PRIVACY. EVOLUZIONI E CENNI SULLA NORMATIVA*

Dott. Gianluigi Fioriglio

SOMMARIO: 1. ORIGINE DEL DIRITTO ALLA PRIVACY 2. CENNI SULL'EVOLUZIONE DEL DIRITTO ALLA PRIVACY IN ITALIA 3. IL C.D. CODICE DELLA PRIVACY: ASPETTI GENERALI 4. IL GDPR: ASPETTI GENERALI 5.1. DATI PERSONALI E LORO TRATTAMENTO 5.2. TITOLARE, INTERESSATO E ALTRI SOGGETTI 5.3. CENNI SULL'AUTENTICAZIONE INFORMATICA 5.4. CENNI SU CASI CONCRETI

1. ORIGINE DEL DIRITTO ALLA PRIVACY

I cambiamenti politici, sociali ed economici avvenuti nell'Ottocento hanno profondamente inciso sulla vita dell'uomo, facendo segnare il passaggio da un'economia rurale ad una industrializzata, con un conseguente accrescimento dei nuclei urbani, che hanno oltretutto facilitato la diffusione di strumenti di comunicazione di massa, in primo luogo i giornali.

Proprio alcuni pettegolezzi sulla propria moglie, apparsi sul *Saturday Evening Gazette*, si dice abbiano spinto Samuel D. Warren a scrivere, insieme con Louis D. Brandeis, un breve saggio intitolato *The Right to Privacy*, pubblicato nel 1890 sulle pagine dell'*Harvard Law Review*[1]. Questo saggio costituisce la prima compiuta formulazione del diritto alla privacy quale *right to be let alone*.

Già in alcuni procedimenti giudiziari, come Prince Albert *v*. Strange[2], i giudici avevano affermato la violazione, nel caso di specie, del diritto alla *privacy*, dunque riconoscendolo e rendendo palese la sua importanza non solo dal punto di vista teorico, ma soprattutto pratico, come dimostra la ricostruzione di Warren e Brandeis, nelle cui parole emerge la funzione della riservatezza quale argine contro gli attacchi di un giornalismo finalizzato non ad informare ma piuttosto a scandalizzare.

I due autori riconoscono, dunque, l'esistenza di un generale diritto alla privacy, ben distinto dal diritto di proprietà e caratterizzato dalla sua esplicazione mediante entità sia materiali che immateriali. Questo diritto nasce in risposta ai cambiamenti politici, economici e sociali che costituiscono l'evoluzione della società e che recano con sé il bisogno di riconoscimento di nuove posizioni giuridiche soggettive, soddisfatte dall'opera creativa della *common law*, che si dimostra in alcuni casi pronta al recepimento delle istanze mosse in tal senso dalla società. In concreto, la tutela del diritto alla privacy si può ottenere, secondo i due giuristi, tramite un'azione di responsabilità civile, ossia un "*tort for damages*" che si può sempre esercitare, oppure, in casi limitati, tramite una *injuction*. La responsabilità civile sussisterebbe in qualunque caso di *"injury to feelings"*[3].

A detta degli autori, non ci si può esimere da responsabilità nel caso in cui si proceda alla pubblicazione di fatti o eventi caratterizzati da verità, poiché in tali ipotesi si verifica una lesione del *right to privacy*, che si trova su un differente piano logico, essendo ben distinto dal diritto all'identità personale. Parimenti, l'assenza di dolo e i motivi che hanno spinto a violare il diritto alla riservatezza non costituiscono una scusante se il fatto si è verificato, visto che una volta che questo è stato compiuto non si può più tornare alla situazione *quo ante*. A queste conclusioni spinge un esame dell'intera *law of torts*, ai sensi della quale ciascuno è responsabile degli atti che compie intenzionalmente, anche se questi sono commessi in buona fede.

---

* Parte della presente dispensa è stata estratta, con modificazioni e aggiornamenti, da G. Fioriglio, *Temi di informatica giuridica*, Aracne, Roma, 2004 (l'intero volume è liberamente scaricabile da www.dirittodellinformatica.it).

[1] S. D. Warren, L. D. Brandeis, *The right to privacy*, in Harvard Law Review, 1890, 4, p. 193, ora in *Landmarks of Law*, 1960, p. 261.

[2] Prince Albert *v*. Strange,1 McN & G. 25 (1849).

[3] S. D. Warren, L. D. Brandeis, *op. cit.*, p. 275.

Secondo Warren e Brandeis sarebbe necessario apprestare anche una tutela penale del diritto alla riservatezza, soprattutto nei casi di estrema gravità della lesione che si realizzano, ad esempio, quando una eventuale pubblicazione abbia ampia diffusione[4]. Ovviamente, in tali eventualità è necessario un espresso intervento legislativo, poiché non si può procedere alla creazione di nuovi reati in via interpretativa. La necessità di una così forte forma di tutela sarebbe giustificata dalla considerazione che, mediante una tutela individualizzata dei vari cittadini, si riuscirebbe ad ottenere la tutela della società nel suo complesso[5].

Le tesi dei due giuristi statunitensi stupiscono ancor oggi per la loro modernità, soprattutto se si considera l'enorme divario tecnologico che separa gli Stati Uniti del finire dell'Ottocento dall'odierna Società dell'informazione. Oggi, ai progressi in campo tecnico-scientifico e ai conseguenti benefici, si accompagna una pluralità di situazioni potenzialmente lesive della *privacy* di ciascuno di noi: basti pensare agli strumenti di acquisizione visiva e sonora, alla capillare diffusione dei *mass media*, all'avvento dell'informatica, alla diffusione di Internet e di strumenti tecnologici sempre più avanzati ma anche sempre più interconnessi.

Tutti questi nuovi strumenti riescono a fornire una enorme libertà all'uomo, ma allo stesso tempo possono renderlo un "uomo di vetro", sottoposto ad infiniti sguardi indiscreti altrui. In merito, il problema principale sussiste quando si verifica lo scontro fra diritti configgenti, in primo luogo fra la riservatezza e il diritto di cronaca e di manifestazione del pensiero. Queste circostanze fanno da più parti ritenere superato il concetto di *privacy* quale diritto dell'uomo ad essere lasciato solo, spostando l'attenzione sul diritto all'autodeterminazione informativa quale prerogativa di ciascun soggetto cui i dati personali fanno riferimento.

Ciò risponde a quelle tendenze evolutive ben individuate da Stefano Rodotà, che possono indicarsi nel "diritto di mantenere il controllo sulle proprie informazioni" e conseguentemente come il citato "diritto all'autodeterminazione informativa"; vi sono, inoltre, due ulteriori passaggi, "dalla privacy alla non discriminazione" e "dalla segretezza al controllo"[6].

Si verifica, pertanto, il passaggio da una connotazione sostanzialmente negativa (diritto a *essere lasciati soli*, a non subire illegittime ingerenze nell'ambito della propria sfera privata) a una sostanzialmente positiva (diritto di *controllare* le informazioni che riguardano la predetta sfera).

Si potrebbe comunque sostenere che la vecchia concezione di Warren e Brandeis, nell'affermare un diritto ad essere lasciato solo, implichi anche la possibilità di decidere dell'uso, o del non uso, di tutte quelle informazioni che riguardano solo ed esclusivamente quella certa persona. Nella società odierna, tuttavia, in cui l'informazione assume sempre più rilevanza, anche e soprattutto da un punto di vista economico, sancire un diritto all'autodeterminazione informativa permette di centralizzare il ruolo dell'uomo quale unico soggetto legittimato a decidere dell'uso di tutti i suoi dati personali.

La vera essenza del diritto alla privacy non sta comunque nella sua potenziale patrimonializzazione, ma piuttosto nel suo carattere di diritto fondamentale ed inviolabile dell'uomo, che consente l'esercizio di altri diritti che sono legati alla possibilità di evitare inopportuni giudizi altrui, con riferimento a scelte di per sé insindacabili, come quelle legate a dati sensibili ed inerenti alle scelte religiose e sessuali, alle concezioni filosofiche, ecc. La lesione della riservatezza, inoltre, si riverbera anche sulla sfera psichica del soggetto che vede violato un suo diritto di rango costituzionale, che dovrebbe cedere solo dinanzi a casi concreti di particolare gravità ed in seguito all'effettuazione di un'operazione di

[4] Ibid.
[5] Ibid.
[6] Sul punto vedi S. Rodotà, *Privacy e costruzione della sfera privata*, in Pol. dir., 1991, e ora in Tecnologie e diritti, 1995, p. 108, e Id., *Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali*, in Riv. crit. dir. priv., 1997, 4, p. 589.

bilanciamento fra diritti configgenti.

Ad ogni buon conto, è d'uopo sottolineare che la perdita di controllo sui propri dati personali non è necessariamente una conseguenza di una condotta illecita posta in essere da terze parti (almeno per quanto riguarda l'ipotesi della prima comunicazione o diffusione delle informazioni), ma ben può realizzarsi in virtù delle azioni, più o meno consapevoli, dell'interessato, come nei casi di prestazione del consenso per finalità promozionali o di marketing nonché di pubblica diffusione di propri dati personali.

Le conseguenze possono essere di varia tipologia e spaziano, a titolo esemplificativo e non esaustivo, dallo spam al furto di identità, dalla discriminazione al mancato accesso al credito, dal licenziamento alla profilazione, e così via. Indipendentemente dalla sua regolamentazione, la privacy può dunque essere protetta tenendo una condotta diligente, ad esempio negando il consenso al trattamento dei dati personali per finalità promozionali e di marketing, utilizzando email non identificative del nome e del cognome dell'utente nonché password sicure, e, ancora, installando programmi anti-virus e anti-malware eventualmente anche su dispositivi mobili.

2. CENNI SULL'EVOLUZIONE DEL DIRITTO ALLA PRIVACY IN ITALIA

Il diritto alla riservatezza ha inizialmente trovato riconoscimento e tutela nell'ordinamento italiano in via interpretativa, grazie all'apporto di dottrina e giurisprudenza, cui si sono contrapposti per lungo tempo pochi interventi legislativi, sporadici oltreché inadeguati, ispirati a logiche settoriali e non incentrati sulla protezione di un diritto umano fondamentale.

I primi contributi in materia risalgono agli anni trenta, periodo nel quale dobbiamo ricordare il contributo di Ravà[7], che individua, nel novero dei diritti della personalità, "un generale diritto alla riservatezza"; pochi anni più tardi anche De Cupis[8] si mostra favorevole al riconoscimento di questo diritto. Inizia dunque un dibattito che coinvolge alcuni fra i più importanti studiosi italiani di diritto, divisi fra chi ritiene che la legge italiana tutela il diritto alla riservatezza[9] e fra chi sostiene il contrario[10].

Le discussioni in materia trovano nuovo vigore negli anni cinquanta, quando l'autorità giudiziaria viene investita di due procedimenti promossi per tutelare la riservatezza di due personaggi celebri, Enrico Caruso[11] e Claretta Petacci[12].

Nel "caso Caruso", in primo grado si afferma l'esistenza nel nostro ordinamento di un diritto alla riservatezza, tutelabile mediante l'applicazione analogica della disciplina del diritto all'immagine[13]. Nel 1953, il Tribunale di Roma afferma che tale diritto consiste "nel divieto di qualsiasi ingerenza estranea nella sfera della vita privata della persona, e di qualsiasi indiscrezione da parte di terzi, su quei fatti o comportamenti personali che, non pubblici per loro natura, non sono destinati alla pubblicità delle persone che essi

[7] A. Ravà, *Istituzioni di diritto privato*, Padova 1938, p. 197.

[8] A. De Cupis, *I diritti della personalità*, in *Trattato di diritto civile Cicu – Messineo*, Milano 1942, I, p. 148.

[9] Fra gli altri, A. De Cupis (v. per tutte: *I diritti della personalità*, cit.) e G. Giampiccolo, *La tutela giuridica della persona umana e il cd diritto alla riservatezza*, in Riv. trim. dir. proc. civ., 1958, p. 458.

[10] Fra gli altri, G. Pugliese (v. per tutte: *Il diritto alla riservatezza nel quadro dei diritti della personalità*, in Riv. dir. civ., 1963, p. 605).

[11] Questa vicenda è stata originata dalla realizzazione del film *Leggenda di una voce*, che ricostruiva, in modo romanzato, la vita del celebre tenore Enrico Caruso; gli eredi di questi ritenevano alcune scene del film lesive della memoria, dell'onore e della riservatezza del defunto cantante e convenivano pertanto in giudizio la società produttrice del film.

[12] La lite era stata provocata dalla pubblicazione di un libro in cui l'autore ricostruiva la personalità di Claretta Petacci, con asserzioni e toni tali da violare, secondo la famiglia della Petacci, la sua *privacy* e quella dei suoi congiunti.

[13] Trib. Roma 14 settembre 1953, in Foro it., 1954, I, c. 115; invece App. Roma 17 maggio 1956, in Foro it., 1956, I, c. 796, non si pronuncia sul problema dell'esistenza o meno del diritto alla riservatezza.

riguardano"[14]. Il giudizio prosegue poi innanzi la Corte di Cassazione[15], la quale ribalta l'impostazione seguita dai giudici di merito, e, seguendo la tesi prospettata da Pugliese[16], afferma che "il semplice desiderio di riserbo non è stato ritenuto dal legislatore un interesse tutelabile"[17] e quindi che nell'ordinamento italiano non esiste "un generale diritto alla "riservatezza", o "privatezza""[18].

Questo orientamento non viene formalmente contraddetto dalla Suprema Corte sette anni più tardi[19], quando viene chiamata a pronunciarsi sul "caso Petacci"; come nel "caso Caruso", i giudici di merito[20] riconoscono l'esistenza del diritto alla riservatezza, ma stavolta viene invocata, come norma regolatrice del caso, l'art. 8 della Convenzione del Consiglio d'Europa per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, ratificata in Italia con la legge 4 agosto 1955, n. 848, ai sensi del quale "Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza". La Cassazione respinge questa tesi e nega ancora l'esistenza di un diritto alla riservatezza, purtuttavia "deve ammettersi la tutela nel caso di violazione del diritto assoluto di personalità inteso quale diritto *erga omnes* alla libertà di autodeterminazione nello svolgimento della personalità dell'uomo come singolo. Tale diritto è violato se si divulgano notizie della vita privata le quali, per tale loro natura, debbono ritenersi riservate"[21] e trovano tutela nell'art. 2 Cost., che ammette "un diritto di libera autodeterminazione nello svolgimento della personalità nei limiti di solidarietà" politica, economica e sociale.

Nonostante questi contrasti, il legislatore interviene solo nel 1970 emanando la legge 20 maggio 1970 n. 300, il c.d. Statuto dei lavoratori, che contiene alcune previsioni a tutela della privacy dei lavoratori e pertanto applicabili solo nell'ambito del rapporto di lavoro. Più specificatamente, ha disposto il divieto di:

a) utilizzare impianti audiovisivi e altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori (art. 4; tale norma è stata sostituita nel 2015 in attuazione della l. 183/2014, il c.d. Jobs Act, v. *infra*)[22];
b) effettuare accertamenti sulla idoneità e sulla infermità per malattia o infortunio del lavoratore dipendente (art. 5)[23];
c) effettuare visite di controllo sulla persona (salvo se indispensabili per la tutela del

[14] Così Trib. Roma, *sent. ult. cit.*
[15] Cass., 22 dicembre 1956, n. 4487, in Giust. Civ., 1957, I, p.5.
[16] Si veda G. Pugliese, *Il preteso diritto alla riservatezza e le indiscrezioni cinematografiche*, in Foro it., 1954, c. 116, nota a Trib. Roma 14 settembre 1953.
[17] Cass., *sent. ult. cit.*, p.10.
[18] Ivi, p. 5.
[19] Cass. 20 aprile 1963 n. 990, in Foro it., 1963, I, c. 879.
[20] Corte d'appello di Milano, 26 agosto 1960, in Foro it., 1961, I: ""Violato è […] il diritto alla riservatezza, […] uno dei fondamentali diritti della personalità, […] facoltà giuridica di escludere ogni invadenza estranea dalla sfera della propria intimità personale e familiare".
[21] Cass., *sent. ult. cit.*, c. 879.
[22] Nella sua formulazione originaria così disponeva (v. *infra* per la formulazione vigente, in seguito all'approvazione del c.d. Jobs Act): "È vietato l'uso di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori. Gli impianti e le apparecchiature di controllo che siano richiesti da esigenze organizzative e produttive ovvero dalla sicurezza del lavoro, ma dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori, possono essere installati soltanto previo accordo con le rappresentanze sindacali aziendali, oppure, in mancanza di queste, con la commissione interna. In difetto di accordo, su istanza del datore di lavoro, provvede l'Ispettorato del lavoro, dettando, ove occorra, le modalità per l'uso di tali impianti" […].
[23] "Sono vietati accertamenti da parte del datore di lavoro sulla idoneità e sulla infermità per malattia o infortunio del lavoratore dipendente. Il controllo delle assenze per infermità può essere effettuato soltanto attraverso i servizi ispettivi degli istituti previdenziali competenti, i quali sono tenuti a compierlo quando il datore di lavoro lo richieda. Il datore di lavoro ha facoltà di far controllare la idoneità fisica del lavoratore da parte di enti pubblici ed istituti specializzati di diritto pubblico".

patrimonio aziendale, previo accordo) (art. 6)[24];

d) svolgere indagini (pre o post-assunzione) su opinioni politiche, religiose o sindacali, o fatti non rilevanti circa l'attitudine professionale (art. 8)[25].

La sopracitata norma in tema di videosorveglianza (art. 4) è stata modificata nel 2015 dal d.lgs. 151/2015 (decreto di attuazione del Jobs Act). In particolare, le informazioni raccolte mediante gli strumenti ammessi dalla legge possono essere utilizzate a tutti i fini connessi al rapporto di lavoro purché il lavoratore sia informato delle modalità d'uso degli strumenti e di effettuazione dei controlli, fermo restando il rispetto della vigente normativa in materia di protezione dei dati personali. Più specificatamente, gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dei lavoratori possono essere impiegati solo per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale (purché siano concordati con le rappresentanze sindacali o previa autorizzazione della Direzione Territoriale del Lavoro). Gli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e quelli di registrazione degli accessi e delle presenze, invece, possono essere adoperati dal datore di lavoro senza bisogno di previa autorizzazione od accordo[26].

Le norme dello Statuto dei lavoratori fanno segnare dunque un passo avanti nella tutela della privacy, ma manca un intervento legislativo che esplicitamente lo riconosca e che effettivamente lo tuteli in modo più ampio. Fortunatamente, all'inerzia del legislatore fa seguito un intervento suppletivo della giurisprudenza della Suprema Corte, la quale nel 1975 muta orientamento nella sua pronuncia sul c.d. "caso Soraya"[27], che rappresenta il *leading case* in

[24] "Le visite personali di controllo sul lavoratore sono vietate fuorché nei casi in cui siano indispensabili ai fini della tutela del patrimonio aziendale, in relazione alla qualità degli strumenti di lavoro o delle materie prime o dei prodotti. In tali casi le visite personali potranno essere effettuate soltanto a condizione che siano eseguite all'uscita dei luoghi di lavoro, che siano salvaguardate la dignità e la riservatezza del lavoratore e che avvengano con l'applicazione di sistemi di selezione automatica riferiti alla collettività o a gruppi di lavoratori. Le ipotesi nelle quali possono essere disposte le visite personali, nonché, ferme restando le condizioni di cui al secondo comma del presente articolo, le relative modalità debbono essere concordate dal datore di lavoro con le rappresentanze sindacali aziendali oppure, in mancanza di queste, con la commissione interna. In difetto di accordo, su istanza del datore di lavoro, provvede l'Ispettorato del lavoro" […].

[25] "È fatto divieto al datore di lavoro, ai fini dell'assunzione, come nel corso dello svolgimento del rapporto di lavoro, di effettuare indagini, anche a mezzo di terzi, sulle opinioni politiche, religiose o sindacali del lavoratore, nonché su fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore".

[26] "1. Gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale e possono essere installati previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali. In alternativa, nel caso di imprese con unità produttive ubicate in diverse province della stessa regione ovvero in più regioni, tale accordo può essere stipulato dalle associazioni sindacali comparativamente più rappresentative sul piano nazionale. In mancanza di accordo gli impianti e gli strumenti di cui al periodo precedente possono essere installati previa autorizzazione della Direzione territoriale del lavoro o, in alternativa, nel caso di imprese con unità produttive dislocate negli ambiti di competenza di più Direzioni territoriali del lavoro, del Ministero del lavoro e delle politiche sociali. 2. La disposizione di cui al comma 1 non si applica agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze. 3. Le informazioni raccolte ai sensi dei commi 1 e 2 sono utilizzabili a tutti i fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196".

[27] Cass., 27 maggio 1975, n. 2129, in Foro it., 1976, I, c. 2895. Il caso è stato provocato dalla pubblicazione sul n. 29 del 1968 del periodico "Gente" di un servizio fotografico, realizzato con teleobbiettivo, da cui risultavano ripresi in vari atteggiamenti, anche molto intimi, il regista Franco Indovina e la principessa Soraya Esfandiari, nell'interno della villa di quest'ultima. La Esfandiari lamentava la violazione del suo domicilio, della sua riservatezza e della sua immagine, con pregiudizio del decoro, dell'onore e della reputazione. Il fatto aveva anche un diretto risvolto economico, dal momento che alla principessa era stato attribuito un appannaggio a condizione che mantenesse una vita integra ed illibata.

materia e il formale riconoscimento dell'esistenza del diritto alla privacy nel nostro ordinamento, diritto "consiste[nte] nella tutela di quelle vicende strettamente personali e familiari le quali, anche se verificatesi fuori dal domicilio domestico, non hanno per i terzi un interesse socialmente apprezzabile, contro le ingerenze che, sia pure compiute con mezzi leciti, per scopi non esclusivamente speculativi e senza offesa per l'onore, la reputazione o il decoro, non siano giustificate da interessi pubblici preminenti"[28]. Le norme a fondamento del diritto alla riservatezza individuate dalla Cassazione sono numerose; fra esse si possono citare gli artt. 2 e 3 Cost., l'art. 8 st. lav. e l'art. 8 e 10 della Convenzione del Consiglio d'Europa per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali.

Risulta pertanto di palese evidenza che il diritto alla riservatezza abbia trovato accoglimento in Italia grazie al lavorìo di dottrina e giurisprudenza, ed a parte la legge 121/81 sull'amministrazione della pubblica sicurezza nonché alcuni disegni di legge mai approvati dal Parlamento per svariati motivi, il silenzio legislativo perdura di fatto sino al 1996, anno in cui viene emanata la legge 31 dicembre 1996, n. 675, ossia la c.d. legge sulla *privacy*[29].

Negli anni successivi al caso Soraya, la riflessione dottrinale e giurisprudenziale in tema di riservatezza non si è comunque arrestata, in virtù della sempre crescente problematicità del rapporto tra la tutela della vita privata dell'individuo e il diritto costituzionalmente garantito di libertà di manifestazione del pensiero, con riferimento soprattutto al diritto di cronaca[30]. Nel 1984 il dibattito in materia è diventato molto acceso, in seguito all'emanazione della nota sentenza della Corte di cassazione che ha stabilito il c.d. decalogo dei giornalisti[31], ossia l'identificazione di quelle condizioni al verificarsi delle quali il diritto di cronaca può prevalere sul diritto alla riservatezza. Più precisamente, la Suprema Corte individua tre limiti:

- il *pubblico interesse*, ossia l'utilità sociale della notizia,
- la *verità* dei fatti divulgati;
- la *continenza*, cioè la forma civile dell'esposizione, non eccedente rispetto allo scopo informativo ed improntata a serena obiettività, con esclusione di ogni preconcetto intento denigratorio.

Non è questa la sede per soffermarsi su ulteriori pronunce giurisprudenziali, ma ai nostri fini si può evidenziare che proprio l'operato dei giudici è stato fondamentale per tutelare la privacy anche prima della legge n. 675/96; essi si sono dimostrati molto più pronti del legislatore nel riconoscimento di un diritto fondamentale della persona umana che oltretutto assume un carattere di "garanzia-presupposto" dell'esercizio di altri diritti fondamentali perché violando la sfera intima si può dissuadere l'individuo dal compiere quelle scelte esistenziali per mezzo delle quali esercita il suo diritto di autodeterminarsi[32].

Il concreto soddisfacimento di queste istanze, a volte anche inconsce, della società, è dunque dovuto all'impegno di dottrina e giurisprudenza, che hanno più volte colmato i vuoti

[28] Cass., *sent. ult. cit.*, c. 2905.

[29] Ai sensi della quale ogni ente, impresa od associazione che deteneva archivi magnetici per l'inserimento di dati od informazioni di cittadini, di ogni natura, avrebbe dovuto notificarne l'esistenza al ministero degli interni, consegnandone copia presso la questura territorialmente competente. In caso di dati erronei, incompleti o illegittimamente raccolti, l'interessato avrebbe potuto chiedere al tribunale la cancellazione o l'integrazione (se incompleti); questa legge, emanata nel c.d. periodo dell'emergenza, è stata poi parzialmente abrogata dall'art. 43 comma 1 l. n. 675/96.

[30] G. Giacobbe, *Il diritto alla riservatezza: da diritto di elaborazione giurisprudenziale a diritto codificato*, in *Iustitia*, 1999, 2, p. 111.

[31] Cass. 18 ottobre 1984, n. 5259, in Dir. inf., 1985, 1, p. 143, con nota di S. Fois, G. Giacobbe, F. Morozzo Della Rocca.

[32] M. Aimo*, I «lavoratori di vetro»: regole di trattamento e meccanismi di tutela dei dati personali*, in *Riv. giur. prev. soc.*, 2002, 1, p. 48.

di tutela colpevolmente lasciati dal legislatore[33] mentre sin dagli anni settanta in diversi paesi (si possono qui ricordare Assia, Baviera e Svezia) era iniziato il lungo percorso della regolamentazione dei dati personali e del loro trattamento. La diffusione di sistemi informatici e il loro utilizzo per la creazione e l'utilizzo di banche dati aveva infatti suscitato timori per le conseguenze sulla privacy dei cittadini: non a caso, si parlava sempre più di "privacy informatica", poiché il trattamento automatizzato e incrociato di dati personali metteva (e mette) sempre più in pericolo il diritto alla privacy di ciascuna persona, sia considerata singolarmente che nell'ambito di formazioni sociali delle tipologie più varie. Si consideri, infatti, che soprattutto dal punto di vista quantitativo i trattamenti effettuati con strumenti informatici sono, in linea di principio, estremamente più efficienti di quelli effettuati con strumenti manuali: basti pensare che le tecnologie dell'informazione e della comunicazione permettono di archiviare, memorizzare, reperire, elaborare, comunicare e diffondere dati personali in tempi estremamente rapidi.

L'emanazione della legge n. 675/96 ha comunque posto termine alla lunga inerzia del legislatore italiano in materia di tutela del diritto alla riservatezza, in netto ritardo rispetto ai similari interventi normativi che in alcuni paesi (Svezia, Danimarca, Francia, ecc.) si erano avuti già negli anni settanta, ma appena in tempo per rispettare le prescrizioni dettate dall'Accordo di Schengen del 1985 e dalla direttiva della Comunità Europea 24 ottobre 1995, n. 46. Indipendentemente dalla valutazione qualitativa della legge in oggetto, è evidente che essa, anche grazie all'ottimo operato del Garante per la protezione dei dati personali, ha avuto grande risonanza a livello di riflessione scientifica, come dimostrano i numerosi contributi in materia[34], e, soprattutto, è stata progressivamente recepita dalla popolazione.

Come ribadito dalla Suprema Corte, la fonte primaria del diritto alla riservatezza rimane comunque l'art. 2 Cost., ancorché esso sia previsto da altre norme più specifiche, e la sua violazione dà luogo ad un fatto illecito i cui effetti pregiudizievoli sono risarcibili. La risarcibilità non è tuttavia automatica, giacché il danno non è *in re ipsa*: "il pregiudizio, morale o patrimoniale che sia, attesa la maggiore ampiezza dell'illecito in questione rispetto a quello che si realizza nel caso di lesione del decoro, dell'onore o della reputazione, deve essere provato secondo le regole ordinarie. La parte che chiede il risarcimento del danno prodotto da tale illecito dunque deve provare il pregiudizio alla sua sfera patrimoniale o personale, quale ne sia l'entità e quale che sia la difficoltà di provare tale entità"[35].

[33] L'assenza di normative cogenti ha in alcuni (rari) casi portato a posizioni indifendibili da una parte, seppur infinitesimale, della magistratura: basti pensare a quella sentenza del 1996 del Tribunale di Roma in cui si afferma che [se l'attore] "avesse davvero voluto tutelare la propria riservatezza, alla quale sembra tenere nel presente procedimento, avrebbe dovuto trovare una diversa forma di tutela dei propri diritti e non rivolgersi all'autorità giudiziaria" (Trib. Roma 24 gennaio 1996, in Dir. inf., 1996, 4–5, p. 572, con nota di V. Zeno-Zencovich). ferma restando l'inconcepibilità di una siffatta sentenza, con la quale il giudice romano sembra voler incentivare l'idea di farsi giustizia da sé, bisogna purtroppo ammettere che nel caso di violazione del diritto alla privacy il processo, per sua natura pubblico, potrebbe contribuire all'aggravamento della lesione suddetta. Si pensi al caso Soraya, che, come si è detto, costituisce il *leading case* in materia e che per tale motivo è citato in qualsiasi lavoro che si occupi della ricostruzione storica del diritto alla riservatezza, dunque ben al di fuori dei limiti della vicenda processuale. In ogni caso, successivamente alla emissione di un atto giudiziario un sacrificio della *privacy* si verificherà sempre e comunque, ragion per cui l'attenzione dovrebbe spostarsi verso forme di tutela preventiva che impediscano che si realizzi l'offesa, perché una volta che questa si concretizza nessuna forma di riparazione può consentire un effettivo ripristino della situazione preesistente, potendosi ottenere, al più, un risarcimento monetario.

[34] Ad esempio, C. M. Bianca, F. D. Busnelli. (a cura di), *Tutela della privacy*, in Nuove leggi civ. comm., 1999, 2–3; G. Buttarelli, *Banche dati e tutela della riservatezza. La privacy nella Società dell'Informazione*, Milano 1997; E. Giannantonio, M. G. Losano, V. Zeno–Zencovich, *Commentario alla legge 31 dicembre 1996, n. 675*, Padova 1997.

[35] Cass. 25 marzo 2003, n. 4366, in Dir. inf., 2003, 3, p. 523.

3. IL C.D. CODICE DELLA PRIVACY: ASPETTI GENERALI

In pochi anni la legge n. 675/96 ha subito numerose modifiche ed il suo contenuto è stato in gran parte trasfuso, seppur in alcuni casi con notevoli variazioni, nel d.lgs. 30 giugno 2003, n. 196, ossia il *Codice in materia di protezione dei dati personali* – già detto Codice della privacy (d'ora in poi cod. priv.)[36].

Il Codice, assai vasto e corredato di diversi allegati (fra cui il Disciplinare tecnico in materia di misure minime di sicurezza), è diviso in tre parti: nella prima sono contenute le disposizioni generali e nella seconda alcune disposizioni specifiche, mentre nella terza trovano posto le norme relative alle forme di tutela, alle sanzioni ed all'ufficio del Garante per la protezione dei dati personali (d'ora in poi Garante); le norme del cod. priv. possono, inoltre, essere integrate dalle disposizioni contenute nei codici di deontologia e buona condotta.

La vastità del d.lgs. in oggetto rende palese la sempre maggiore importanza della tutela del diritto alla privacy in una molteplicità di situazioni, e sorprende come in pochi anni la normativa in tema di diritto alla riservatezza abbia fortunatamente colmato una pluridecennale lacuna legislativa, evolvendo da una legge approvata con poca cura per ottemperare ai citati obblighi internazionali dell'Italia ad un codice che, per usare le parole del Garante per la protezione dei dati personali, "rappresenta il primo tentativo al mondo di conformare le innumerevoli disposizioni relative anche in via indiretta alla privacy"[37]. Esso costituisce, inoltre, il recepimento, oltre che di gran parte della legge n. 675/96 e delle norme che l'hanno modificata, anche delle pronunce emanate del Garante e dei pareri forniti dalla medesima *authority*, la cui attività è stata connotata da ragionevolezza e capacità di comprensione delle istanze avanzate da più parti nell'ambito dell'odierna Società dell'informazione.

L'introduzione del Regolamento UE 679/2016 ha tuttavia comportato la necessità di abrogare o modificare il cod. priv.; il legislatore italiano ha alla fine scelto la seconda strada, per cui il Codice è stato fortemente modificato dal d.lgs. 101/2018, recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)".

Il d.lgs. 101/2018 è entrato in vigore il 19 settembre 2018. Il "cuore" della disciplina vigente è però oggi costituito dal c.d. GDPR.

4. IL GDPR: ASPETTI GENERALI

Il GDPR (*General Data Protection Regulation*) è il Regolamento dell'Unione Europea n. 2016/679 del 27 aprile 2016. Ha ad oggetto la protezione delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati all'interno dell'Unione Europea.

Essendo un regolamento europeo, le sue disposizioni sono integralmente obbligatorie ed automaticamente vincolanti in tutti gli Stati membri fin dalla sua entrata in vigore. È bene ricordare che esso prevale su eventuali leggi degli Stati membri incompatibili o contrastanti, in forza del principio del primato (o di preminenza) del diritto europeo su quello nazionale.

Il GDPR costituisce un sostanziale rinnovamento della disciplina previgente e abroga la già citata direttiva 95/46/CE. Essa, a fronte di un celere sviluppo tecnologico, era oramai diventata

[36] La vastità del cod. priv. ne impone, in questa sede, una trattazione esigua, se paragonata alla molteplicità di questioni che scaturiscono dal suo esame, ma comunque finalizzata a fornire al lettore gli elementi di base necessari per una prima lettura del testo in oggetto.

[37] Così si legge nella *Newsletter* n. 176 del Garante per la protezione dei dati personali. Nel cod. priv., del resto, trovano posto disposizioni che toccano tematiche e settori importanti e delicati, come il lavoro e la previdenza sociale, i sistemi bancari, finanziari ed assicurativi, le comunicazioni elettroniche, e così via.

inadeguata e, oltretutto, lasciava ampi margini in relazione al suo recepimento, il che ha comportato un quadro legislativo europeo non del tutto armonizzato in riferimento alla protezione dei dati personali. Tali margini si ridurranno, ma non potranno essere del tutto eliminati, con l'avvento del GDPR: ciascuno Stato membro ha infatti dovuto emanare delle normative in materia, seppur godendo di una minore "libertà d'azione" rispetto alla normativa previgente.

È interessante notare che, nonostante la data di entrata in vigore del GDPR debba individuarsi nel 24 maggio 2016, la sua applicazione diretta sia stata sin dal principio rinviata al 25 maggio 2018: ciò per consentire agli Stati membri di allineare la propria normativa nazionale in materia con le disposizioni del Regolamento, nonché alle aziende di adeguare i propri processi.

Le sanzioni in caso di violazione del GDPR sono molto elevate, potendo giungere sino a venti milioni di euro o al quattro per cento del fatturato globale annuo.

La normativa è molto ampia e complessa, per cui in questa sede è possibile unicamente effettuare brevi cenni senza alcuna pretesa di esaustività o di completezza[38].

Si può partire citando i seguenti principi:

a) **accountability**: il titolare del trattamento deve mettere in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al GDPR. Deve tenere conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche. Dette misure sono riesaminate e aggiornate qualora necessario. Ove ciò sia proporzionato rispetto alle attività di trattamento, le suddette misure includono l'attuazione di politiche adeguate in materia di protezione dei dati da parte del titolare del trattamento;
b) **privacy by design**: il titolare deve mettere in atto misure tecniche e organizzative adeguate (ad es. la pseudonimizzazione) finalizzate ad attuare in modo efficace i principi di protezione dei dati (ad es., la minimizzazione) e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati. Deve tenere conto dello stato dell'arte e dei costi di attuazione, della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento; deve altresì tenere conto dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto.

   Sul titolare grava l'obbligo di attuare misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. Queste misure devono garantire che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.

Tanto premesso, può osservarsi, in relazione all'ambito di applicazione, che il GDPR si applica qualora vi sia un trattamento di dati personali contenuti in un archivio o destinati a figurarvi non solo qualora esso sia effettuato da un titolare che abbia uno stabilimento all'interno dell'Unione europea, ma anche qualora detto stabilimento si trovi al di fuori dell'Unione medesima e ciò nonostante vengano offerti prodotti o servizi (anche

[38] Molte informazioni sul Regolamento sono reperibili dal sito del Garante per la protezione dei dati personali (http://www.garanteprivacy.it/regolamentoue). Non mancano comunque approfondimenti e discussioni sia sui siti web sia sulle riviste giuridiche.

gratuitamente) a interessati ubicati nell'UE o comunque se quest'ultimi sono monitorati nel loro comportamento.

5.1 DATI PERSONALI E LORO TRATTAMENTO

La nozione di dato personale è molto ampia. Per esso si intende "qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale" (art. 4(1) GDPR). Come nella normativa previgente, le persone giuridiche non vengono considerate "interessati".

Anche la nozione di trattamento di dati personali è molto ampia. Esso consiste in "qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione" (art. 4(2) GDPR). In breve, qualsiasi operazione compiuta sui dati personali costituisce attività di trattamento.

I dati personali devono essere:

a) trattati in modo lecito, corretto e trasparente;
b) raccolti e registrati per finalità determinate, esplicite e legittime;
c) esatti e, se necessario, aggiornati. I dati personali devono essere:
d) pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati («minimizzazione» dei dati);
e) conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati;
f) trattati garantendone un'adeguata sicurezza.

Ai sensi dell'art. 6 GDPR, ogni trattamento deve essere fondato su una idonea base giuridica, ossia:

- il consenso,
- l'adempimento di obblighi contrattuali,
- la necessità di tutelare gli interessi vitali della persona interessata o di terzi,
- gli obblighi di legge,
- l'interesse pubblico o l'esercizio di pubblici poteri,
- l'interesse legittimo prevalente del titolare o di terzi cui i dati vengono comunicati.

I diritti dell'interessato sono disciplinati dagli articoli da 15 a 22 del GDPR e brevemente consistono nei diritti di:

- accesso ai propri dati personali;
- rettifica, cancellazione, limitazione del trattamento;
- portabilità;
- opposizione.

5.2 TITOLARE, INTERESSATO E ALTRI SOGGETTI

Diverse figure regolate dalla precedente disciplina sono state "confermate" nel GDPR: in particolare, il titolare, il responsabile e l'interessato. Di particolare interesse è invece l'inserimento del Responsabile della protezione dei dati (RPD, meglio noto con l'acronimo

inglese DPO, ossia "Data Protection Officer").

Il titolare è "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri" (art. 4(7) GDPR). In ogni caso, il titolare deve avere un quadro chiaro e inequivocabile dei trattamenti effettuati e deve utilizzare tutti gli strumenti previsti dal GDPR finalizzati a proteggere adeguatamente i diritti degli interessati, mettendo inoltre in atto misure tecniche e organizzative adeguate a ciascun trattamento specifico, garantendone sempre una sicurezza adeguata al relativo rischio. Possono esservi più titolari ("contitolari").

L'interessato, come si è visto al paragrafo precedente, è la persona fisica cui si riferiscono i dati personali.

Il responsabile è "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento" (art. 4(8) GDPR).

Il responsabile non deve essere confuso con il sopracitato RPD, ossia con il consulente, esperto e qualificato, che affianca il titolare nella gestione delle questioni connesse al trattamento dei dati personali e che lo aiuta a rispettare la normativa vigente. Esso affianca per compiti e responsabilità il titolare stesso; viene nominato dal titolare o dal responsabile del trattamento e può essere selezionato tra i dipendenti del titolare; può altresì essere un libero professionista, esterno e autonomo, incaricato di svolgere questo ruolo.

Oltre al DPO, il GDPR prevede altri soggetti come il "destinatario": "la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi" (art. 4 (9) GDPR). La medesima norma precisa che "le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento".

Il "terzo" è invece "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile" (art. 4(10) GDPR).

5.3 IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Il Garante per la protezione dei dati personali è un'autorità amministrativa indipendente istituita dalla legge 675/96 e poi disciplinata dal cod. priv.; nella versione oggi vigente del cod. priv., il Garante viene designata quale autorità di controllo ai sensi del GDPR.

Il Garante è composto dal Collegio (il suo vertice) e dall'Ufficio; in particolare, il Collegio è composto da quattro componenti eletti due dalla Camera e due dal Senato con voto limitato; durano in carica sette anni e non possono essere rinnovati. In caso di parità, prevale il voto del presidente.

Il Garante ha diversi compiti, fra cui:

- controllare la conformità dei trattamenti alla normativa vigente;
- esaminare i reclami;
- rivolgere ammonimenti al titolare e/o al responsabile;
- ingiungere di conformare i trattamenti al GDPR;
- imporre limitazioni provvisorie o definite al trattamento;
- ordinare la rettifica, la cancellazione di dati o la limitazione del trattamento, ecc.

5.4 CENNI SULL'AUTENTICAZIONE INFORMATICA

Per consentire a un sistema informatico di riconoscere un eventuale utilizzatore è possibile far ricorso a strumenti che lo identificano, basati su qualcosa che:

- conosce (ad es., nome utente e password),
- possiede (ad es., un token USB che genera password casuali riconosciute dal sistema),
- ha (ad es., l'impronta digitale),
- o loro combinazioni (ad es., password e token USB).

La prassi mostra come le problematiche di sicurezza siano estremamente delicate e come anche sistemi informatici di titolarità di importanti aziende possano essere violati: fra i tanti, basti pensare al caso di Adobe, avvenuto nell'ottobre del 2013, quando i dati di milioni di utenti sono stati acquisiti. È interessante notare come, dall'esame della lista delle password più utilizzate, emerga un disinteresse degli utenti verso la scelta della propria password: ad es., nel caso anzidetto, le password più utilizzate risultavano essere 123456, 123456789, password, adobe123, 12345678, ecc. (e altrettanto può dirsi in relazione a numerosi altri casi simili che si verificano costantemente).

5.5 CENNI SU ALCUNI CASI CONCRETI

Si effettuano di seguito brevi cenni su alcuni casi concreti particolarmente significativi (relativi, ovviamente, alla normativa precedente al GDPR).

Diritto all'oblio e motori di ricerca

La rimozione di dati personali dalla SERP di un motore di ricerca è una questione alquanto delicata ed espressione delle difficoltà di esercitare il diritto all'oblio nell'era di Internet. Nel caso di specie, un cittadino spagnolo lamentava che, all'esito di una ricerca sul motore Google, venivano indicati due link relativi a un annuncio, pubblicato su un quotidiano del 1998, di vendita all'asta di immobili connessa ad un pignoramento effettuato per la riscossione coattiva di crediti previdenziali. La questione era stata tuttavia definita da diversi anni e dunque la sua menzione non aveva più alcuna rilevanza, per cui egli si rivolgeva all'Agencia Española de Protección de Datos (AEPD) per ottenere sia la soppressione o la modificazione delle predette pagine (o l'utilizzo di strumenti di protezione dei suoi dati sui motori di ricerca) sia l'eliminazione o l'occultamento dei dati dalla SERP.

L'AEPD ha respinto il reclamo nei confronti dell'editore del quotidiano, ma non nei confronti di Google, in quanto soggetto intermediario della Società dell'informazione e responsabile dei trattamenti dei dati personali; può pertanto ordinarsi la rimozione dei dati nonché il divieto di accesso a taluni dati da parte dei gestori di motori di ricerca, qualora la localizzazione e la diffusione degli stessi possano ledere il diritto fondamentale alla protezione dei dati e la dignità delle persone in senso ampio, e ciò anche prescindendo dalla cancellazione dei dati o delle informazioni dal sito web indicizzato.

La questione è stata decisa dalla Corte di Giustizia dell'Unione europea il 13 maggio 2014, confermando sostanzialmente quanto affermato dall'AEPD. In particolare, secondo la Corte, i diritti fondamentali di cui agli artt. 7 (Rispetto della vita privata e della vita familiare) e 8 (Protezione dei dati di carattere personale) della Carta dei diritti fondamentali dell'Unione europea "prevalgono, in linea di principio, non soltanto sull'interesse economico del gestore del motore di ricerca, ma anche sull'interesse di tale pubblico ad accedere all'informazione suddetta in occasione di una ricerca concernente il nome di questa persona. Tuttavia, così non sarebbe qualora risultasse, per ragioni particolari, come il ruolo ricoperto da tale

persona nella vita pubblica, che l'ingerenza nei suoi diritti fondamentali è giustificata dall'interesse preponderante del pubblico suddetto ad avere accesso, in virtù dell'inclusione summenzionata, all'informazione di cui trattasi".

Google ha poi reso disponibile un modulo on line di richiesta di rimozione dei risultati (https://support.google.com/legal/contact/lr_eudpa?product=websearch); l'azienda afferma che provvederà a valutare ogni richiesta effettuando "un bilanciamento tra il diritto alla privacy della persona e il diritto di rendere accessibili le informazioni e l'interesse pubblico a trovarle", considerando "se i risultati includono informazioni obsolete sul richiedente e se le informazioni sono di interesse pubblico".

Caso Peppermint

Il celebre caso Peppermint è stato originato dalla ricezione di numerose segnalazioni. Esso si è verificato quando una società svizzera ha acquisito l'indirizzo IP relativo a migliaia di utenti che condividevano e scaricavano determinate opere dell'ingegno (fra cui brani musicali) mediante reti di P2P. La Peppermint Jam Records GMBH ha dunque chiesto, in via giudiziaria, che il relativo provider fornisse i dati identificativi dei propri abbonati relativamente ai suddetti indirizzi IP. Ottenuti i dati di 3.636 intestatari, sono state inviate altrettante diffide che hanno tuttavia suscitato forti polemiche e che hanno portato all'intervento del Garante. Del resto, anche ammesso che un'opera dell'ingegno sia stata illecitamente scaricata e condivisa mediante una linea identificabile grazie al raffronto fra l'indirizzo IP dell'elaboratore mediante il quale è stata posta in essere la condotta illecita e fra la singola linea che corrisponde a quell'indirizzo IP in base a quanto risulta dai registri informatici (i c.d. log), dell'Internet provider, non è detto che l'intestatario della linea stessa abbia materialmente posto in essere la violazione contestata, dal momento che ad una singola linea possono essere connessi in rete più elaboratori, addirittura contro la volontà dell'intestatario della linea stessa.

La situazione giudiziaria, così, si è ribaltata e il Tribunale di Roma, con ordinanza del 16 luglio 2007, ha affermato che la compressione del diritto alla riservatezza può avvenire solo "per la tutela di valori di rango superiore e che attengono alla difesa della collettività ovvero alla protezione dei sistemi informatici".

Inoltre, con provvedimento del 28 febbraio 2008, il Garante ha disposto "il divieto dell'ulteriore trattamento dei dati personali relativo a soggetti ritenuti responsabili di aver scambiato file protetti dal diritto d'autore tramite reti peer-to-peer" e la loro cancellazione entro il 31 marzo 2008.

Caso Google Street View

Il caso di Google Street View (15 ottobre 2010) è stato portato all'attenzione del Garante in seguito alla ricezione di numerose segnalazioni. L'Autorità ha disposto l'esecuzione di diverse misure per tutelare la privacy delle persone che si trovano nei luoghi ripresi dai mezzi di Google: in particolare, pubblicazione della notizia della raccolta sul web e su due quotidiani, svolgimento di pubblicità via radio e modalità per garantire la riconoscibilità delle auto utilizzate.

Di particolare interesse risulta una delle motivazioni addotte da Google: "poiché si tratta di un servizio globale gestito in modo centralizzato, era difficile per Google tenere conto di tutte le normative privacy dei singoli Stati dove il servizio è attivo e soddisfare tutti i singoli requisiti da esse previsti". Ovviamente, tale tesi non può trovare accoglimento, poiché un soggetto non può esimersi dall'applicazione della normativa di uno stato in cui opera.

Con ordinanza-ingiunzione del 18 dicembre 2013, Google Inc. è stata condannata a pagare 1.000.000,00 di Euro a titolo di sanzione amministrativa pecuniaria per la violazione

del combinato disposto di cui agli artt. 13, 161 e 164-bis, comma 2, del cod. priv..

Telemarketing e telefonate "mute"

Con delibera del 20 febbraio 2014 (in G.U. 4 aprile 2014), il Garante, facendo seguito alla relativa consultazione pubblica del 30 ottobre 2013, ha disposto l'adozione di specifiche misure per combattere il fenomeno delle chiamate "mute" dovuto alla condotta di numerosi *call center* (per cui le chiamate vengono effettuate prima ancora che vi sia un operatore libero). Numerosi interessati hanno infatti segnalato la ricezione di molte telefonate di tale tipologia, senza sapere se venivano effettuate per l'appunto da call-center oppure da eventuali malintenzionati (palese il riferimento allo stalking).

Fra le predette regole, si possono qui ricordare:

- obbligo di tracciamento delle "chiamate mute" (durata massima: 3 secondi dalla risposta);
- massimo 3 telefonate "mute" ogni 100 andate "a buon fine";
- divieto di attesa silenziosa e obbligo di generazione di rumore ambientale;
- divieto di contatto per 5 giorni dopo 1 "chiamata muta", con obbligo di successiva chiamata mediante operatore;
- obbligo di conservazione per 2 anni dei report statistici delle telefonate "mute".

Spam e phishing

Lo spam consiste, in linea generale, nell'invio massiccio e ripetuto di comunicazioni non richieste, in violazione del d.lgs. 196/2003. Può essere realizzato utilizzando vari strumenti: email, fax, telefono, sms, mms.

È bene ricordare che lo spam non è finalizzato esclusivamente all'invio di comunicazioni pubblicitarie, ma è spesso legato a truffe on line, con particolare riferimento al fenomeno del *phishing* (quando un soggetto tenta di convincere un altro soggetto a fornire dati particolarmente delicati, come quelli di accesso al proprio *home banking*. Ciò viene normalmente effettuato mediante email costruite, anche graficamente, in modo da sembrare provenienti da un istituto bancario).

È estremamente arduo lottare contro tali fenomeni e anche in questi casi è necessario adottare una condotta diligente. Così, non è opportuno rispondere a un messaggio di spam o effettuare click su link presenti in simili email, atteso che in tali casi lo "spammer" viene a conoscenza del fatto che l'indirizzo email in questione è attivamente utilizzato. Qualora, invece, vi sia una ragionevole certezza che il messaggio provenga effettivamente da un soggetto "affidabile" che ciò nonostante potrebbe aver violato il cod. priv., sarà invece opportuno effettuare una opposizione al trattamento dei dati personali, come previsto dalla normativa vigente. Non bisogna, ovviamente, scaricare e installare file eseguibili (spesso "mascherati" con finte estensioni che precedono quella propria dei file eseguibili) né inviare incautamente le proprie credenziali di accesso[39].

[39] Ulteriori approfondimenti saranno effettuati nel corso della lezione dedicata a "Le insidie della Rete".