001, pp. 763-783; GRJVA ZABERT, *Trattamento dei dati personali e tutela della privacy nelle comunicazioni elettroniche (Commento a Dir. CE 2002/58)*, in *I Contratti*, 2002, pp. 1069-1071; MAGRO, *Internet e privacy. L'utente consumatore e modelli di tutela penale della riservatezza*, in *Ind. pen.*, 2005, pp. 931-981; STUMPO, *Privacy e Internet: un connubio ancora difficile*, in *Riv. pers. ente loc.*, 2001, pp. 53-83; TOSI, *Prime osservazioni sull'applicabilità della disciplina generale della tutela dei dati personali a Internet e al commercio elettronico*, in *Dir. inf.*, 1999, pp. 591-607.

rilascia di associare determinati contenuti informativi ad un utente univocamente identificato, aprendo perciò la strada a forme di profilazione, soprattutto a scopo commerciale. È però anche vero che tali strumenti svolgono anche funzioni positive che riverberano sia a vantaggio del fornitore di servizi sia a vantaggio dell'utente che li utilizza. Si tratta in particolare di facilitazioni alla navigazione, personalizzazione di servizi, recupero di informazioni, la cui utilità è stata riconosciuta anche a livello europeo ([32]). In definitiva, fin quando l'accesso alla storia della navigazione personale si mantiene atomizzato sia sotto il profilo soggettivo sia sotto quello oggettivo, nel senso che i *cookie* vengono installati da una pluralità di soggetti distinti che hanno accesso soltanto alla porzione della navigazione dell'utente relativa alle pagine da loro direttamente pubblicate, il bilanciamento tra vantaggi in termini di servizi e svantaggi in termini di riduzione della privacy appare sostanzialmente equilibrato e il fenomeno, nelle sue linee generali, non sembra destare reale preoccupazione ([33]). Come sempre accade in materia di protezione dei dati personali, stabilire dei "muri", delle aree di incomunicabilità tra *database* diversi, rappresenta infatti uno dei modi più efficaci di tutelare la privacy. La situazione evidentemente

([32]) Cfr. direttiva 2002/58/CE, considerando n. 25: "Tuttavia, tali dispositivi, per esempio i cosiddetti marcatori ('cookies'), possono rappresentare uno strumento legittimo e utile, per esempio per l'analisi dell'efficacia della progettazione di siti web e della pubblicità, nonché per verificare l'identità di utenti che effettuano transazioni 'on-line'. Allorché tali dispositivi, ad esempio i marcatori ('cookies'), sono destinati a scopi legittimi, come facilitare la fornitura di servizi della società dell'informazione, il loro uso dovrebbe essere consentito purché siano fornite agli utenti informazioni chiare e precise, a norma della direttiva 95/46/CE, sugli scopi dei marcatori o di dispositivi analoghi per assicurare che gli utenti siano a conoscenza delle informazioni registrate sull'apparecchiatura terminale che stanno utilizzando. Gli utenti dovrebbero avere la possibilità di rifiutare che un marcatore o un dispositivo analogo sia installato nella loro apparecchiatura terminale. Ciò riveste particolare importanza qualora utenti diversi dall'utente originario abbiano accesso alle apparecchiature terminali e quindi a dati contenenti informazioni sensibili in relazione alla vita privata che sono contenuti in tali apparecchiature. L'offerta di informazioni e del diritto di opporsi può essere fornita una sola volta per l'uso dei vari dispositivi da installare sull'attrezzatura terminale dell'utente durante la stessa connessione e applicarsi anche a tutti gli usi successivi, che possono essere fatti, di tali dispositivi durante successive connessioni. Le modalità di comunicazione delle informazioni, dell'offerta del diritto al rifiuto o della richiesta del consenso dovrebbero essere il più possibile chiare e comprensibili. L'accesso al contenuto di un sito Internet specifico può tuttavia continuare ad essere subordinato all'accettazione in conoscenza di causa di un marcatore o di un dispositivo analogo, se utilizzato per scopi legittimi".

([33]) Esistono per la verità anche altre ragioni di attenzione, segnalate da attenta dottrina già molti anni fa, cfr. Tosi, *op. ult. cit.*, p. 604, che ravvisa l'illiceità di questo strumento "(...) qualora il c.d. *cookie* registri – senza il consenso dell'interessato – un profilo del consumatore non in forma anonima ma riferibile immediatamente ad un utente individuato oppure non si limiti alla registrazione di dati di natura commerciale ma trasferisca informazioni relative al contenuto della memoria di massa del computer di navigazione".

muta in maniera radicale quando l'atomizzazione venga meno sotto il profilo soggettivo o sotto quello oggettivo. Nel primo caso, quello che attualmente si registra, può accadere che uno stesso soggetto abbia accesso ad una sostanziale porzione della navigazione dell'utente o comunque ad una porzione che comprende *anche* pagine create da soggetti diversi. Ciò sembra attualmente avvenire nei seguenti casi: abusivo accesso a *cookie* collocati da altri soggetti; *cookie* di produttore terzo rispetto al soggetto che li colloca, c.d. *third party cookie*; *cookie* collocati da motori di ricerca. A parte la prima ipotesi, evidentemente patologica e comunque limitata nella casistica, le ultime due paiono assai interessati sia per la parvenza di legittimità giuridica sia per i rischi, notevoli, che comportano in termini di tutela dei dati personali e dell'anonimato.

6.2. Third-party cookie *e DoubleClick.*

Caso veramente paradigmatico di *cookie* realizzati da terze parti è rappresentato da quelli distribuiti dalla società DoubleClick, che ha costruito una parte significativa della propria fortuna commerciale su tali strumenti. In sostanza, la società in questione sottoscrive accordi commerciali con soggetti terzi gestori di siti, che si impegnano ad installare *cookie* di DoubleClick sull'*hard disk* degli utenti di volta in volta collegati. In questo modo la società in questione ottiene l'accesso a, e dunque può associare fra loro, tutte le informazioni relative ai siti aderenti al suo programma visitati dall'utente. È chiaro che in questo contesto i rischi di profilazione sono notevoli ([34]), e non a caso il *cookie* di DoubleClick viene spesso marcato da programmi di contrasto a *malware* e ad altre minacce informatiche come *tracking cookie* ([35]), ossia come *cookie* di

([34]) Secondo la denuncia depositata da Epic il 20 aprile 2007 alla Federal Trade Commission, cfr. EPIC, *Complaint and Request for Injunction, Request for Investigation and for Other Relief*, URL *www.epic.org/privacy/internet/ftc/DCLK_complaint.pdf*, p. 4: "DoubleClick ha compilato ad oggi approssimativamente 100 milioni di profili di utenti Internet".

([35]) PENENBERG, *op. cit.*,: "Le eccezioni sono costituite da *third-party cookie*, noti anche come 'tracking cookie', collocati da un soggetto (in genere una società di *marketing* o di pubblicità) interessata nel catalogare i visitatori. In molti casi servono a fare in modo che l'utente non riceva lo stesso messaggio pubblicitario due volte; in altri casi assicurano che chi si interessa ad esempio di eventi sportivi riceva pubblicità diverse da chi ha l'hobby dei *gadget*. Ma i *third-party cookie* potrebbero anche essere usati per realizzare profili di abitudini nella navigazione"; cfr. anche WIKIPEDIA, *English, DoubleClick*, URL *en.wikipedia.org/wiki/Doubleclick*. Tuttora DoubleClick prevede la sola possibilità per l'utente di fare *opt-out*, cfr. URL *www.doubleclick.-com/privacy/opting_out.aspx*. Va ricordato che ciò costituisce in termini di diritto nazionale e comunitario vigente una violazione della normativa sulla protezione dei dati personali. Va altresì ricordato che la DoubleClick ha fatto uso di *web bug* per tracciare gli utenti, ossia di uno

tracciamento. La società è stata peraltro oggetto di alcuni procedimenti giudiziari ([36]).

6.3. *Il* cookie *permanente di Google e i* server log.

Passando ai ben più pericolosi *cookie* installati dai motori di ricerca, il caso paradigmatico qui è rappresentato dal *cookie* di Google. Per chiarire meglio il contesto, si presenta un esempio di *server log* creato in seguito alle ricerche effettuate dagli utenti, nel caso di specie in occasione della ricerca della parola "cars", ossia "automobili". Ecco come si presenta il *log*:

"*123.45.67.89 – 25/Mar/2003 10:15:32 – http://www.google.com/search?q=cars – Firefox 1.0.7; Windows NT 5.1 – 740674ce2123e969*" ([37]).

La spiegazione, offerta direttamente da Google, è la seguente:

"* 123.45.67.89 è l'indirizzo del Protocollo Internet assegnato all'utente dal suo ISP (...) (ossia l'IP, *n.d.a.*);

* 25/Mar/2003 10:15:32 sono la data e l'ora della richiesta;

* http://www.google.com/search?q=cars è l'URL richiesto, compreso l'oggetto della ricerca (si noti la parola *cars*, *n.d.a.*);

* Firefox 1.0.7; Windows NT 5.1 sono il *browser* ed il sistema operativo usati; e

* 740674ce2123a969 è il *cookie* ID particolare che viene assegnato ad un computer la prima volta che questo visita Google (la sequenza alfanumerica è l'identificativo dell'utente, *n.d.a.*) ([38])".

Si noti che le parole chiave cercate, in questo caso "cars", possono poi essere collegate alle pagine effettivamente visitate dall'utente, ossia ai collegamenti realmente "cliccati" dall'utente, tra quelli che vengono proposti dal

---

strumento considerato potenzialmente lesivo della privacy dalla direttiva 2002/58/CE, cfr. EPIC, *Complaint*, cit., p. 4.

([36]) Il caso DoubleClick è stato oggetto d'esame da parte dalla Federal Trade Commission dal febbraio 2002 al gennaio dell'anno successivo senza che venissero tuttavia riscontrate a carico della società violazioni. Occorre comunque notare che le accuse riguardavano profilo diverso, ossia l'incrocio di dati *offline* della società Abacus Direct con quelli *online* della Doubleclick. È stata anche presentata una *class action* per profilazione ad uso di pubblicità commerciale degli utenti *online* innanzi alla Corte Distrettuale. Infine è in corso l'azione promossa da Epic, di cui si è già detto.

([37]) L'esempio di *log* e la successiva spiegazione per punti, riportata tra virgolette, sono tratti dall'informativa di Google, URL *www.google.it/intl/it/privacy_faq.html#personalinfo*.

([38]) Ovviamente viene identificato un elaboratore, non direttamente un utente, nel senso che è possibile che tale elaboratore sia utilizzato da soggetti diversi. Benché ciò sia vero, altre indicazioni associate, come quelle temporali, aiutano a circoscrivere l'identificazione.

motore di ricerca. Si osservi ancora che tali parole possono riguardare anche informazioni sensibili, come ad esempio termini medici associati a particolari patologie, o parole attinenti alla sfera sessuale o connesse con orientamenti politici. Il riferimento univoco costituito dal *cookie* (nell'esempio 740674ce2123a969) è il principale collante che permette di collegare ad un centro unitario tutte le ricerche effettuate attraverso una determinata macchina, in definitiva di realizzare una vasta profilazione che si alimenta ad ogni successiva ricerca effettuata dall'utente. Come ha esattamente osservato una nota testata inglese commentando lo scandalo AOL, di cui si dirà tra breve: "Domandiamo a Google cose che esiteremmo a domandare a qualsiasi persona vivente. Il prezzo per le risposte è che Google ricorda tutto" ([39]). Non c'è dubbio infatti che le ricerche quotidianamente effettuate dalla maggior parte degli utenti forniscano una quantità di dati sufficientemente cospicua e diversificata da consentire speculazioni sulla professione, sulle scelte, sui gusti, sulle tendenze, sul tenore di vita, sulle idee politiche, sulle amicizie dell'interessato. Si noti peraltro che non è rilevante che un dato sia veritiero affinché costituisca "dato personale", má è invece rilevante che sia collegabile ad una persona individuata o individuabile. Il dato non veritiero o, ancor peggio, parzialmente veritiero è sotto molti profili assai più lesivo del dato esatto. Non è un caso che il principio della esattezza del dato sia espressamente previsto all'art. 11, comma 1°, lett. a) del d. legisl. 196/2003. Evidentemente, i pericoli connessi con questo tipo di profilazione dipendono, anche, dalla "vita" del *cookie* di Google. Se cioè il *cookie* spirasse in breve tempo e fosse poi sostituito da un *cookie* diverso si otterrebbe l'effetto di frammentare in maniera corrispondente la profilazione (almeno quella effettuata attraverso i *cookie*). Fino alla metà del 2007 il *cookie* di Google era sostanzialmente "eterno", essendo stato programmato con la data più lunga tra quelle consentite dai sistemi informatici. La valutazione espressa in proposito dal Gruppo *ex* art. 29 è stata assai netta: "A proposito del '*cookie di Google*', la sua durata, che è approssimativamente di 30 anni ([40]), è sproporzionata rispetto alle finalità di trattamento svolte e

([39]) Traduzione da STAFF GUARDIAN, *They know all about you*, in *Guardian Unlimited* edizione *online*, 28 agosto 2006, URL *www.guardian.co.uk/g2/story/0,,1859629,00.html.*

([40]) In seguito alle già ricordate pressioni della Comunità Europea, Google ha accettato come si è detto di limitare questa durata a due anni e poi a 18 mesi. Tuttavia, viene fatto osservare che "la durata limitata dei *cookie* non è che una scadenza fittizia: i file che riconoscono gli utenti e ne ricordano le preferenze si dissolvono dopo due anni di mancato accesso alla pagina che li distribuisce, accesso che ne rinnova la scadenza facendo ripartire il *countdown* biennale" (cfr. BOTTÀ, *I biscotti scaduti di Google non piacciono*, in *Punto informatico*, 23 luglio 2007, URL *punto-informatico.it/p.aspx?i=2043594*).

va oltre ciò che sembra 'strettamente necessario' per la fornitura del servizio, in base a quanto previsto dall'art. 5, comma 3° della direttiva 2002/58/CE sulla ePrivacy" ([41]).

È appena il caso di notare che il motore dispone comunque di altre informazioni dell'utente. Ad esempio, il *cookie* è associato a un indirizzo IP, che può consentire di collegare tra loro *cookie* identificativi diversi associati alla stessa macchina ([42]). Nel caso di IP dinamico questa eventualità appare comunque ridotta.

Occorre dire che la pratica di Google non è affatto isolata nel contesto dei motori di ricerca, e rileva semmai per il peso specifico che la società statunitense occupa nel settore. Yahoo! è perfino più esplicita: "Nel corso del processo di registrazione, Yahoo! ti chiede di inserire alcuni dati personali, quali il nome, l'indirizzo e-mail, la data di nascita, il sesso, il CAP, l'occupazione, il settore di attività ed eventualmente i tuoi interessi personali. Una volta registrato su Yahoo! ed utilizzando i nostri servizi, *non sarai quindi più un utente anonimo per noi*. Tieni conto, comunque, che la maggior parte di quanto offerto da Yahoo!, in particolare la nostra guida alla Rete, è liberamente utilizzabile dai nostri utenti in forma completamente anonima. Yahoo! riceve e registra in automatico sui propri *server* alcune informazioni provenienti dal *browser* utilizzato dall'utente, compreso l'indirizzo IP, le informazioni relative ai *cookies* Yahoo! e le *pagine richieste dall'utente*" ([43]) (corsivi aggiunti, *n.d.a.*). Qui la situazione, per esplicita ammissione del titolare, è perfino più allarmante. Infatti il *cookie* identificativo e la storia della navigazione dell'utente sembrerebbero associati anche ai dati rilasciati in occasione della sottoscrizione del servizio.

In tutti questi casi relativi a motori di ricerca viene in definitiva a configurarsi nei fatti un doppio regime nella gestione dell'anonimato: un grado zero di anonimato nei confronti del soggetto privato in posizione di controllo e un'aspettativa di anonimato più o meno consistente nei rapporti con gli altri soggetti terzi.

([41]) Gruppo *ex* art. 29, lettera 16 maggio 2007, URL cit., p. 2.

([42]) Non è un caso che la società dichiari nel proprio stringato comunicato del marzo 2007 che per rendere anonimi i propri *log* non è sufficiente anonimizzare i *cookie* ma occorre anche intervenire sul numero IP. Cfr. Google, *Google Log Retention Policy FAQ, cit.*: "*Che cosa vuol dire rendere i* log *anonimi*. Cambieremo alcuni *bit* nell'indirizzo IP che si trova nei *log* e cambieremo le informazioni del *cookie*. Stiamo ancora sviluppando l'esatto metodo scientifico e l'approccio da seguire, ma riteniamo che queste modifiche comporteranno un'aggiunta significativa alla protezione della privacy degli utenti" (traduzione non ufficiale, *n.d.a.*).

([43]) Cfr. Yahoo!, informativa, URL *info.yahoo.com/privacy/it/yahoo*.

Come risulta dall'informativa di Yahoo! ([44]), i *cookie* Yahoo! vengono utilizzati sostanzialmente per le stesse finalità di quelli di Google, ossia, in via principale, a scopo di profilazione commerciale dell'utente.

6.4. *Contromisure in difesa della privacy.*

Sul versante delle contromisure, va chiarito che i *cookie* possono venire cancellati dal proprio sistema e si può preventivamente configurare il proprio *browser* in maniera tale da rifiutare questi ultimi. Ciò non elimina interamente gli aspetti problematici. Quanto alla cancellazione dei *cookie* presenti sull'elaboratore, si tratta pur sempre di un'operazione successiva alla loro collocazione sull'*hard disk*, e peraltro di scarsa efficacia dal momento che i *cookie* rimossi sono rimpiazzati da altri *cookie* non appena si torna a collegarsi con i siti che li avevano collocati. Quanto alla possibilità di rifiutare preventivamente i *cookie*, si tratta di una modalità che non tutti i *browser* hanno nessariamente tra le opzioni preimpostate, con la conseguenza che in questi casi dovrà essere l'utente a farsi parte attiva. Inoltre, la funzionalità di alcuni siti può risultare compromessa se non si accettano i *cookie*. Si rimanda per considerazioni più estese al paragrafo che segue.

6.5. *I* web beacon.

In conclusione, pare necessario segnalare, sia pure stringatamente, un altro strumento di tracciamento, che risulta essere utilizzato da Yahoo!. Si tratta dei *web beacon*, noti anche come *web bug* ([45]). Può solo ricordarsi in proposito che questo genere di strumenti va considerato con particolare sospetto, e che la direttiva 2002/58/CE, considerando n. 24 si esprime a questo proposito in termini assai netti: "I cosiddetti software spia, bachi invisibili ('web bugs'), identificatori occulti ed altri dispositivi analoghi possono introdursi nel terminale dell'utente a sua insaputa al fine di avere accesso ad informazioni, archi-

---

([44]) Cfr. informativa Yahoo!, voce "cookie", URL *info.yahoo.com/privacy/it/yahoo/cookies*.

([45]) Cfr. *info.yahoo.com/privacy/it/yahoo*, "Yahoo! riceve e registra in automatico sui propri *server* alcune informazioni provenienti dal *browser* utilizzato dall'utente, compreso l'indirizzo IP, le informazioni relative ai *cookies* Yahoo! e le pagine richieste dall'utente. Yahoo! utilizza anche altri sistemi automatici di raccolta di informazioni come, per esempio, i cosiddetti *web beacons* ed i *cookies*".

viare informazioni occulte o seguire le attività dell'utente e possono costituire una grave intrusione nella vita privata di tale utente. L'uso di tali dispositivi dovrebbe essere consentito unicamente per scopi legittimi e l'utente interessato dovrebbe esserne a conoscenza". L'informativa Yahoo! in effetti menziona chiaramente questi strumenti, dunque non si può negare che l'interessato ne sia a conoscenza. Circa la qualificazione degli scopi, sembra esservi comunque un disallineamento tra quelli propri dei servizi offerti e quelli che giustificherebbero l'utilizzo dei *web bug*.

7. Lo scandalo AOL.

I pericoli di identificazione connessi alle profilazioni si sono rivelati tutt'altro che teorici il 4 agosto 2006, quando AOL, attualmente quarto motore di ricerca e acquirente di Google per alcuni servizi, ha reso pubblici per qualche ora dati relativi a ricerche effettuate da 650.000 utenti nell'arco di tre mesi, ritenendo erroneamente che l'utilizzo di codici alfanumerici anziché di nomi potesse valere a garantire la privacy degli interessati ([46]). Il *database* di AOL si è in realtà rivelato una miniera infinita di storie personali, di brandelli di vita. L'unico modo per dare conto della reale portata di queste informazioni è riportarne un estratto pubblicato da una celebre testata giornalistica inglese.

"Nel marzo di quest'anno un uomo con la passione per il calcio portoghese, residente in una città della Florida, stava bevendo pesantemente perché sua moglie lo tradiva. Ha digitato i suoi problemi nella finestra di ricerca del suo computer. 'Mia moglie non mi ama più' ha detto al computer. Ha cercato: 'fermare il divorzio' e 'voglio vendicarmi contro mia moglie', prima di dedicarsi ad un auto-esame con le ricerche: 'uscire dall'alcool', 'sintomi da disintossicazione da alcool' (alle 10 del mattino) e 'problemi d'erezione'. Il primo aprile era in cerca di un *medium* locale che potesse 'predire il mio futuro'. (...) Il 4 aprile (...), l'utente numero 14162375, il malinconico luso-americano in Florida, sembra essere crollato sulla tastiera alle 18:20, quando ha inserito all'improvviso le sequenze 'llllfkkgjnnvjjfokrb' e poi 'vvvvbmkmjk' e 'vvglhkitopppfoppr'. Un'ora più tardi si era sufficientemente ripreso per cercare alcune varianti del nome della moglie, pensava che si fosse spostata nel New England. La sera del 16 aprile, la situazione è esplosa. 'Mia moglie mi tradisce'; e poi, cinque volte, 'voglio uccidermi', e poi 'voglio far soffrire mia moglie', seguito immediatamente da 'kill my wifes mistress', 'my wifes ass', 'a cheating

([46]) Cfr. Staff Guardian, *ult. op. cit.*; Wikipedia, *English, AOL search data scandal.*

wife'. Due giorni dopo cercava cimici e dispositivi per la registrazione di suoni e quattro settimane più tardi sembrava essersi rimesso e cercava un'assicurazione per la moto ([47])" ([48]).

Già questa piccola porzione di dati sembra sufficiente a rendere identificabile l'utente in questione, e non soltanto per la sua cerchia di stretti conoscenti. Basti osservare che sono stati introdotti dati significativi, come varianti del nome della moglie e indicazioni geografiche (corroborati da alcuni errori grammaticali nel testo inglese, che potrebbero essere indicativi della provenienza non americana o, forse, di un basso livello scolare). Come è stato assai correttamente notato: "Queste storie, con tutte le informazioni rivelatrici che contengono ([49]), non possono sempre essere collegate con facilità ad un soggetto individuato, ma in alcuni casi ciò è possibile. Il *social security number*, assegnato a ciascun cittadino americano, è composto secondo uno schema facile da ricercare tra i dati pubblicati da AOL. Lo stesso deve dirsi dei numeri telefonici. In Internet si può comprare di tutto in qualsiasi parte del mondo, ma ci sono alcune cose, come ad esempio i servizi per gli animali da compagnia, che la gente preferisce scegliere vicino a casa, per cui risulta facile dedurre dove vive. Le persone poi spesso cercano i loro stessi nomi, che possono essere incrociati con i dati della rubrica telefonica" ([50]).

In effetti è stato facile per il New York Times, soggetto terzo, ricostruire l'identità di uno degli interessati, e vari *blogger* si sono sperimentati in questo genere di ricerche ([51]). Si tenga presente, per meglio inquadrare il caso, che i dati resi pubblici riguardano una porzione minima del *database* di AOL e che si riferiscono ad un arco temporale assai limitato. Si tenga anche presente da ultimo che il motore di ricerca può assai facilmente conoscere, e di regola in-

---

([47]) Altro caso di diffusione massiccia di dati personali, sia pure di natura completamente diversa si è registrato peraltro nel 2003 quando un gruppo di centinaia di migliaia di messaggi email interni della società Enron vennero pubblicati sul sito della Federal Energy Regulatory Commission, in occasione dell'indagine condotta dall'Agenzia sulla società in questione. Nonostante qualcuna delle email contenesse materiale utile all'indagine, la maggior parte conteneva informazioni di altro genere. Cfr. HAFNER, *Researchers Yearn to Use AOL Logs, but They Hesitate*, 23 agosto 2006, in *NYTimes.com*, URL *www.nytimes.com/2006/08/23/technology/23search.html?ei=5090&en=cc87040aed34a2d0&ex=1313985600&partner=rssuserland&emc=rss&pagewanted=print.*

([48]) Traduzione da STAFF GUARDIAN, *ult. op. cit.*

([49]) Deve incidentalmente notarsi che i dati di AOL hanno un notevolissimo valore come materiale scientifico. Cfr. in proposito, HAFNER, *ult. op. cit.*

([50]) Traduzione da STAFF GUARDIAN, *ult. op. cit.*

([51]) Cfr. BARBARO - ZELLER - HANSELL, *A Face Is Exposed for AOL Searcher No. 4417749*, in *NYTimes.com*, 9 agosto 2006, URL *query.nytimes.com/gst/fullpage.html?res=9E0CE3DD1F3FF93AA3575BC0A9609C8B63&sec=&spon=&pagewanted=all.*

fatti registra, la localizzazione territoriale dell'utente, con ciò aumentando significativamente le possibilità di identificazione ([52]).

8. Profili di violazione della normativa sulla protezione dei dati personali.

Occorre evidenziare che i *cookie* di soggetti terzi e i *cookie* rilasciati dai motori di ricerca paiono porsi in violazione di diverse norme in materia di protezione dei dati personali. Innanzitutto, va chiarito che, se si adotta il modello dell'anonimato ragionevole fatto proprio dal legislatore in questo ambito, sembra fuori di dubbio l'applicabilità della normativa sulla protezione dei dati personali, essendo assai improbabile qualificare come anonimi i dati degli utenti associati al *cookie*. Del resto costituisce sicuramente dato personale il numero IP. In generale, i contenuti dei *server log* dei motori di ricerca si collocano facilmente entro i termini del d. legisl. 196/2003 e della direttiva 95/46/CE. Come è stato chiaramente evidenziato dal Gruppo *ex* art. 29: "Come noto i *server log* sono informazioni che possono essere collegate ad una persona fisica identificata o identificabile e possono, di conseguenza, essere considerati dati personali secondo la definizione di cui alla direttiva 95/46/CE. Per tale ragione la loro raccolta e conservazione deve rispettare le norme in materia di protezione dei dati personali" ([53]). Nella già citata *Risoluzione sulla protezione della privacy e i motori di ricerca* approvata in occasione della 28ª Conferenza internazionale delle Autorità Garanti, si evidenzia inoltre che "i fornitori di motori di ricerca hanno la capacità di tracciare dettagliati profili degli interessi degli utenti. Molti *log* di indirizzi IP, specialmente quando combinati con i relativi dati registrati presso i fornitori di accesso alla rete, permettono l'identificazione degli utenti. Posto che l'uso dei motori di ricerca è oggi pratica comune tra gli utenti di Internet, i dati di traffico registrati dai fornitori dei maggiori motori di ricerca consentono una dettagliata profilazione di interessi, pensieri e attività in diversi ambiti (ad esempio lavoro, tempo libero, ma anche in particolare dati sensibili relativi, ad esempio, alle opinioni politiche, alle credenze religiose, o perfino alle preferenze sessuali)" ([54]). In defini-

---

([52]) Chiunque può fare un semplice esperimento collegandosi a qualcuno di quei siti che indicano a scopo dimostrativo i dati dell'utente connesso, comprensivi di IP, data e ora, sistema operativo, Stato e città. Ci si colleghi per esempio all'URL *www.ipaddresslocation.org*.

([53]) Traduzione non ufficiale. Il testo della lettera è disponibile al già segnalato URL *ec.europa.eu/justice_home/fsj/privacy/news/docs/pr_google_16_05_07_en.pdf*.

([54]) Cfr. *Risoluzione cit.*, p. 1.

tiva, profilare non è la stessa cosa che identificare, dal momento che si può ben creare un profilo individuale senza giungere all'identificazione di un soggetto. È tuttavia intuitivo che quanto più ricco è l'insieme di informazioni che si raccolgono tanto più circoscritto è il cerchio di ipotesi all'interno delle quali condurre l'indagine identificativa. Esempi fattuali sono offerti per l'appunto dai casi esaminati in precedenza relativamente alle stringhe di ricerca pubblicate da AOL.

Posto che deve quindi essere ritenuta applicabile la normativa sulla protezione dei dati personali, una prima violazione si riscontra nel fatto che l'utente non è di regola chiamato a esprimere alcun consenso né gli viene fornita un'informativa che chiarisca quantomeno le finalità e le modalità del trattamento realizzato attraverso il *cookie* e l'ambito di comunicazione dei dati. Trattandosi di informazioni criptate, l'utente non ha neppure accesso alle informazioni contenute nel *cookie* e registrate sul suo stesso elaboratore. Non viene effettuata peraltro, per quanto è dato sapere, alcuna notificazione al Garante per la protezione dei dati personali, pure in presenza delle condizioni di cui all'art. 37, comma 1°, lett. a) e d) d. legisl. 196/2003. Più in generale, è difficile non ravvisare in questa sistematica registrazione dei minimi segmenti che compongono la navigazione dell'utente in rete una lesione del principio di necessità di cui all'art. 3 d. legisl. 196/2003. Sembrano infine essere violati quantomeno anche il principio di proporzionalità e il principio della conservazione per un periodo limitato, introdotti rispettivamente all'art. 11, comma 1°, lett. d) e lett. e) del decreto.

9. Combinazione di servizi diversi forniti dallo stesso gestore.

Il quadro finora tracciato non è sufficiente ad evidenziare tutti i rischi che minacciano la protezione dell'anonimato degli utenti in rete. Occorre infatti tenere conto del fatto che i principali motori di ricerca gestiscono anche servizi di email. Come è stato evidenziato da un'autorevole testata *online*, Cnet: "Se la storia delle ricerche effettuate, le email e le informazioni conferite al momento della registrazione venissero combinate, un soggetto potrebbe conoscere dettagli intimi relativi alla salute, alla vita sessuale, alla religione, alle condizioni economiche e alle preferenze di spesa" ([55]). Google peraltro non si limita a gestire un potente motore di ricerca e un affermato servizio di posta

([55]) Mills, *Google balances privacy, reach*, in *Cnet News.com*, 14 luglio 2005, URL *www.news.com/Google-balances-privacy,-reach/2100-1032_3-5787483.html.*

(Gmail), ma fornisce anche un'ampia serie di servizi ulteriori e assai diversificati, che vanno dalle ricerche geografiche di GoogleEarth e GoogleMaps, ad un pacchetto di software *online* per l'ufficio, al servizio Adsense, alla barra di ricerca da installare sul *browser*, la Google *toolbar* ([56]), al programma di ricerca per scansionare e indicizzare il contenuto dell'intera memoria dell'elaboratore, denominato Google *desktop* ([57]). "Se ci si registra per avere il servizio di pubblicità di Google sul proprio sito *web*, la società viene a conoscenza di informazioni sul conto bancario e sull'indirizzo di abitazione, come del resto di ogni ricerca effettuata. Se si ha un *blog* sul servizio gratuito messo a disposizione da Google, Google ne è proprietaria. La società cononosce anche, naturalmente, i percorsi cercati sulle mappe di Google" ([58]).

Tutto ciò moltiplica esponenzialmente i pericoli già inviduati. Si tenga presente che nell'anno in corso (2007): "(i)l gruppo di tutela dei diritti Privacy International ha valutato il gigante della ricerca come 'ostile' alla privacy in un rapporto che classificava le aziende che operano sul *web* in base al modo in cui gestiscono i dati personali. Il gruppo ha sostenuto che Google sia il capofila di una 'corsa verso il basso' tra quelle società *web* che hanno in gran parte *policy* ben poco garantiste dei diritti degli utenti. Google si è classificata all'ultimo posto quanto a rispetto della privacy" ([59]).

10. Combinazione di dati provenienti da *database* di soggetti diversi.

Si è già notato che una sostanziale misura per assicurare un adeguato livello di protezione dei dati personali è quella di mantenere *database* separati ([60]). Possono darsi numerosi esempi di *database* contenenti informazioni

---

([56]) Secondo il gruppo Google-Watch la Google *toolbar* è uno *spyware*, cfr. URL *www.google-watch.org/bigbro.html*.

([57]) Deve segnalarsi che Google *desktop* non consentirebbe l'estrazione da parte di Google di informazioni contenute nel computer dell'utente, cfr. Mills, *op. cit.*: "Correzione: la prima versione di questo articolo suggeriva in maniera non corretta che Google Desktop Search potesse tracciare il contenuto del computer dell'utente. Tale servizio non rivela invece i dati registrati dall'utente a Google o a terzi, senza il consenso esplicito dell'utente medesimo".

([58]) Staff Guardian, *ult. op. cit.*

([59]) Staff BBC, *Google ranked 'worst' on privacy*, in *BBC News*, *International version*, 11 giugno 2007, URL *news.bbc.co.uk/2/hi/technology/6740075.stm*.

([60]) Sia pure su oggetto soltanto limitrofo, cfr. sulla gestione dei collegamenti tra *database* le osservazioni espresse da Garante prot. dati pers., parere, 16 marzo 2007, in *Boll.*, 2007, n. 81, doc. web n. 1397123.

personali di notevole rilevanza, in alcuni casi persino dati sensibili, ma gestiti da titolari che non sono grado, non possono giuridicamente oppure non hanno interesse ad incrociare le proprie informazioni con quelle di altri titolari. A mero titolo esemplificativo, e per porre immediatamente la materia su un piano concreto, si pensi agli archivi informatici delle biblioteche, che indicano i libri presi in prestito, e che perciò contengono dati anagrafici, recapiti e informazioni utili a profilare e perfino dati potenzialmente sensibili ([61]); ai *database* delle segreterie universitarie, contenenti dati anagrafici, elenchi di esami superati, informazioni reddituali, e molto altro ancora; allo sterminato *database* degli abbonati tenuto dalla Rai Radiotelevisione Italiana, con dati anagrafici e recapiti replicati dagli archivi dell'anagrafe; agli archivi elettronici dell'anagrafe; del catasto; al registro dei carichi pendenti; al registro delle imprese; ai *database* delle aziende sanitarie collegati per estrarre i fascicoli sanitari elettronici; agli archivi di società di trasporto ferroviario, aereo, marittimo ([62]); ai *database* tenuti da soggetti privati come le raccolte di curriculum *online*, risorsa questa di inestimabile valore. Che cosa accadrebbe per esempio se fosse possibile incrociare dati come quelli trattati dal sito italiano MioJob ([63]) con le informazioni di Google? L'ipotesi della fusione di *database* appartenenti a titolari diversi non è peregrina, se si considera l'annunciata acquisizione di DoubleClick da parte di Google, e se si tiene conto di altri episodi analoghi verificatisi nel passato.

11. Fusioni e acquisizioni aziendali: i pericoli per la privacy.

È dei primi mesi del 2007 la notizia che Google ha espresso la sua intenzione di acquistare la società DoubleClick. I rischi in termini di profilazione dell'utente sono evidenti: da un lato il motore di ricerca registra le parole immesse e i *link* scelti dall'utente, dall'altro DoubleClick è in grado di tracciare la navigazione che avviene al di fuori del motore di ricerca, almeno per quanto

---

([61]) Sull'utilità del patrimonio informativo contenuto negli archivi delle biblioteche, cfr. ACLU, *Surveillance Under the Usa Patriot Act*, 3 aprile 2003, URL *www.aclu.org/safefree/general/17326res20030403.html*; cfr. Staff NYTimes, *Revising the Patriot Act*, in *NYTimes.com*, 10 aprile 2005, URL *www.nytimes.com/2005/04/10/opinion/10sun1.html?_r=1&pagewanted=all&position=&oref=slogin*.

([62]) Si tenga peraltro conto che di regola questi soggetti inviano email di conferma per i servizi acquistati, rendendo di conseguenza accessibile la ricostruzione dei viaggi ai gestori di email.

([63]) URL *http://miojob.repubblica.it*.

riguarda i siti associati al suo programma. È stato notato che se l'operazione dovesse avere esito favorevole, grandi quantità di informazioni sui navigatori del *web* correrebbero il rischio di essere combinate. L'Electronic Privacy Information Center ha protestato per mesi contro la proposta di acquisizione sollevando profili relativi alla privacy, e ha recentemente promosso una petizione nei confronti della Federal Trade Commission per bloccare l'operazione (64). In linea generale, è difficile ignorare che uno degli *asset* che passano di mano in occasione di fusioni e acquisizioni è costituito proprio da cospicui patrimoni informativi. Occorre ricordare che già in passato DoubleClick si era fusa con la società Abacus Direct, alimentando timori che la combinazione dei dati delle due società potesse collegare i profili degli utenti *online* della prima alle informazioni anagrafiche gestite dalla seconda. In seguito alle polemiche sollevate dal progetto, DoubleClick rinunciò ad integrare i propri servizi con quelli di Abacus Direct (65).

12. I PERICOLI DELLA COLLABORAZIONE TRA MULTINAZIONALI E GOVERNI.

Il 18 gennaio 2006 il Dipartimento di Giustizia degli Stati Uniti ha richiesto attraverso un *subpoena* ai quattro principali motori di ricerca, ossia Google, Yahoo!, Microsoft, AOL di fornire dati relativi alle ricerche *online* degli utenti (66). Ciò allo scopo di reprimere con maggiore efficacia la pedopornografia *online*. La richiesta è stata rifiutata soltanto da Google (67), che ha impugnato il *subpoena* (68). Nel momento in cui si scrive la controversia non risulta ancora definita (69). La circostanza che nel caso di specie Google abbia

(64) Traduzione da UTTER, *EU: Google, DoubleClick Privacy? No Worries*, 15 ottobre 2007, in *Webpronews.com*, URL *www.webpronews.com/topnews/2007/10/15/eu-google-doubleclick-privacy-no-worries*.

(65) Cfr. EPIC, *Complaint cit.*; cfr. anche WIKIPEDIA, *English, DoubleClick, cit.*

(66) La richiesta riguardava inizialmente tutte le *query* di ricerca inserite nei motori di ricerca tra il 1° giugno e il 31 luglio 2005.

(67) Cfr. MOHAMMED, *op. cit.*; HAFNER - RICHTEL, *Google Resists U.S. Subpoena of Search Data*, in *NYTimes.com*, 20 gennaio 2006, URL *www.nytimes.com/2006/01/20/technology/20google.html*; MCCULLAGH, *FAQ: What does the Google subpoena mean?*, in *Cnet News*, 20 gennaio 2006, URL *www.news.com/FAQ-What-does-the-Google-subpoena-mean/2100-1029_3-6029042.html*.

(68) ID., *Court date set for Google lawsuit*, in *Cnet News*, 26 gennaio 2006, URL *www.news.com/Court-date-set-for-Google-lawsuit/2100-1030_3-6031941.html*. Si può trovare copia dell'atto di impugnazione del *subpoena* all'URL *googleblog.blogspot.com/pdf/Google_Oppo_to_-Motion.pdf*.

(69) Le notizie più recenti si apprendono direttamente da un *post* pubblicato il 17 febbraio

scelto di resistere alla richiesta avanzata dal governo statunitense può da un lato apparire tranquillizzante, ma dall'altro indica inequivocabilmente che la definizione di questioni della massima rilevanza in termini di tutela delle libertà personali si trova allo stato rimessa, in casi come questi, alle imponderabili scelte di un soggetto privato. Come ha esattamente osservato Marc Rotenberg: "Google è sempre stata una sorta di bomba ad orologeria perché Google conserva informazioni relative a soggetti identificabili. (...) Anche nel caso in cui Google abbia intenzione di proteggere la privacy relativa alla navigazione *on-line*, potranno sempre verificarsi circostanze tali da porre gli utenti di Internet a rischio, e tali circostanze includono ordini del Governo come nel caso di specie, ma anche problemi di sicurezza analoghi a quelli che hanno segnato il settore dei servizi finanziari negli ultimi due anni" ([70]). A conferma di queste considerazioni, pare rimarchevole notare che nella vicenda in esame gli altri tre motori di ricerca non hanno opposto significative resistenze all'azione governativa.

Ancora più eclatante, a proposito di cedimenti alle richieste governative, la linea compiacente adottata da Yahoo! dinanzi alle pressioni del governo cinese. Vale la pena ricordare un episodio recente, per il suo intenso significato giuridico e perché si inscrive assai puntualmente nel quadro che si sta tratteggiando. Nel 2005 la società statunitense accondiscese a trasmettere alle autorità del regime asiatico alcune informazioni attraverso le quali fu possibile identificare il giornalista cinese Shi Tao, collaboratore della testata *Contemporary Trade News* di Hunan. Shi Tao venne condannato a 10 anni di reclusione per un'imputazione risibile, quella cioè di aver inviato a un gruppo di difesa della privacy con sede a New York, attraverso il servizio email di Yahoo!, commenti effettuati in una riunione dello staff del suo giornale ([71]), ciò che lo rendeva colpevole di trasmissione all'estero di segreti di Stato ([72]). Ha osser-

---

2006 sul *blog* ufficiale di Google da Nicole Wong, *associate general counsel* dell'azienda, URL *googleblog.blogspot.com/2006/02/response-to-doj-motion.html*.

([70]) Traduzione da MOHAMMED, *Google Refuses Demand for Search Information*, in *Washingtonpost.com*, 20 gennaio 2006, URL *www.washingtonpost.com/wp-dyn/content/article/2006/01/19/AR2006011903331.html*.

([71]) Cfr. tra i molti STAFF BBC, *Yahoo 'helped jail China writer'*, in *BBC News 24*, 7 settembre 2005, URL *news.bbc.co.uk/1/hi/world/asia-pacific/4221538.stm*.

([72]) Google non si è segnalata per indipendenza nei confronti del regime cinese, avendo acconsentito a filtrare le ricerche effettuate attraverso il proprio motore da computer con IP cinese. In particolare è negato l'accesso a siti *web* che contengono elementi di critica e parole come "Taiwan", "indipendenza", "Tibet" o "Tienanmen". Cfr. Parlamento Europeo, *Risoluzione del Parlamento europeo sulle relazioni UE-Cina*, 2005/2161(INI), considerando AC, URL *www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+20060907+ITEM-S+DOC+XML+V0//IT*.

vato esattamente, in altro contesto, Vincenzo Ricciuto a proposito dell'anonimato, che esso deve considerarsi "nella prospettiva di tutela di quelle situazioni dove si vogliono reclamare libertà fondamentali senza esporsi a forme repressive, anche a rischio di limitazione alla libertà personale (si pensi alla libertà di espressione e di dissenso politico in Paesi a regime politico totalitario, alle denunce di violazioni di diritti umani, ecc.)" ([73]).

In definitiva, la condizione di anonimato di cui gode l'utente in rete, anche quando sia formalmente assistito dalle più ampie garanzie giuridiche, assume sempre una valenza precaria, dal momento che le tracce delle relazioni intrattenute in rete sono archiviate, talvolta *sine die*, in repertori elettronici dai quali possono prima o poi essere estratte. Tale circostanza, la cui esistenza si deve in ultima analisi alla sostanziale inerzia o debolezza dei meccanismi giuridici di controllo e repressione nazionali o comunitari, deve essere valutata con la massima attenzione quando si considera l'anonimato *online*. Dinanzi al motore di ricerca o al gestore di posta, l'anonimato è sostanzialmente a coefficiente zero, mentre, nei rapporti intrattenuti con altri soggetti, questo tende a dispiegarsi nelle forme consuete.

13. Altre possibilità di identificazione su Internet attraverso la combinazione di informazioni.

A parte il caso delle macroscopiche violazioni realizzate da pochi centri di controllo privati, occorre brevemente considerare, in chiusura, quali siano le opportunità di *data mining* accessibili all'utente medio in rete, senza cioè bisogno di godere di una particolare posizione di controllo né di avere particolari conoscenze tecniche. Si tratta evidentemente di un'ipotesi marginale e di rilevanza modesta a questo punto dell'analisi, ma vale la pena farvi cenno almeno per completezza d'esame. In prima istanza deve certamente prendersi atto che le risorse informative presenti in rete sono ovviamente cospicue e consentono ricerche sufficientemente mirate. L'uso dei motori di ricerca facilita enormemente nell'assemblaggio di profili, anche da parte dell'utente medio. Si pensi soltanto alla possibilità di associare una foto ad un nome o di rintracciare dati potenzialmente sensibili come la partecipazione a petizioni *online* o a gruppi di discussione di carattere politico. Indagini più specifiche richiedono tuttavia una precisa conoscenza dei siti da analiz-

([73]) Ricciuto, *La tutela della persona di fronte alle reti telematiche*, in Nivarra–Ricciuto (a cura di), *op. cit.*, p. 14.

zare. Senza entrare nel dettaglio di un'elencazione, e facendo a puro titolo di esempio qualche considerazione sugli archivi statunitensi pubblicamente disponibili *online*, si può ricordare che entrando nel sito *www.census.gov* dell'ufficio per il censimento statunitense si possono visualizzare dati statistici per microaree relativi al reddito medio, al numero medio di componenti del nucleo familiare, e perfino dati sull'origine etnica dei cittadini statunitensi. In alcuni casi ciò rende possibile indovinare, con un discreto grado di approssimazione, il tenore di vita di un certo soggetto e supporre quale possa essere la sua provenienza familiare. Dal *database* Whois si possono estrarre i nomi dei soggetti che hanno registrato siti. Attraverso gli elenchi telefonici *online* si può associare un nome estratto dal Whois ad una abitazione. Per questa via, assemblando insieme le risorse menzionate, diventa insomma possibile risalire ad informazioni sul luogo di residenza, sul verosimile tenore di vita e perfino sulla probabile origine etnica di un soggetto che abbia registrato un sito *web*. Conferme sull'origine etnica della famiglia possono essere poi ricavate con un po' di fortuna dal *database* di *www.ellisisland.org*. Si potrebbe andare avanti, ma si vede che già così, semplicemente utilizzando servizi mirati accessibili a chiunque, possono condursi alcune semplici profilazioni.

Queste considerazioni permettono di pervenire a riflessioni più generali su alcune caratteristiche peculiari della rete, che non si danno normalmente nel mondo fisico. Internet in definitiva consente di superare sia i limiti soggettivi nell'accesso alle ricerche, sia i limiti di carattere oggettivo, nel senso che le informazioni possono essere raccolte senza necessità di spostamenti fisici da un luogo all'altro, sia infine i limiti temporali: in Internet possono reperirsi informazioni remote, e non sono mancati anzi casi in cui proprio per tali ragioni sono state contestate lesioni del diritto all'oblio. È interessante notare che in questo assetto di cose l'anonimato dell'utente si trova sempre esposto a possibili identificazioni *a posteriori*.

14. Conclusioni.

Va riconosciuto all'utente in Internet un generale diritto all'anonimato. Nonostante sia necessario tenere conto del bilanciamento con diritti prevalenti e nonostante si registrino nel nostro Paese alcuni peculiari limiti di carattere normativo, non sembra possa dirsi, sotto il profilo del rapporto tra cittadini e governo, che l'anonimato *online*, dal punto di vista normativo, incontri una compressione davvero significativa, almeno allo stato attuale, e senza tener conto delle ricorrenti proposte di sottoporre ad una stretta regolamentazione

alcuni aspetti della rete. Inoltre, la materia si trova comunque ricondotta entro le guide sicure dello stato di diritto e nell'alveo del dibattito giuridico.

Il vero, macroscopico, problema risiede altrove, ed è costituito da una situazione fattuale del tutto anomala e storicamente priva di paralleli nel mondo fisico: la concentrazione di potere in settori strategici della rete nelle mani di pochi soggetti privati. A tale profilo, che appare assolutamente decisivo quando ci si occupa di anonimato in rete, è stato di conseguenza dedicato ampio spazio nel presente capitolo. La situazione è riassunta con efficacia nell'avvertimento contenuto nell'informativa di Yahoo!: "Una volta registrato su Yahoo! ed utilizzando i nostri servizi, non sarai quindi più un utente anonimo per noi".

Quello dei motori di ricerca non costituisce peraltro l'unico settore strategico caratterizzato da una concentrazione di controllo privato sulle informazioni personali. In materia di comunicazioni elettroniche relative al trasferimento di denaro, va per esempio ricordato il notevole caso Swift, che rivela un preoccupante indebolimento delle garanzie dei cittadini europei, esposti a penetranti rischi di profilazione dei loro trasferimenti, senza contare l'aspetto ancora più vistoso, ma estraneo al nucleo di questa trattazione, relativo ai rischi di spionaggio industriale ai danni delle imprese comunitarie. Dinanzi a situazioni così anomale di controllo privato, le quali peraltro, come si è notato, confliggono con più di una norma a tutela della privacy, la reazione delle istituzioni nazionali e di quelle comunitarie stenta ad affermarsi, e le iniziative sono condotte soprattutto con gli strumenti della negoziazione piuttosto che con quelli della coercizione, come normalmente avverrebbe dinanzi a soggetti privati economicamente meno potenti. Se da un lato ciò può apparire tutto sommato nell'ordine delle cose, non si può non rilevare che sotto il profilo giuridico costituisce un allarmante segno di affievolimento della sovranità, tanto di quella statale quanto di quella attribuita mediante i trattati alle istituzioni comunitarie. Peraltro, in materia di protezione dei dati personali, si riscontra uno specifico fattore di debolezza dovuto alla frammentazione su base nazionale delle Autorità Garanti, e alla mancanza di un unico soggetto referente di livello comunitario (74) in grado di portare avanti una forte strategia comune, come avviene per esempio nel settore *antitrust*.

Uno degli aspetti più allarmanti, come si è evidenziato, è costituito dal fatto che i soggetti privati in grado di esercitare questo penetrante controllo sui dati personali si fanno sostanzialmente garanti di se stessi, con tutte le conseguenze che possono derivare da cattive scelte nella gestione dell'enorme po-

(74) Non è esattamente questa la funzione dell'European Data Protection Supervisor.

tenziale informativo di cui dispongono (scandalo AOL) o da accordi commerciali con altri soggetti (DoubleClick-Abacus, Google-DoubleClick) o da cedimenti nei confronti di governi nazionali (Yahoo! e Google ([75]) nei confronti della dittatura cinese; Yahoo! nei confronti del Dipartimento di Giustizia del governo statunitense). In definitiva, manca del tutto un potere di controllo degli interessati sul trattamento riservato ai loro dati personali da questi potenti soggetti economici, al punto che agli utenti non è possibile conoscere neppure il contenuto delle informazioni registrate nei *cookie* che vengono rilasciati sui loro *hard disk*.

In ciò si rileva, al di là dei gravi episodi contingenti segnalati, una macroscopica stortura nell'assetto strutturale e nella gestione di alcuni servizi di Internet, che non può non costituire la premessa di preoccupanti eventi futuri. Veramente non si può non dissentire da Marc Rotenberg quando definisce i gestori di tali risorse strategiche delle bombe ad orologeria pronte ad esplodere. Ciò è tanto più significativo se si pensa che l'anonimato, quello che si è proposto di definire sinteticamente come "positivo", rappresenta una modalità o uno strumento essenziale per l'esercizio e l'affermazione di diritti fondamentali. Le conseguenze della repressione dell'anonimato positivo dovute ad una gestione del tutto personalistica e fuori controllo del patrimonio informativo illegittimamente registrato hanno peraltro già avuto una loro emblematica rivelazione nella vicenda del giornalista Shi Tao.

Da ultimo, e sotto un profilo decisamente residuale, devono considerarsi i restanti rapporti tra privati che non occupino sostanziali posizioni di controllo sui servizi della rete. In tali ipotesi, le possibilità che pure sono offerte di aggregare informazioni per ricostruire profili personali appaiono certamente ragguardevoli rispetto a quanto è normalmente sperimentabile nel mondo fisico, tuttavia, rapportate in scala alle dimensioni dei problemi più sopra rappresentati, si riducono a elementi di importanza secondaria.

([75]) Cfr. *infra* nota n. 72.