Corso di Diritto di Internet
2017-2018

DIRITTO DI INTERNET: CASI E MATERIALI
INDICE

INTERNET E CYBERLAW............................................. 5
N. Lugaresi - Diritto pubblico di Internet e cyberlaw .................................................... 7
1. INTERNET, CYBERSPACE, DIRITTO .................................................... 11
   1.1. Tecnologia e diritto .................................................................................. 13
       Supreme Court of the United States, 11 June 2001, n.99-8508 (Kyllo v. United States) [syllabus] .............................................................................................................. 13
   1.2. Luoghi reali, luoghi virtuali, cyberspace .................................................. 15
       United States Court of Appeals, 11th Circuit, 21 September 2001, n.00-16346 (Voyeur Dorm v. City of Tampa) ................................................................. 15
   1.3. Accesso a Internet .................................................................................... 19
       Supreme Court of the United States, 19 June 2017, n.15-1194 (Packingham v. North Carolina) [syllabus] ............................................................... 19
2. INTERNET E GIURISDIZIONE .................................................. 21
   2.1. Giurisdizione e valori .............................................................................. 23
       Tribunal de Grande Instance de Paris, ordonnance 22 mai 2000 (LICRA v. Yahoo) ........................................................................................................... 23
   2.2. Trasferimento di dati e livello di tutela in altra giurisdizione ..................... 27
       Corte di Giustizia dell’Unione Europea, 6 ottobre 2015 (causa C-382/14) ...................................................................................................................... 27
       Corte di Giustizia dell’Unione Europea, 1 ottobre 2015 (causa C-230/14) .................................................................................................................. 39
   2.3. Tutela dei dati personali e stabilimento in altro Stato membro .................. 39
       Corte di Giustizia dell’Unione Europea, 6 ottobre 2015 (causa C-382/14) ...................................................................................................................... 27
3. LE REGOLE DI INTERNET .................................................. 47
   3.1. Analogia, metafore, cyberspace .............................................................. 49
       Supreme Court of California, 30 June 2003, n.S103781 (Intel v. Hamidi) .............. 49
   3.2. Reati commessi a mezzo Internet e analogie ......................................... 53
       Corte di Cassazione, sez.I penale, 28 aprile 2015, n.24431 .................................. 53
   3.3. L’anarchia della Rete ............................................................................. 55
   3.4. Le norme sociali ...................................................................................... 57
       RFC 1855 – Netiquette guidelines, 28 October 1995 ........................................... 57
   3.5. Internet e principi .................................................................................... 61
       Dichiarazione dei diritti in Internet (Camera dei Deputati, luglio 2015) ................. 61
4. RESPONSABILITÀ DELL’INTERNET SERVICE PROVIDER ..................... 65
   4.1. Responsabilità dell’Internet service provider per commenti di utenti ............ 67
       European Court of Human Rights, Grand Chamber, 16 June 2015, appl. n.64569/09 (Delfi v. Estonia) ................................................................. 67
       European Court of Human Rights, Fourth Section, 2 February 2016, appl. n.22947/13 (MTE and Index.hu v. Hungary) ........................................... 91
   4.2. Mancata informativa e responsabilità del provider .................................... 83
       Corte di Cassazione, sez.III penale, 3 febbraio 2014, n.5107 .................................. 83
   4.3. Qualità dei commenti e responsabilità dell’Internet service provider .......... 91
   4.4. Ruolo neutro o attivo del service provider ............................................. 103
       Corte di Giustizia dell’Unione Europea, 23 marzo 2010 (cause da C-236/08 a C-238/08) .................. 103
   4.5. Responsabilità del fornitore di rete locale senza fili .................................. 111
       Corte di Giustizia dell’Unione Europea, 15 settembre 2016 (causa C-484/14) ........... 111
5. PRIVACY E PROTEZIONE DEI DATI PERSONALI .............................. 121
   5.1. Trattamenti e trasferimenti di dati personali in Rete .................................. 123
       Corte di Giustizia della Comunità Europea, 6 novembre 2003 (causa C-101/01) .......... 123
   5.2. Diritti di proprietà intellettuale e tutela della riservatezza ............................ 129
       Corte di Giustizia delle Comunità Europee, 29 gennaio 2008 (causa C-275/06) .......... 129
6. PRIVACY E COMUNICAZIONI ................................................ 133
   6.1. Comunicazioni elettroniche e sorveglianza .......................................... 135
       Corte di Giustizia delle Comunità Europee, 8 aprile 2014 (cause riunite C-293/12 e C-594/12) ..................................................... 135
   6.2. Posta elettronica non sollecitata .............................................................. 143
Garante per la protezione dei dati personali, provv. generale 4 luglio 2013 ........................................... 143

7. PRIVACY E DIRITTO ALL’OBLIO ........................................................................................................... 151

7.1. Diritto all’oblio in Rete ....................................................................................................................... 153

Garante per la protezione dei dati personali, provv. 10 novembre 2004 ..................................................... 153

7.2. Diritto all’oblio e responsabilità del motore di ricerca .................................................................... 157

Corte di Giustizia dell’Unione Europea, 13 maggio 2014 (causa C-131/12) .............................................. 157

8. PRIVACY E PERSONALITÀ ................................................................................................................... 171

8.1. Privacy ed espressione della personalità ........................................................................................... 173

Consiglio di Stato, sez.III, 21 febbraio 2014, n.848 .................................................................................. 173

9. LIBERTÀ’ DI ESPRESSIONE IN RETE .................................................................................................. 179

9.1. Linguaggio offensivo e indecente in Rete e libertà di parola ............................................................... 181

Supreme Court of the United States, 26 June 1997, n.96/511 (Reno v. ACLU) [syllabus] ....................... 181

9.2. Pedopornografia virtuale e libertà di parola ...................................................................................... 185

Supreme Court of the United States, 16 April 2002, n.00-795 (Ashcroft v. Free Speech Coalition) [syllabus] ........................................................................................................................................... 185

9.3. Minacce in Rete e libertà di espressione ............................................................................................ 189

Corte di Appello degli Stati Uniti, 9th Circuit, 16 May 2002, n.99-35320 (Planned Parenthood of the Columbia/Willamette Inc. v. ACLA) .......................................................................................................................... 189

9.4. Libertà di espressione e hate speech .................................................................................................. 195

Code of conduct on countering illegal hate speech online ...................................................................... 195

10. LIBERTÀ’ DI INFORMAZIONE IN RETE ............................................................................................ 199

10.1. Diritto all’oblio e aggiornamento delle notizie in Rete .................................................................... 201

Corte di Cassazione, sez.II civile, 5 aprile 2012, n.5525 ......................................................................... 201

10.2. Testata giornalistica telematica e sequestro preventivo .................................................................. 209

Corte di Cassazione, sez.un. penali, 29 gennaio 2015, n.31022 .............................................................. 209

10.3. Giornale telematico e tutela costituzionale ...................................................................................... 223

Corte di Cassazione, sez.un. civili, 25 ottobre 2016, n.23469 ................................................................. 223

11. DIRITTI ECONOMICI E SOCIETÀ DELL’INFORMAZIONE .............................................................. 231

11.1. Diritti d’autore e ruolo del provider ................................................................................................ 233

Corte di Giustizia dell’Unione Europea, 16 febbraio 2012 (causa C-360/10) ............................................. 233

11.2. Diritto d’autore e link ...................................................................................................................... 239

Corte di Giustizia dell’Unione Europea, 13 febbraio 2014 (causa C-466/12) ............................................. 239

11.3. Diritto d’autore e cache .................................................................................................................. 243

Corte di Giustizia dell’Unione Europea, 5 giugno 2014 (causa C-360/13) ............................................... 243

12. L’USO DI INTERNET SUL LUOGO DI LAVORO .............................................................................. 249

12.1. Controlli in Rete sul lavoratore e privacy ....................................................................................... 251

European Court of Human Rights, Fourth Section, 3 April 2007 – appl. n.62617/00 (Copland v. United Kingdom) ........................................................................................................................................ 251

12.2. Controllo della corrispondenza sul luogo di lavoro ....................................................................... 255

European Court of Human Rights, Grand Chamber, 5 September 2017, appl. n.61496/08 (Bârbulescu v. Romania) ........................................................................................................................................ 255

12.3. Uso di posta elettronica ed Internet sul luogo di lavoro ................................................................. 263

Garante per la protezione dei dati personali, delib. n.13 del 1 marzo 2007 ............................................. 263

12.4. Pubblici dipendenti e uso di posta elettronica ed Internet .............................................................. 271

Presidenza del Consiglio dei Ministri, direttiva n.2/2009 del 26 maggio 2009 ........................................ 271
INTERNET E CYBERLAW
N. Lugaresi - Diritto pubblico di Internet e cyberlaw

(Il presente scritto riprende, con parziali modificazioni, l’articolo “Regole, diritti ed interessi in Rete: il diritto pubblico di Internet”, pubblicato su Giustizia Amministrativa on-line, n.10-2006)

1. Cyberlaw e diritto di Internet

Il termine cyberlaw, comunemente usato nei Paesi anglosassoni, non è facilmente traducibile. Diritto di Internet potrebbe essere una soluzione, ma Internet Law e cyberlaw non sono necessariamente coincidenti. Ancora più complesso è stabilire se con il termine cyberlaw sia possibile identificare una branca autonomo del diritto, non nuova, ma ancora in via di costruzione ed elaborazione, o se invece tale termine abbia solamente una connotazione descrittiva. Certo è interessante notare come anche negli Stati Uniti, che hanno un approccio generalmente più pragmatico e concreto al diritto rispetto all’Europa continentale, un dibattito di questo tipo, di carattere prevalentemente teorico, si sia sviluppato. Infine, non è chiaro quale sia lo spazio che il diritto pubblico, ed in particolare il diritto amministrativo, possano occupare in un settore che ancora sta cercando una propria sistemazione.

Al di là della sua autonomia o meno, la cyberlaw (per comodità si preferisce per il momento utilizzare questa definizione) costituisce un diritto relativamente nuovo, per il quale non sempre possono essere utilizzati, direttamente o per analogia, criteri giuridici già esistenti. In questo senso, come diritto complesso, che interagisce con le altre branchie tradizionali, esso comporta una rivisitazione di principi giuridici, di cui si deve verificare la capacità di adattamento di fronte a nuovi fenomeni. Si tratta di un diritto in via di continuo e frenetico sviluppo, che segue e nel contempo cerca di precedere, la tecnologia, e nel quale è possibile, più che in altri settori, un’attività creativa, di carattere normativo, interpretativo, giurisprudenziale.

L’oggetto della cyberlaw è, se non totalmente, almeno difficilmente compatibile con costruzioni dogmatiche e classificazioni astratte, sia per la velocità con cui nascono i problemi (rapporti interprivati, rapporti tra cittadini e pubblici poteri, profili internazionali), e conseguentemente devono essere ricercate le soluzioni giuridiche (in sede normativa o giurisprudenziale, ma anche in sede di autoregolamentazione), sia in rapporto all’evoluzione dei riferimenti tecnologici (hardware, software, architettura della Rete). Anche se, rispetto ad altre branche, si può dire che si tratti di differenze quantitative, più che qualitative (i cambiamenti di contesto, e normativi, sono comuni a tutto il diritto vivente), ciò non toglie che la velocità del cambiamento costituisca un elemento sostanziale di valutazione.

D’altra parte, anche qualora non si volesse riconoscere alla cyberlaw una sua autonomia “ontologica”, il dibattito teorico su di essa non è aprioristicamente destinato ad un insuccesso. Se nel dibattito teorico non si perde il contatto con le problematiche giuridiche reali, tenendo conto della funzionalità degli aspetti teorici rispetto alla ricerca di soluzioni giuridiche idonee a migliorare la situazione di fatto, ecco allora che le energie impiegate nello sforzo non saranno da ritenersi sprecate. La considerazione dei profili teorici può aggiungere, e non togliere, un valore alla migliore comprensione dei nuovi fenomeni giuridici che l’interrelazione con Internet quotidianamente comporta. Diritto pubblico e diritto amministrativo non possono rimanere estranei a tale processo.

2. L’evoluzione della cyberlaw

La cyberlaw è, e sarà sempre di più, soggetta a processi evolutivi. Si può prevedere che, per essa, ci siano tre possibili alternative: a) la cyberlaw conquista e consolida un certo livello di autonomia, in virtù delle sue caratteristiche intrinseche; b) la cyberlaw, nel rispetto di una propria autonomia, si divide in sottodiscipline, anche per motivi pratici legati alla formazione degli operatori del diritto; c) le discipline tradizionali si riappropriano progressivamente delle tematiche attualmente considerate dalla cyberlaw, e quindi, pro quota, della cyberlaw stessa, che viene pertanto progressivamente smembrata fino a scomparire. Ognuna di queste teorie ha un suo fondamento.

a) La cyberlaw può essere vista come disciplina autonoma, in quanto ha principi ed istituti comuni. Al di là degli aspetti soggettivi (backgrounds e modi di pensare, intesi anche come metodologie comuni), che costituiscono un elemento di unificazione della disciplina, l’aspetto
tecnologico è un altro fattore rilevante, inteso sia in senso strumentale (Internet come oggetto della ricerca), che in senso sostanziale (la regolamentazione inserita nella tecnologia stessa). In questo senso la cyberlaw ha un carattere autonomo, ma anche trasversale, e proprio tale trasversalità potrebbe garantire alla stessa autonomia.

(b) Se si può riconoscere non solo una certa autonomia, ma anche una certa unitarietà, alla cyberlaw, la tendenza è però nel senso di un cambiamento, che porta la stessa a dividersi in più sottodiscipline, con punti di contatto, ed eventualmente istituti e principi comuni, ma anche con caratteristiche sostanzialmente divergenti, proprio per la connessione naturale con le branche tradizionali del diritto. L’alternativa è di considerare la cyberlaw quale momento di eversione complessiva delle categorie giuridiche tradizionali. La distinzione in sottodiscipline è probabilmente destinata a costituire non tanto l’esito finale, quanto una fase intermedia, anche se di lunga durata, in virtù di due fattori. Da un lato, la vastità, destinata ad aumentare, degli argomenti trattati dalla cyberlaw, richiede conoscenze ed esperienze diverse, difficilmente riassumibili in una sola sede. Dall’altro, la diffusa mancanza di capacità, o di interesse, ad affrontare tali tematiche nell’ambito delle discipline tradizionali potrà rallentare il passaggio alla fase successiva.

(c) L’assorbimento delle sottodiscipline della cyberlaw nelle discipline tradizionali è in questo senso un processo, se non ineluttabile, assai probabile. Questo non significa che la cyberlaw non possa mantenere una propria, seppure limitata, autonomia attorno ad un nucleo comune costituito da aspetti trasversali e strumentali. La cyberlaw potrà sopravvivere come diritto, in un certo senso, procedurale, anche se in un’accezione diversa da quella usuale. Gli aspetti sostanziali si fonderanno invece nelle discipline tradizionali, non in maniera neutra e passiva, ma anzi contaminando le stesse. La cyberlaw, comunque intesa, non sarà pertanto altro che una parte, “moderna”, delle singole branche del diritto.

3. Il diritto pubblico di Internet

Considerando gli oggetti di cui la cyberlaw si occupa, ci si può chiedere se essa possa essere affrontata in via unitaria. Se è vero che ci sono aspetti comuni, che chiunque si troverà ad affrontare la porzione “cyber” della propria disciplina dovrà conoscere (si pensi ad aspetti tecnologici, quali l’uso della crittografia o degli strumenti di identificazione, ma anche a limiti oggettivi, quali quelli relativi alla giurisdizione, che caratterizzano fortemente il settore), è anche vero che la vastità trasversale degli oggetti della disciplina non rendono credibile un approccio olistico ed omnicomprensivo.

Dal punto di vista di un sistema di civil law, le normative esistenti potranno essere applicate frequentemente anche ai nuovi fenomeni, e altre volte potranno costituire uno strumento di interpretazione analogica. Ma altre volte ancora, poche o molte non importa da un punto di vista teorico, le risposte dovranno essere costruite ex novo, e probabilmente il diritto (in generale, non solo la cyberlaw) subirà comunque un processo di aggiustamento dovuto alle nuove esigenze.

La considerazione unitaria ed autonoma della cyberlaw, anche se temporaneamente limitata, offrirà poi la possibilità di rivedere l’equilibrio interno della stessa. Attualmente, per una serie di motivi, essa è sbilanciata, facendo riferimento alle categorie generali tradizionali, verso il diritto privato, ai danni del diritto pubblico. Probabilmente, la consapevolezza di tale squilibrio è già presente, portata alla luce da problemi insorti nell’ambito di una visione estremamente commerciale della Rete, dopo quella militare, quella accademica e quella relazionale, e, conseguentemente, del suo diritto.

In questo senso la cyberlaw è destinata a superare, almeno parzialmente, la distinzione tra categorie spesso troppo rigide, non potendosi sempre tracciare una netta linea di confine, aiutando a conoscere sempre di più “l’altro settore”, ed a cercare di entrare in un “altro” habitus mentale, per capire il proprio. Ciò è evidente in riferimento a macrocategorie (diritto pubblico e diritto privato), ma anche in riferimento a sottocategorie (ad esempio, diritto dell’informazione e diritto della proprietà intellettuale).

In questo senso, non è una novità che nuove branche del diritto non possano essere incluse nella bipartizione diritto privato - diritto pubblico (si pensi al diritto ambientale). La novità della cyberlaw è l’estensione del suo carattere trasversale, che da un lato ne determinerà probabilmente l’assorbimento, anche se forse non totale, da parte delle altre discipline, ma che dall’altro ne costituirà, altrettanto probabilmente, il valore aggiunto, come momento di ripensamento di molte parti del diritto.
Lo studio della cyberlaw, e dei fenomeni ad essa afferenti, può del resto essere affrontato secondo due prospettive. La prima è una prospettiva “interna”, dell’utilizzatore di Internet, che si trova ad operare in un luogo, o in un non-luogo, il cyberspace, caratterizzato da dinamiche spesso diverse da quelle proprie del “mondo reale”. La seconda è una prospettiva “esterna”, che fa riferimento alle applicazioni tecnologiche che stanno alla base della creazione del cyberspace (sistemi di connessione, reti, trasferimento di dati e così via) ed alle relazioni di tali applicazioni con le attività umane giuridicamente rilevanti, cercando di coglierne le specificità ed i caratteri distintivi. In ogni caso, la modificazione del cyberspace, secondo la prima prospettiva, o delle applicazioni tecnologiche, nella seconda prospettiva, richiedono la costruzione di categorie giuridiche duttili e mobili, aventi un obiettivo di sistemazione costante e continua della disciplina.

Prima ancora, la regolamentazione del cyberspace, sia che si tratti di regolamentazione da parte dei pubblici poteri, di autoregolamentazione, o di regolamentazione indiretta attraverso scelte tecnologiche, necessita di principi, di criteri, di riferimenti di carattere generale. È in questo spazio, giuridico, che diritto pubblico e diritto amministrativo devono intervenire per fissare gli obiettivi fondamentali, garantire l’interesse pubblico, assicurare la convivenza tra cittadini, operatori economici, pubbliche amministrazioni, formazioni sociali.

In sostanza, il diritto pubblico di Internet dovrebbe analizzare le diverse problematiche che Internet propone, cercando di fornire soluzioni che riproducano i valori che la collettività ritiene prioritari. In via esemplificativa, e senza pretese di completezza, il diritto pubblico dovrà occuparsi dei profili di regolamentazione (attraverso l’intervento legislativo e regolamentare), regolazione (attraverso atti di regolazione di autorità amministrative indipendenti, attraverso il riconoscimento ed il controllo della self-regulation, attraverso l’intervento sull’architettura della Rete, attraverso il riconoscimento del ruolo del mercato e delle norme sociali) e di garanzia (tutela degli interessi diffusi degli utenti); dei profili relativi alla tutela dei diritti e degli interessi individuali e collettivi (tutela della privacy; della libertà di espressione; della segretezza delle comunicazioni; della libertà di stampa); dei profili organizzativi (autorità garanti e organismi tecnici); dei profili relativi alla società dell’informazione ed all’e-government (circolazione delle informazioni pubbliche; fornitura di servizi al cittadino; accesso agli atti), all’e-procurement e a tutti quegli altri profili caratterizzati dall’influenza della rivoluzione digitale. Il diritto pubblico di Internet, in sostanza, si deve occupare di individuazione delle regole, di tutela dei diritti, di cura degli interessi pubblici. Nel farlo, dovrà misurarsi con i cambiamenti continui della tecnologia, con le concorrenti prospettive giuridiche (privatistiche, penalistiche, internazionalistiche, e così via) proprie di altri settori, con la necessità di ripensare categorie e classificazioni tradizionali del diritto. Se manterrà un equilibrio nella sua esistenza, corta o lunga che sia, il diritto pubblico di Internet riuscirà a trasmettere qualcosa, e a non rappresentare solamente una parentesi descrittiva delle soluzioni innovative individuate per rispondere a problematiche relative a fenomeni nuovi.

Riferimenti bibliografici essenziali

LESSIG, L., Code and Other Laws of Cyberspace, Basic Books, 1999

*****

DISCUSSIONE

1. È rilevante, per voi, classificare e riconoscere autonomia alla cyberlaw?
2. Quale è il rapporto tra cyberlaw e tecnologia?
3. Quali sono i possibili stadi evolutivi della cyberlaw?
4. Di cosa si occupa il diritto pubblico di Internet?
1. INTERNET, CYBERSPACE, DIRITTO
Supreme Court of the United States, 11 June 2001, n.99-8508 (Kyllo v. United States)

[ syllabus ]

Suspicious that marijuana was being grown in petitioner Kyllo’s home in a triplex, agents used a thermal imaging device to scan the triplex to determine if the amount of heat emanating from it was consistent with the high-intensity lamps typically used for indoor marijuana growth. The scan showed that Kyllo’s garage roof and a side wall were relatively hot compared to the rest of his home and substantially warmer than the neighboring units. Based in part on the thermal imaging, a Federal Magistrate Judge issued a warrant to search Kyllo’s home, where the agents found marijuana growing. After Kyllo was indicted on a federal drug charge, he unsuccessfully moved to suppress the evidence seized from his home and then entered a conditional guilty plea. The Ninth Circuit ultimately affirmed, upholding the thermal imaging on the ground that Kyllo had shown no subjective expectation of privacy because he had made no attempt to conceal the heat escaping from his home. Even if he had, ruled the Court, there was no objectively reasonable expectation of privacy because the thermal imager did not expose any intimate details of Kyllo’s life, only amorphous hot spots on his home’s exterior.

Held: Where, as here, the Government uses a device that is not in general public use, to explore details of a private home that would previously have been unknowable without physical intrusion, the surveillance is a Fourth Amendment “search,” and is presumptively unreasonable without a warrant.

(a) The question whether a warrantless search of a home is reasonable and hence constitutional must be answered no in most instances, but the antecedent question whether a Fourth Amendment “search” has occurred is not so simple. This Court has approved warrantless visual surveillance of a home, see California v. Ciraolo [...] ruling that visual observation is no “search” at all, see Dow Chemical Co. v. United States [...]. In assessing when a search is not a search, the Court has adapted a principle first enunciated in Katz v. United States [...] A “search” does not occur - even when its object is a house explicitly protected by the Fourth Amendment - unless the individual manifested a subjective expectation of privacy in the searched object, and society is willing to recognize that expectation as reasonable, see, e.g., California v. Ciraolo [...].

(b) While it may be difficult to refine the Katz test in some instances, in the case of the search of a home’s interior - the prototypical and hence most commonly litigated area of protected privacy - there is a ready criterion, with roots deep in the common law, of the minimal expectation of privacy that exists, and that is acknowledged to be reasonable. To withdraw protection of this minimum expectation would be to permit police technology to erode the privacy guaranteed by the Fourth Amendment. Thus, obtaining by sense-enhancing technology any information regarding the home’s interior that could not otherwise have been obtained without physical “intrusion into a constitutionally protected area”, Silverman v. United States [...], constitutes a search - at least where (as here) the technology in question is not in general public use. This assures preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.

(c) Based on this criterion, the information obtained by the thermal imager in this case was the product of a search. The Court rejects the Government’s argument that the thermal imaging must be upheld because it detected only heat radiating from the home’s external surface. Such a mechanical interpretation of the Fourth Amendment was rejected in Katz, where the eavesdropping device in question picked up only sound waves that reached the exterior of the phone booth to which it was attached. Reversing that approach would leave the homeowner at the mercy of advancing technology - including imaging technology that could discern all human activity in the home. Also rejected is the Government’s contention that the thermal imaging was constitutional because it did not detect “intimate details”. Such an approach would be wrong in principle because, in the sanctity of the home, all details are intimate details. See e.g., United States v. Karo [...] Dow Chemical Co. v. United States [...]. It would also be impractical in application, failing to provide a workable accommodation between law enforcement needs and Fourth Amendment interests. See Oliver v. United States [...].
(d) Since the imaging in this case was an unlawful search, it will remain for the District Court to determine whether, without the evidence it provided, the search warrant was supported by probable cause - and if not, whether there is any other basis for supporting admission of that evidence.

*****

DISCUSSIONE

1. Cosa è, per voi, una ragionevole aspettativa di riservatezza? Cambia, con la tecnologia? Come?
2. La Corte Suprema ha ritenuto che l’uso dello strumento di rilevazione termica fosse equivalente ad una perquisizione? Su quali basi?
3. Siete d’accordo con l’interpretazione della Corte?
4. Il fatto che tale strumento non fosse di uso comune è rilevante? Se sì, in che senso?
5. Ritenete che quelli rilevati attraverso lo strumento di rilevazione termica fossero “dettagli intimi”? Erano rilevati all’interno o all’esterno dell’abitazione?
6. Quale è il bilanciamento che viene individuato in questo caso tra diritti di libertà personale ed esigenze di protezione sociale?
7. Secondo voi, la decisione sarebbe la stessa, oggi?
8. Il caso non riguarda Internet: perché ne parliamo in questo corso?

*****

NORME

- Quarto Emendamento, Costituzione degli Stati Uniti
1.2. Luoghi reali, luoghi virtuali, cyberspace

United States Court of Appeals, 11th Circuit, 21 September 2001, n.00-16346 (Voyeur Dorm v. City of Tampa)

[...] This appeal arises from Voyeur Dorm L.C.'s ("Voyeur Dorm") alleged violation of Tampa's City Code based on the District Court's characterization of Voyeur Dorm as an adult entertainment facility. Because we conclude the District Court misapplied Tampa's City Code because it erroneously found that Voyeur Dorm offered adult entertainment to the public at the residence in question, we reverse the judgment of the District Court.

I. Background

As alleged in its complaint, Voyeur Dorm is a Florida limited liability company that maintains offices and conducts its business in Hillsborough County, Florida. Voyeur Dorm operates an Internet based website that provides a 24-hour a day Internet transmission portraying the lives of the residents of 2312 West Farwell Drive, Tampa, Florida. Throughout its existence, Voyeur Dorm has employed 25 to 30 different women, most of whom entered into a contract that specifies, among other things, that they are "employees," on a "stage and filming location," with "no reasonable expectation of privacy," for "entertainment purposes". Subscribers to "voyeurdorm.com" pay a subscription fee of $34.95 a month to watch the women employed at the premises and pay an added fee of $16.00 per month to "chat" with the women. From August 1998 to June 2000, Voyeur Dorm generated subscriptions and sales totaling $3,166,551.35.

In 1998, Voyeur Dorm learned that local law enforcement agencies had initiated an investigation into its business. In response, counsel for Voyeur Dorm sent a letter to Tampa's Zoning Coordinator requesting her interpretation of the City Code as it applied to the activities occurring at 2312 West Farwell Drive. In February of 1999, Tampa's Zoning Coordinator, Gloria Moreda, replied to counsel's request and issued her interpretation of the City Code, concluding in relevant part:
«The following generally describes the activities occurring on the property:
1. 5 unrelated women are residing on the premises.
2. 30 Internet cameras are located in various rooms in the house; such as the bedrooms, bathrooms, living rooms, shower and kitchen.
3. For a fee, Internet viewers are able to monitor the activities in the different rooms.
4. The web page address is http://www.voyeurdorm.com/
5. The web page shows various scenes from the house, including a woman with exposed buttocks. Statements on the page describe activities that can be viewed such as "The girls of Voyeur Dorm are fresh, naturally erotic and as young as 18. Catch them in the most intimate acts of youthful indiscretion".

The web page can be found by going to Yahoo! and entering “Voyeurdorm” on the search. The name of the website is, itself, advertising the adult nature of the entertainment. Voyeur is defined in the American Heritage Dictionary, Second College Edition as "A person who derives sexual gratification from observing the sex organs or sexual acts of others, especially from a secret vantage point".

It is my determination that the use occurring at 2312 W. Farwell Dr., as described in your letter, is an adult use. [...] Please be aware that the property is zoned RS-60 Residential Single Family, and an adult use business is not permitted use. You should advise your client to cease operation at that location.»

Thereafter, in April of 1999, Dan and Sharon Gold Marshlack appealed the Zoning Coordinator's decision to Tampa's Variance Review Board. On or about July 13, 1999, the Variance Review Board conducted a hearing. At the hearing, Voyeur Dorm's counsel conceded the following: that five women live in the house; that there are cameras in the corners of all the rooms of the house; that for a fee a person can join a membership to a website wherein a member can view the women 24 hours a day, seven days a week; that a member, at times, can see someone disrobed; that the women receive free room and board; that the women are part of a business
enterprise; and that the women are paid. At the conclusion of the hearing, the Variance Review Board unanimously upheld the Zoning Coordinator's determination that the use occurring at 2312 West Farwell Drive was an adult use. Subsequently, Mr. and Mrs. Marshlack filed an appeal from the decision of the Variance Review Board to the City Council. The Tampa City Council held a hearing in August of 1999, at the conclusion of which the City Council unanimously affirmed the decision of the Variance Review Board.

Voyeur Dorm filed this action in the middle district of Florida. The City of Tampa and Voyeur Dorm then filed cross-motions for summary judgment. The District Court granted Tampa's motion for summary judgment, from which Voyeur Dorm now appeals.

II. Issues

1. Whether the District Court properly determined that the alleged activities occurring at 2312 West Farwell Drive constitute a public offering of adult entertainment as contemplated by Tampa's zoning restrictions.

3. Whether the predicate evidence that Tampa relied upon to adopt its adult use restrictions must contemplate Internet forms of communication in order to restrict Internet forms of communication.

IV. Discussion

The threshold inquiry is whether section 27-523 of Tampa's City Code applies to the alleged activities occurring at 2312 West Farwell Drive. Because of the way we answer that inquiry, it will not be necessary for us to analyze the thorny constitutional issues presented in this case.

Section 27-523 defines adult entertainment establishments as:

"Any premises, except those businesses otherwise defined in this chapter, on which is offered to members of the public or any person, for a consideration, entertainment featuring or in any way including specified sexual activities, as defined in this section, or entertainment featuring the displaying or depicting of specified anatomical areas, as defined in this section; "entertainment" as used in this definition shall include, but not be limited to, books, magazines, films, newspapers, photographs, paintings, drawings, sketches or other publications or graphic media, filmed or live plays, dances or other performances either by single individuals or groups, distinguished by their display or depiction of specified anatomical areas or specified sexual activities, as defined in this section."

Tampa argues that Voyeur Dorm is an adult use business pursuant to the express and unambiguous language of Section 27-523 and, as such, cannot operate in a residential neighborhood. In that regard, Tampa points out: that members of the public pay to watch women employed on the premises; that the Employment Agreement refers to the premises as "a stage and filming location;" that certain anatomical areas and sexual activities are displayed for entertainment; and that the entertainers are paid accordingly. Most importantly, Tampa asserts that nothing in the City Code limits its applicability to premises where the adult entertainment is actually consumed.

In accord with Tampa's arguments, the District Court specifically determined that the "plain and unambiguous language of the Code ... does not expressly state a requirement that the members of the public paying consideration be on the premises viewing the adult entertainment" (Voyeur Dorm, L.C., et al., v. City of Tampa, n.99-2180 [...]). While the public does not congregate to a specific edifice or location in order to enjoy the entertainment provided by Voyeur Dorm, the District Court found 2312 West Farwell Drive to be "a premises on which is offered to members of the public for consideration entertainment featuring specified sexual activities within the plain meaning of the City Code", [...].

Moreover, the District Court relied on Supreme Court and Eleventh Circuit precedent that trumpets a city's entitlement to protect and improve the quality of residential neighborhoods. See City of Renton v. Playtime Theatres, Inc. [...] ("A city's interest in attempting to preserve the quality of urban life is one that must be accorded high respect") (quoting Young v. American Mini Theatres, Inc. [...]}; Sammy's of Mobile, Ltd. v. City of Mobile [...] (noting that it is well established that the regulation of public health, safety and morals is a valid and substantial state interest); Corn v. City of Lauderdale Lakes [...] (noting that the "Supreme Court has held that restrictions may be imposed to protect family values, youth values and the blessings of quiet seclusion" [...].
In opposition, Voyeur Dorm argues that it is not an adult use business. Specifically, Voyeur Dorm contends that section 27-523 applies to locations or premises wherein adult entertainment is actually offered to the public. Because the public does not, indeed cannot, physically attend 2312 West Farwell Drive to enjoy the adult entertainment, 2312 West Farwell Drive does not fall within the purview of Tampa's zoning ordinance. We agree with this argument.

The residence of 2312 West Farwell Drive provides no "offering of adult entertainment to members of the public". The offering occurs when the videotaped images are dispersed over the Internet and into the public eye for consumption. The City Code cannot be applied to a location that does not, itself, offer adult entertainment to the public. As a practical matter, zoning restrictions are indelibly anchored in particular geographic locations. Residential areas are often cordoned off from business districts in order to promote a State's interest. See e.g., City of Renton […] ("A city's interest in attempting to preserve the quality of urban life is one that must be accorded high respect"). It does not follow, then, that a zoning ordinance designed to restrict facilities that offer adult entertainment can be applied to a particular location that does not, at that location, offer adult entertainment. Moreover, the case law relied upon by Tampa and the District Court concern adult entertainment in which customers physically attend the premises wherein the entertainment is performed. Here, the audience or consumers of the adult entertainment do not go to 2312 West Farwell Drive or congregate anywhere else in Tampa to enjoy the entertainment. Indeed, the public offering occurs over the Internet in "virtual space". While the District Court read Section 27-523 in a literal sense, finding no requirement that the paying public be on the premises, we hold that section 27-523 does not apply to a residence at which there is no public offering of adult entertainment. Accordingly, because the District Court misapplied section 27-523 to the residence of 2312 West Farwell Drive, we reverse the District Court's order granting summary judgment to Tampa. Since the resolution of this threshold issue obviates the need for further analysis, we do not reach the remaining issues regarding the constitutionality of Tampa's zoning restrictions as applied to Voyeur Dorm.

Reversed
[…]

*****

**DISCUSSIONE**

1. Voyeur Dorm può essere considerato un “adult use business”? Se sì, perché non dovrebbe essere soggetto alle norme urbanistiche di Tampa?
2. Dove si svolge l’attività di intrattenimento per adulti? A Tampa, nelle case degli abbonati, in Internet, nel cyberspace?
3. Internet e cyberspace sono secondo voi sinonimi? Cosa intende la Corte d’appello per “virtual space”?
4. Esiste, secondo voi, un cyberspace? Se sì, come lo definireste?
1.3. Access to a Internet

Supreme Court of the United States, 19 June 2017, n.15-1194 (Packingham v. North Carolina) [syllabus]

[...] North Carolina law makes it a felony for a registered sex offender “to access a commercial social networking Web site where the sex offender knows that the site permits minor children to become members or to create or maintain personal Web pages”. N.C. Gen. Stat. Ann. §§14-202.5(a), (e). According to sources cited to the Court, the State has prosecuted over 1,000 people for violating this law, including petitioner, who was indicted after posting a statement on his personal Facebook profile about a positive experience in traffic court. The trial court denied petitioner’s motion to dismiss the indictment on the ground that the law violated the First Amendment. He was convicted and given a suspended prison sentence. On appeal, the State Court of Appeals struck down §14–202.5 on First Amendment grounds, but the State Supreme Court reversed.

Held: The North Carolina statute impermissibly restricts lawful speech in violation of the First Amendment.

(a) A fundamental First Amendment principle is that all persons have access to places where they can speak and listen, and then, after reflection, speak and listen once more. Today, one of the most important places to exchange views is cyberspace, particularly social media, which offers “relatively unlimited, low-cost capacity for communication of all kinds”, Reno v. American Civil Liberties Union, 521 U.S. 844, 870, to users engaged in a wide array of protected First Amendment activity on any number of diverse topics. The Internet’s forces and directions are so new, so protean, and so far reaching that courts must be conscious that what they say today may be obsolete tomorrow. Here, in one of the first cases the Court has taken to address the relationship between the First Amendment and the modern Internet, the Court must exercise extreme caution before suggesting that the First Amendment provides scant protection for access to vast networks in that medium.

(b) This background informs the analysis of the statute at issue. Even assuming that the statute is content neutral and thus subject to intermediate scrutiny, the provision is not “narrowly tailored to serve a significant governmental interest”. McCullen v. Coakley, 573 U. S. ___., ___. Like other inventions heralded as advances in human progress, the Internet and social media will be exploited by the criminal mind. It is also clear that “sexual abuse of a child is a most serious crime and an act repugnant to the moral instincts of a decent people” Ashcroft v. Free Speech Coalition, 535 U. S. 234, 244, and that a legislature “may pass valid laws to protect children” and other sexual assault victims, id., at 245. However, the assertion of a valid governmental interest “cannot, in every context, be insulated from all constitutional protections”. Stanley v. Georgia, 394 U. S. 557, 563.

Two assumptions are made in resolving this case. First, while the Court need not decide the statute’s precise scope, it is enough to assume that the law applies to commonplace social networking sites like Facebook, LinkedIn, and Twitter. Second, the Court assumes that the First Amendment permits a State to enact specific, narrowly-tailored laws that prohibit a sex offender from engaging in conduct that often presages a sexual crime, like contacting a minor or using a website to gather information about a minor.

Even with these assumptions, the statute here enacts a prohibition unprecedented in the scope of First Amendment speech it burdens. Social media allows users to gain access to information and communicate with one another on any subject that might come to mind.

With one broad stroke, North Carolina bars access to what for many are the principal sources for knowing current events, checking ads for employment, speaking and listening in the modern public square, and otherwise exploring the vast realms of human thought and knowledge. Foreclosing access to social media altogether thus prevents users from engaging in the legitimate exercise of First Amendment rights. Even convicted criminals - and in some instances especially convicted criminals - might receive legitimate benefits from these means for access to the world of ideas, particularly if they seek to reform and to pursue lawful and rewarding lives.
(c) The State has not met its burden to show that this sweeping law is necessary or legitimate to serve its purpose of keeping convicted sex offenders away from vulnerable victims. No case or holding of this Court has approved of a statute as broad in its reach. The State relies on Burson v. Freeman, 504 U. S. 191, but that case considered a more limited restriction - prohibiting campaigning within 100 feet of a polling place - in order to protect the fundamental right to vote.

The Court noted, moreover, that a larger buffer zone could “become an impermissible burden” under the First Amendment. Id., at 210. The better analogy is Board of Airport Comm’rs of Los Angeles v. Jews for Jesus, Inc., 482 U. S. 569. If an ordinance prohibiting any “First Amendment activities” at a single Los Angeles airport could be struck down because it covered all manner of protected, nondisruptive behavior, including “talking and reading, or the wearing of campaign buttons or symbolic clothing”, id., at 571, 575, it follows with even greater force that the State may not enact this complete bar to the exercise of First Amendment rights on websites integral to the fabric of modern society and culture.

368 N. C. 380, 777 S. E. 2d 738, reversed and remanded.

[...]

**DISCUSSIONE**

1. Quale è, secondo la Corte, il rapporto tra Primo Emendamento e cyberspace (in particolare, social media)?
2. Quale è, secondo la Corte il ruolo dei social media nella società moderna? A quali funzioni possono adempiere?
3. Cosa, secondo la Corte, lo Stato della North Carolina non ha provato, per rendere legitima la restrizione?
4. A quali precedenti fa riferimento la Corte per giustificare la propria decisione?
5. Siete d'accordo con la Corte nel giudicare eccessivo il divieto di accesso alla Rete per soggetti che hanno commesso in passato reati a sfondo sessuale?

****

**NORME**

- Primo Emendamento, Costituzione degli Stati Uniti
2. INTERNET E GIURISDIZIONE
2.1. Giurisdizione e valori

Tribunal de Grande Instance de Paris, ordonnance 22 mai 2000 (LICRA v. Yahoo)
(traduzione non ufficiale di Nicola Lugaresi)

[...]

Avendo constatato e fatto constatare da ufficiale giudiziario che sul sito Yahoo.com, accessibile a tutti i navigatori che si connettono dalla Francia, appare una pagina “AUCTIONS” (aste) che propone la vendita di numerosi oggetti nazisti e considerando che questa esposizione di oggetti offerti in vendita costituisca non solamente una violazione delle disposizioni dell'art.R.645-1 c.p., ma anche la più grande iniziativa di banalizzazione del nazismo possibile, la Ligue Internationale contre le racisme et l'antisémitisme (LICRA), il cui oggetto sociale è in particolare quello di combattere con tutti i mezzi il razzismo e l'antisemitismo [...] e di difendere l'onore e la memoria dei deportati, chiede di ordinare alla società Yahoo! Inc., proprietaria di Yahoo.com, di adottare le misure necessarie per impedire l'esposizione e la vendita attraverso il suo sito Yahoo.com di oggetti nazisti su tutto il territorio francese (procedimento n.00/05308);

L'Unione degli Studenti Ebrei di Francia, che ha appoggiato la richiesta di LICRA e che contesta inoltre a Yahoo! Inc. e a Yahoo France di favorire la diffusione dell'anti-semitismo, in primo luogo ospitando su suo servizio Geocities.com due monumenti della letteratura contemporanea antisemita, il Mein Kampf di Adolf Hitler e i Protocolli dei Savì di Sion (celebre documento falso che intendeva stabilire la corruzione ebraica e il relativo piano di dominio), in secondo luogo fornendo un link attraverso Yahoo.com alle pagine dove si offre il servizio d'aste, in aggiunta ad una rubrica "revisionisti", a partire dalla quale ci si può consultare un sito intitolato "Air photo evidence", che si propone di dimostrare con le immagini l'inesistenza delle camere a gas, chiede di (procedimento n.00/05309):

[...]

1. Ordinare a Yahoo! Inc. [...] di distruggere tutti i dati informatici immagazzinati, direttamente o indirettamente, sul suo server e interrompere correttivamente qualsiasi archiviazione e qualsiasi messa a disposizione nel territorio della Repubblica a partire dal sito "Yahoo.com":
   - di messaggi, immagini e testi relativi a oggetti, cimeli, stemmi ed emblemi e bandiere naziste o che evocchino il nazismo e possano essere acquistati sul servizio "Aste"
   - di pagine web che espongano testi, estratti o citazioni dal Mein Kampf e dai Protocolli dei Savì di Sion, che possano essere visualizzati, riprodotti o scaricati dal servizio hosting Geocities di Yahoo! Inc., presso i seguenti indirizzi:
     - "www.geocities.com/SouthBeach(...)748/mk.html"
     - "www.geocities.com/Athena/Thebes/(...)otocol1tot8.htm"

2. Ordinare a Yahoo! Inc. e Yahoo France [...] di eliminare, in ogni directory di navigazione accessibile sul territorio della Repubblica francese, da siti Yahoo.com e Yahoo.fr:
   - la rubrica di indicizzazione intitolata "negazionisti";
   - tutti gli hyperlinks che uniscono, assimilano o si presentano, direttamente o indirettamente, come equivalenti ai siti indicizzati sotto la voce "holocausto" e quelli classificati come negazionisti [...].

Considerando che non è contestato che l'utente che si collega a Yahoo.com dal territorio francese, direttamente o attraverso il link proposto da Yahoo.fr; possa visualizzare sul proprio schermo le pagine, i servizi e i siti ai quali Yahoo.com consente l'accesso, in particolare il servizio di aste, ospitato presso Geocities.com, servizio di hosting di Yahoo! Inc., compresa la parte specifica relativa ai cimeli nazisti.

Considerando che l'esposizione per la vendita di cimeli nazisti costituisce una violazione del diritto francese (art.R. 645-2 c.p.), ma prima ancora un'offesa alla memoria collettiva del Paese profondamente segnato dalle atrocità commesse dalla, e per conto della, organizzazione criminale nazista contro i suoi cittadini residenti ed in particolare contro i suoi cittadini di religione ebraica;

Considerando che con il permettere la visualizzazione in Francia di questi oggetti e la partecipazione eventuale di un utente residente in Francia ad una tale esposizione o vendita, Yahoo! Inc. commette quindi un illecito, il cui carattere non interzionale è evidente, ma che ha
causato un danno sia per la LICRA che per l'Unione degli Studenti Ebrei di Francia, che hanno come scopo di contrastare in Francia qualsiasi forma di banalizzazione del nazismo, a prescindere dal carattere residuale dell'attività contestata rispetto all'insieme del servizio di aste offerto sul sito Yahoo.com;

Considerando che, essendo i danni subiti in Francia, la nostra giurisdizione è quindi competente per conoscere la presente controversia ai sensi dell'art.46 del Nuovo Codice di Procedura Civile;

Considerando che Yahoo! Inc. sostiene che è tecnicamente impossibile controllare l'accesso al suo servizio di aste o ad altri servizi e, di conseguenza, impedire a un utente che si connette dalla Francia di visualizzare tali pagine sul proprio schermo;

Considerando che Yahoo! Inc. desidera tuttavia precisare che mette in guardia tutti i visitatori contro qualsiasi utilizzazione di questi servizi per scopi "degni di disapprovazione per qualsiasi motivo", in particolare a fini di discriminazione razziale o etnica (v. Condizioni di utilizzo);

Ma considerato che Yahoo! Inc. è in grado di identificare l'origine geografica del sito che si collega allo stesso, attraverso l'indirizzo IP dell'utente, il che dovrebbe permettergli di impedire agli utenti collegati dalla Francia, con tutti i mezzi appropriati, di accedere ai servizi e siti la cui visualizzazione su uno schermo localizzato in Francia, seguita eventualmente da download e riproduzione di contenuti, o da qualsiasi altra iniziativa giustificata dalla natura del sito consultato, sia suscettibile di ricevere in Francia una connotazione di carattere penale e/o di costituire un'attività manifestamente illecita ai sensi degli artt.808 e 809 del Nuovo Codice di Procedura Civile, che è chiaramente il caso dell'esibizione di uniformi, stemmi, emblemi che ricordino quelli portati o esibiti dai nazisti;

Considerando che per quanto riguarda gli utenti che transitano attraverso siti che garantiscono loro l'anonimato, Yahoo! Inc. ha minori possibilità di controllo eccetto, per esempio, quella di rifiutare sistematicamente l'accesso a qualsiasi visitatore che non rivelì la sua origine geografica;

Considerando che, quindi, le difficoltà reali incontrate da Yahoo non costituiscono ostacoli insormontabili; che sarà quindi ordinato di adottare tutte le misure idonee a dissuadere e a rendere impossibile ogni accesso di un utente che si collega dalla Francia a siti e servizi contestati, il cui titolo e/o contenuto possano nuocere all'ordine pubblico interno, ed in particolare al sito di vendita di cimeli nazisti;

Considerando che deve poter essere utilmente discussa la natura di queste misure nel quadro del presente procedimento; che un periodo di due mesi sarà quindi concesso a Yahoo per permettere di formulare proposte di misure tecniche suscettibili di favorire la composizione della presente controversia;

Considerando che, per quanto riguarda Yahoo France, occorre precisare che il sito Yahoo.fr non offre direttamente agli utenti che si collegano dalla Francia l'accesso a siti e servizi il cui sito e/o contenuto costituiscano una violazione alla legge francese; che quindi, non permette l'accesso a siti o servizi di vendita all'asta di cimeli nazisti;

Ma considerando che, di fronte all'utente che fornisce un link a Yahoo.com intitolato "ulteriori ricerche su Yahoo.com", senza particolari precauzioni;

O, considerando che, conoscendo il contenuto dei servizi offerti da Yahoo.com, e nella fattispecie il servizio di vendita all'asta comprensivo la vendita di cimeli nazisti, è tenuto a comunicare all'utente, attraverso un avviso, ancor prima che l'utente continui la sua ricerca su Yahoo.com; che qualora il risultato della sua ricerca su Yahoo.com, sia attraverso link successivi, sia attraverso parole chiave lo conduca a siti, pagine o forum, il cui titolo e/o dei contenuti costituiscano una violazione del diritto francese, quali siti che facciano, direttamente o indirettamente, intenzionalmente o meno, apologia del nazismo, deve interrompere la consultazione del sito in questione per non incorrere nelle sanzioni previste dalla legislazione francese o rispondere alle azioni giudiziarie che potrebbero essere promosse contro di lui;

Considerando che queste misure risultano allo stato adeguate [...].

P.Q.M.

[...]

Ordiniamo a Yahoo! Inc. di adottare tutte le misure idonee a dissuadere e rendere impossibile qualsiasi accesso tramite Yahoo.com al servizio di aste di cimeli nazisti e a qualsiasi altro sito o servizio che costituisca un'apologia del nazismo o neghi i crimini nazisti;
Ordiniamo a Yahoo France di avvertire qualsiasi utente che consulti Yahoo.fr, e prima che faccia uso del link che gli consenta di continuare le ricerche su Yahoo.com, che, se il risultato delle ricerche, sia attraverso link successivi, sia attraverso parole chiave, lo indirizzi verso siti, pagine o forum il cui titolo e/o i cui contenuti costituiscano una violazione del diritto francese, così come la consultazione di siti che facciano apologia del nazismo e/o esibiscano uniformi, stemmi, emblemi che ricordino quelli che sono stati portati o esposti dai nazisti, o mettano in vendita oggetti o opere la cui vendita è strettamente proibita in Francia, deve interrompere la consultazione del sito in questione per non incorrere nelle sanzioni previste dalla legislazione francese o rispondere alle azioni giudiziarie che potrebbero essere promosse contro di lui;

Ordiniamo la prosecuzione del procedimento all’udienza di lunedì 24 luglio 2000 [...] in cui Yahoo! Inc. presenterà le misure che intende adottare per porre fine ai danni ed alle sofferenze subiti dai ricorrenti e per prevenire ogni ulteriore problema.

[...]  

*****  

DISCUSSIONE  

1. Quali sono le differenze tra modello francese e modello statunitense, in relazione all’esposizione di cimeli e simboli nazisti? Quale vi piace di più? Perché?

2. Quali sono gli strumenti individuati dal Tribunale per evitare la violazione della legge francese? Sono efficaci, secondo voi? Quali alternative erano possibili?

3. Quali conseguenze può avere, in relazione allo sviluppo della Rete, l’adozione di misure analoghe a quelle previste nella sentenza in oggetto?

4. Quali possono essere i limiti di effettività di questa sentenza?

5. Perché, secondo voi, Yahoo si è adeguata alla decisione di un tribunale straniero?
2.2. Trasferimento di dati e livello di tutela in altra giurisdizione

Corte di Giustizia dell'Unione Europea, 6 ottobre 2015 (causa C-362/14)


2. Tale domanda è stata presentata nell’ambito di una controversia fra il sig. Schrems e il Data Protection Commissioner (commissario per la protezione dei dati; in prosieguo: il «commissario») concernente il rifiuto, da parte di quest’ultimo, di istituire una denuncia presentata dal sig. Schrems per il fatto che Facebook Ireland Ltd (in prosieguo: «Facebook Ireland») trasferisce negli Stati Uniti i dati personali dei propri utenti e li conserva su server ubicati in tale paese.

 [...] 

Procedimento principale e questioni pregiudiziali


27. Chiunque risieda nel territorio dell’Unione e desideri utilizzare Facebook è tenuto, a momento della sua iscrizione, a sottoscrivere un contratto con Facebook Ireland, una controllata di Facebook Inc., situata, da parte sua, negli Stati Uniti. I dati personali degli utenti di Facebook residenti nel territorio dell’Unione vengono trasferiti, in tutto o in parte, su server di Facebook Inc. ubicati nel territorio degli Stati Uniti, ove essi sono oggetto di un trattamento.

28. Il 25 giugno 2013 il sig. Schrems ha investito il commissario di una denuncia, con la quale lo invitava, in sostanza, ad esercitare le proprie competenze statutarie, vietando a Facebook Ireland di trasferire i suoi dati personali verso gli Stati Uniti. In tale denuncia egli faceva valere che il diritto e la prassi vigenti in tale paese non offrivano una protezione sufficiente dei dati personali conservati nel territorio del medesimo contro le attività di controllo ivi praticate dalle autorità pubbliche. Il sig. Schrems si riferiva, a tal riguardo, alle rivelazioni fatte dal sig. Edward Snowden in merito alle attività dei servizi di intelligence degli Stati Uniti, e in particolare a quello della National Security Agency (in prosieguo: la «NSA»).

29. Considerando di non essere obbligato a procedere ad un’indagine sui fatti denunciati dal sig. Schrems, il commissario ha respinto la denuncia in quanto priva di fondamento. Egli ha ritenuto, infatti, che non esistessero prove del fatto che la NSA avesse avuto accesso ai dati personali dell’interessato. Il commissario ha aggiunto che le censure formulate dal sig. Schrems nella sua denuncia non potevano essere fatte valere in maniera utile, in quanto ogni questione relativa all’adeguatezza della protezione dei dati personali negli Stati Uniti doveva essere risolta in conformità alla decisione 2000/520 e che, in tale decisione, la Commissione aveva constatato che gli Stati Uniti d’America assicuravano un livello di protezione adeguato.

30. Il sig. Schrems ha proposto un ricorso dinanzi alla High Court (Corte d’appello) avverso la decisione di cui al procedimento principale. Dopo aver esaminato le prove prodotte dalle parti nel procedimento principale, tale giudice ha dichiarato che la sorveglianza elettronica e l’intercettazione dei dati personali trasferiti dall’Unione verso gli Stati Uniti rispondevano a finalità necessarie e indispensabili per l’interesse pubblico. Tuttavia, detto giudice ha aggiunto che le rivelazioni del sig. Snowden avevano dimostrato che la NSA ed altri organi federali avevano commesso «eccessi considerevoli».

31. Orbene, secondo questo stesso giudice, i cittadini dell’Unione non avrebbero alcun diritto effettivo ad essere sentiti. La supervisione sull’operato dei servizi di intelligence verrebbe effettuata nell’ambito di un procedimento segreto e non contraddittorio. Una volta che i dati personali sono stati trasferiti verso gli Stati Uniti, la NSA e altri organi federali, come il Federal Bureau of
Irgendwessen, die **High Court** (Oberster Gerichtshof) hat festgestellt, dass das irische Recht den Transfer von persönlichen Daten von außerhalb des nationalen Territoriums, in dem die Faktenlagen befanden, verhindern würde; dies beruht auf der Annahme, dass ein solcher Transfer einer gewissen Form von Verletzung des Charakters des Lebensraumes anheimfallen würde. L'importanza dei diritti al rispetto della vita privata e al diritto alla sicurezza del domicilio, garantiti dalla Costituzione irlandese, implica che qualsiasi ingenua in tali diritti sia proporzionata e conforme ai requisiti previsti dalla legge.

33. Orbene, l’accesso massiccio e indifferenziato a dati personali sarebbe manifestamente contrario al principio di proporzionalità e ai valori fondamentali protetti dalla Costituzione irlandese. Affinché intercettazioni di comunicazioni elettroniche possano essere considerate conformi a tale Costituzione, occorrerebbe dimostrare che tali intercettazioni sono mirate, che la sorveglianza su talune persone o taluni gruppi di persone è oggettivamente giustificata nell’interesse della sicurezza nazionale o della repressione della criminalità, e che esistono garanzie adeguate e verificabili. Pertanto, secondo la **High Court** (Oberster Gerichtshof), qualora il procedimento principale dovesse essere definito sulla base del solo diritto irlandese, occorrerebbe constatare che, alla luce dell'esistenza di un serio dubbio sul fatto che gli Stati Uniti d’America assicurino un livello di protezione adeguato ai dati personali, il commissario avrebbe dovuto compiere un’indagine sui fatti lamentati dal sig. Schrems nella sua denuncia e che il commissario ha erroneamente respinto quest’ultima.

34. Tuttavia, la **High Court** (Oberster Gerichtshof) considera che tale causa verte sull’attuazione del diritto dell’Unione ai sensi dell’art.51 della Carta, cosicché la legittimità della decisione di cui al procedimento principale deve essere valutata sulla scorta del diritto dell’Unione. Orbene, secondo tale giudice, la decisione 2000/520 non soddisfa i requisiti risultanti sia dagli artt.7 e 8 della Carta sia dai principi enunciati dalla Corte nell’sentenza Digital Rights Ireland e a. (C-293/12 e C-594/12, […]). Il diritto al rispetto della vita privata, garantito dall’art.7 della Carta e dai valori fondamentali comuni alle tradizioni degli Stati membri, sarebbe svuotato di significato qualora i pubblici poteri fossero autorizzati ad accedere alle comunicazioni elettroniche su base casuale e generalizzata, senza alcuna giustificazione oggettiva fondata su motivi di sicurezza nazionale o di prevenzione della criminalità, specificamente riguardanti i singoli interessati, e senza che tali pratiche siano accompagnate da garanzie adeguate e verificabili.

35. La **High Court** (Oberster Gerichtshof) osserva, inoltre, che il sig. Schrems, nel suo ricorso, ha contestato in realtà la legittimità del regime dell’approdo sicuro istituito dalla decisione 2000/520 e sul quale poggia la decisione di cui al procedimento principale, ma non ha formalmente contestato la validità né della direttiva 95/46 né della decisione 2000/520, secondo tale giudice occorre chiarire se, avuto riguardo all’art.25, §6, di tale direttiva, il commissario fosse vincolato dalla constatazione effettuata dalla Commissione in tale decisione, secondo la quale gli Stati Uniti d’America garantiscono un livello di protezione adeguato, oppure se l’art.8 della Carta autorizzasse il commissario a discostarsi, se del caso, da una siffatta constatazione.

36. È in tale contesto che la **High Court** (Oberster Gerichtshof) ha deciso di sospendere il procedimento e di sottoporre alla Corte le seguenti questioni pregiudiziali:

1) Se, nel decidere in merito a una denuncia presentata a un’autorità indipendente investita per legge delle funzioni di gestione e di applicazione della legislazione sulla protezione dei dati, secondo cui i dati personali sono trasferiti a un paese terzo (nel caso di specie, gli Stati Uniti d’America) il cui diritto e la cui prassi si sostiene non prevedano adeguate tutele per i soggetti interessati, tale autorità sia assolutamente vincolata dalla constatazione in senso contrario dell’Unione contenuta nella decisione 2000/520, tenuto conto degli artt.7, 8 e 47 della Carta, nonostante le disposizioni dell’art.25, §6, della direttiva 95/46.

2) Oppure, in alternativa, se detta autorità possa e/o debba condurre una propria indagine sulla questione alla luce degli sviluppi verificatisi nel frattempo, successivamente alla prima pubblicazione della decisione 2000/520».

**Sulle questioni pregiudiziali**

37. Con le sue questioni pregiudiziali, che occorre esaminare congiuntamente, il giudice del rinvio chiede, in sostanza, se e in che misura l’art.25, §6, della direttiva 95/46, letto alla luce degli artt.7, 8 e 47 della Carta, debba essere interpretato nel senso che una decisione adottata in forza di tale disposizione, come la decisione 2000/520, con la quale la Commissione constata che un
paese terzo assicura un livello di protezione adeguato, osti a che un’autorità di controllo di uno Stato membro, ai sensi dell’art.28 di tale direttiva, possa esaminare la domanda di una persona relativa alla tutela dei suoi diritti e delle sue libertà con riguardo al trattamento di dati personali che la riguardano, i quali sono stati trasferiti da uno Stato membro verso tale paese terzo, allorché tale persona faccia valere che il diritto e la prassi in vigore in quest’ultimo non assicurano un livello di protezione adeguato.

Sui poteri delle autorità nazionali di controllo ai sensi dell’art.28 della direttiva 95/46, in presenza di una decisione della Commissione adottata in forza dell’art.25, §6, di tale direttiva

38. Occorre rammentare, in via preliminare, che le disposizioni della direttiva 95/46, disciplinando il trattamento di dati personali che possono arrecare pregiudizio alle libertà fondamentali e, segnatamente, al diritto al rispetto della vita privata, devono essere necessariamente interpretate alla luce dei diritti fondamentali garantiti dalla Carta (v. sentenze Österreichischer Rundfunk e a., C-465/00, C-138/01 e C-139/01, […], p.to 68; Google Spain e Google, C-131/12, […], p.to 68, nonché Ryneš, C-212/13, […], 28, p.to 29).

39. Risulta dall’art.1, nonché dai considerando 2 e 10 della direttiva 95/46, che essa è intesa a garantire non solo una tutela efficace e completa delle libertà e dei diritti fondamentali delle persone fisiche, e segnatamente del diritto fondamentale al rispetto della vita privata con riguardo al trattamento dei dati personali, ma anche un livello elevato di protezione di tali libertà e diritti fondamentali. L’importanza sia del diritto fondamentale al rispetto della vita privata, garantito dall’art.7 della Carta, sia del diritto fondamentale alla tutela dei dati personali, garantito dall’art.8 della stessa, è inoltre sottolineata nella giurisprudenza della Corte (v. sentenze Rijkeboer, C-553/07, […], p.to 47; Digital Rights Ireland e a., C-293/12 e C-594/12, […], p.to 53, nonché Google Spain e Google, C-131/12, […], p.ti 53, 66 e 74 e la giurisprudenza ivi citata).

40. Per quanto attiene ai poteri di cui dispongono le autorità di controllo nazionali quanto al trasferimento di dati personali verso paesi terzi, si deve rilevare che l’art.28, §1, della direttiva 95/46 obbliga gli Stati membri ad istituire una o più autorità pubbliche incaricate di controllare in piena indipendenza l’osservanza delle norme dell’Unione relative alla tutela delle persone con riguardo al trattamento di tali dati. Detto obbligo risulta altresì dal diritto primario dell’Unione, segnatamente dall’art.8, §3, della Carta e dall’art.16, §2, TFUE (v., in tal senso, sentenze Commissione/Austria, C-614/10, […], p.to 36, e Commissione/Ungheria, C-288/12, […], p.to 47).

41. La garanzia d’indipendenza delle autorità nazionali di controllo è diretta ad assicurare che il controllo del rispetto delle disposizioni in materia di protezione delle persone fisiche con riguardo al trattamento dei dati sia efficace e affidabile e deve essere interpretata alla luce di tale finalità. Essa è stata disposta al fine di rafforzare la protezione delle persone e degli organismi interessati dalle decisioni di tali autorità. L’inistituzione, negli Stati membri, di autorità di controllo indipendenti, costituisce quindi, come rilevato dal considerando 62 della direttiva 95/46, un elemento essenziale del rispetto della tutela delle persone con riguardo al trattamento dei dati personali (v. sentenze Commissione/Germania, C-518/07, […], p.to 25, nonché Commissione/Ungheria C288/12, […], p.to 48 e la giurisprudenza ivi citata).

42. Al fine di garantire tale protezione, le autorità nazionali di controllo devono, segnatamente, assicurare un giusto equilibrio fra, da un lato, il rispetto del diritto fondamentale alla vita privata e, dall’altro, gli interessi che impongono una libera circolazione dei dati personali (v., in tal senso, sentenze Commissione/Germania, C-518/07, […], p.to 24, e Commissione/Ungheria C-288/12, […], p.to 51).

43. A tal fine, dette autorità dispongono di un’ampia gamma di poteri e questi, elencati in maniera non esaustiva all’art.28, §3, della direttiva 95/46, costituiscono altrettanti mezzi necessari all’adempimento dei loro compiti, come sottolineato dal considerando 63 di tale direttiva. In tal senso, dette autorità godono, segnatamente, di poteri investigativi, come quello di raccogliere qualsiasi informazione necessaria all’esercizio della loro funzione di controllo, di poteri effettivi d’intervento, come quello di vietare a titolo provvisorio o definitivo un trattamento di dati o, ancora, del potere di promuovere azioni giudiziarie.

44. È vero che si evince dall’art.28, §§1 e 6, della direttiva 95/46 che i poteri delle autorità nazionali di controllo riguardano i trattamenti di dati personali effettuati nel territorio del loro Stato membro, cosicché esse non dispongono di poteri, sulla base di tale art.28, con riguardo ai trattamenti di siffatti dati effettuati nel territorio di un paese terzo.
45. Tuttavia, l’operazione consistente nel far trasferire dati personali da uno Stato membro verso un paese terzo costituisce, di per sé, un trattamento di dati personali ai sensi dell’art.2, lett.b), della direttiva 95/46 (v., in tal senso, sentenza Parlamento/Consiglio e Commissione, C-317/04 e C-318/04, […] p.to 56) effettuato nel territorio di uno Stato membro. Infatti, tale disposizione definisce il «trattamento di dati personali» alla stregua di «qualsiasi operazione o insieme di operazioni compiute con o senza l’ausilio di processi automatizzati e applicate a dati personali» e menziona, a titolo di esempio, «la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione».

46. Il considerando 60 della direttiva 95/46 precisa che i trasferimenti di dati personali verso i paesi terzi possono aver luogo soltanto nel pieno rispetto delle disposizioni prese dagli Stati membri in applicazione di tale direttiva. A tal riguardo, il capo IV di detta direttiva, nel quale figurano gli artt.25 e 26 della medesima, ha predisposto un regime che mira a garantire un controllo da parte degli Stati membri sui trasferimenti di dati personali verso i paesi terzi. Tale regime è complementare al regime generale attuato dal capo II di questa stessa direttiva, riguardante le condizioni generali di liceità dei trattamenti di dati personali (v., in tal senso, sentenza Lindqvist, C101/01, […] p.to 63).

47. Poiché le autorità nazionali di controllo sono incaricate, ai sensi dell’art.8, §3, della Carta e dell’art.28 della direttiva 95/46, di sorvegliare il rispetto delle norme dell’Unione relative alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, ciascuna di esse è quindi investita della competenza a verificare se un trasferimento di dati personali dal proprio Stato membro verso un paese terzo rispetti i requisiti fissati dalla direttiva 95/46.

48. Riconoscendo al contempo, al suo considerando 56, che i trasferimenti di dati personali dagli Stati membri verso paesi terzi sono necessari allo sviluppo degli scambi internazionali, la direttiva 95/46 pone come principio, al suo art.25, §1, che siffatti trasferimenti possano avere luogo soltanto se tali paesi terzi garantiscono un livello di protezione adeguato.

49. Inoltre, il considerando 57 di detta direttiva precisa che i trasferimenti di dati personali verso paesi terzi che non offrono un livello di protezione adeguato devono essere vietati.

50. Al fine di controllare i trasferimenti di dati personali verso i paesi terzi in funzione del livello di protezione ad essi accordato in ciascuno di tali paesi, l’art.25 della direttiva 95/46 impone una serie di obblighi agli Stati membri e alla Commissione. Risulta, segnatamente, da tale articolo, che la constatazione se un paese terzo assicuri o meno un livello di protezione adeguato può essere effettuata, come rilevato dall’avvocato generale al §86 delle sue conclusioni, vuoi dagli Stati membri vuoi dalla Commissione.

51. La Commissione può adottare, sulla base dell’art.25, §6, della direttiva 95/46, una decisione che constata che un paese terzo garantisce un livello di protezione adeguato. Conformemente al secondo comma di tale disposizione, una siffatta decisione ha come destinatari gli Stati membri, i quali devono adottare le misure necessarie per conformarvisi. Ai sensi dell’art.288, quarto comma, TFUE, essa ha un carattere vincolante per tutti gli Stati membri destinatari e si impone pertanto a tutti i loro organi (v., in tal senso, sentenze Albako Margarinefabrik, 249/85, […] p.to 17, e Mediaset, C-69/13, […] p.to 23), nella parte in cui produce l’effetto di autorizzare trasferimenti di dati personali dagli Stati membri verso il paese terzo da essa interessato.

52. Pertanto, fintantoché la decisione della Commissione non sia stata dichiarata invalida dalla Corte, gli Stati membri e i loro organi, fra i quali figurano le loro autorità di controllo indipendenti, non possono certo adottare misure contrarie a tale decisione, come atti intesi a constatare con effetto vincolante che il paese terzo interessato da detta decisione non garantisce un livello di protezione adeguato. Infatti, gli atti delle istituzioni dell’Unione si presumono, in linea di principio, legittimi e producono pertanto effetti giuridici, finché non siano stati revocati o annullati nel contesto di un ricorso per annullamento ovvero dichiarati invalidi a seguito di un rinvio pregiudiziale o di un’eccezione di illegittimità (sentenza Commissione/Grecia, C-475/01, […] p.to 18 e la giurisprudenza ivi citata).

53. Tuttavia, una decisione della Commissione adottata sulla base dell’art.25, §6, della direttiva 95/46, come la decisione 2000/520, non può impedire alle persone i cui dati personali sono stati o potrebbero essere trasferiti verso un paese terzo di investire le autorità nazionali di controllo di una domanda, ai sensi dell’art.28, §4, di tale direttiva, relativa alla protezione dei loro diritti e delle loro libertà con riguardo al trattamento di tali dati. Analogamente, una decisione di tale natura non può, come rilevato dall’avvocato generale, segnatamente, ai §§61, 93 e 116 delle sue
conclusioni, né elidere né ridurre i poteri espressamente riconosciuti alle autorità nazionali di controllo dall’art. 8, § 3, della Carta, nonché dall’art. 28 di detta direttiva.

54. Né l’art. 8, § 3, della Carta né l’art. 28 della direttiva 95/46 escludono dall’ambito di competenza delle autorità nazionali di controllo il controllo dei trasferimenti di dati personali verso paesi terzi che sono stati oggetto di una decisione della Commissione in forza dell’art. 25, § 6, di tale direttiva.

55. In particolare, l’art. 28, § 4, primo comma, della direttiva 95/46, il quale dispone che «[q]ualsiasi persona (…) può presentare [alle autorità nazionali di controllo] una domanda relativa alla tutela dei suoi diritti e libertà con riguardo al trattamento di dati personali», non prevede alcuna eccezione a tal riguardo nel caso in cui la Commissione abbia adottato una decisione in forza dell’art. 25, § 6, di tale direttiva.

56. Inoltre, sarebbe contrario al sistema predispotto dalla direttiva 95/46, nonché alla finalità degli artt. 25 e 28 della stessa se una decisione della Commissione adottata in applicazione dell’art. 25, § 6, di detta direttiva avesse come effetto di impedire ad un’autorità nazionale di controllo di esaminare la domanda di una persona relativa alla protezione dei suoi diritti e libertà con riguardo al trattamento dei suoi dati personali che sono stati o potrebbero essere trasferiti da uno Stato membro verso un paese terzo interessato da tale decisione.

57. Al contrario, l’art. 28 della direttiva 95/46 si applica, per la sua stessa natura, a ogni trattamento di dati personali. Pertanto, anche in presenza di una decisione della Commissione adottata sulla base dell’art. 25, § 6, di tale direttiva, le autorità nazionali di controllo investite da una persona di una domanda relativa alla protezione dei suoi diritti e libertà con riguardo al trattamento dei dati personali che la riguardano, devono poter verificare, in piena indipendenza, se il trasferimento di tali dati rispetti i requisiti fissati da detta direttiva.

58. Se così non fosse, le persone i cui dati personali sono stati o potrebbero essere trasferiti verso il paese terzo di cui trattasi sarebbero private del diritto, garantito all’art. 8, §§ 1 e 3, della Carta, di investire le autorità nazionali di controllo di una domanda ai fini della protezione dei loro diritti fondamentali (v., per analogia, sentenza Digital Rights Ireland e a., C-293/12 e C-594/12, […] p.to 68).

59. Una domanda, ai sensi dell’art. 28, § 4, della direttiva 95/46, con la quale una persona i cui dati personali sono stati o potrebbero essere trasferiti verso un paese terzo fa valere, come nel procedimento principale, che il diritto e la prassi di tale paese non assicurano, nonostante quanto constatato dalla Commissione in una decisione adottata in base all’art. 25, § 6, di tale direttiva, un livello di protezione adeguato, deve essere intesa nel senso che essa verte, in sostanza, sulla compatibilità di tale decisione con la protezione della vita privata e delle libertà e dei diritti fondamentali della persona.

60. A tal riguardo, occorre richiamare la giurisprudenza costante della Corte secondo la quale l’Unione è un’unione di diritto, nel senso che tutti gli atti delle sue istituzioni sono soggetti al controllo della conformità, segnatamente, ai Trattati, ai principi generali del diritto nonché ai diritti fondamentali (v., in tal senso, sentenze Commissione e a./Kadi, C-584/10 P, C-593/10 P e C-595/10 P, […] p.to 66; Inuit Tapiriit Kanatami e a./Parlamento e Consiglio, C-583/11 P, […] p.to 91, nonché Telefónica/Commissione, C-274/12 P, […] p.to 56). Le decisioni della Commissione adottate in forza dell’art. 25, § 6, della direttiva 95/46 non possono pertanto sfuggire ad un siffatto controllo.

61. Ciò premesso, la Corte è competente in via esclusiva a dichiarare l’invalidità di un atto dell’Unione, quale una decisione della Commissione adottata in applicazione dell’art. 25, § 6, della direttiva 95/46; la natura esclusiva di tale competenza ha lo scopo di garantire la certezza del diritto assicurando l’applicazione univoca del diritto dell’Unione (v. sentenze Melki e AbdeI, C-188/10 e C-189/10, […] p.to 54, nonché CIVAD, C-533/10, […] p.to 40).

62. Per quanto i giudici nazionali siano effettivamente legittimati ad esaminare la validità di un atto dell’Unione, come una decisione della Commissione adottata in forza dell’art. 25, § 6, della direttiva 95/46, essi non sono tuttavia competenti a constatare essi stessi l’invalidità di un siffatto atto (v., in tal senso, sentenze Foto-Frost, 314/85, […] punti da 15 a 20, nonché IATA e ELFAA, C-344/04, […] p.to 27). A fortiori, in sede di esame di una domanda, ai sensi dell’art. 28, § 4, di tale direttiva, avente ad oggetto la compatibilità di una decisione della Commissione adottata in forza dell’art. 25, § 6, di detta direttiva con la protezione della vita privata e delle libertà e dei diritti fondamentali della persona, le autorità nazionali di controllo non sono competenti a constatare esse stesse l’invalidità di una siffatta decisione.
63. Alla luce di tali considerazioni, qualora una persona i cui dati personali sono stati o potrebbero essere trasferiti verso un paese terzo che è stato oggetto di una decisione della Commissione in forza dell’art.25, §6, della direttiva 95/46, investa un’autorità nazionale di controllo di una domanda relativa alla protezione dei suoi diritti e libertà con riguardo al trattamento di tali dati e contesti, in occasione di tale domanda, come nel procedimento principale, la compatibilità di tale decisione con la protezione della vita privata e delle libertà e dei diritti fondamentali della persona, incombe a tale autorità esaminare detta domanda con tutta la diligenza richiesta.

64. Nel caso in cui detta autorità pervenga alla conclusione che gli elementi addotti a sostegno di una siffatta domanda sono privi di fondamento e, per questo motivo, la respinga, la persona che ha proposto detta domanda deve avere accesso, come si evince dall’art.28, §3, secondo comma, della direttiva 95/46, in combinato con l’art.47 della Carta, ai mezzi di ricorso giurisdizionali che le consentono di contestare una siffatta decisione impugnandola dinanzi ai giudici nazionali. Alla luce della giurisprudenza citata ai p.ti 61 e 62 della presente sentenza, tali giudici devono sospendere la decisione e investire la Corte di un procedimento pregiudiziale per accertamento di validità, allorché essi ritengano che uno o più motivi di invalidità formulati dalle parti o, eventualmente, sollevati d’ufficio siano fondati (v., in tal senso, sentenza T & L Sugars e Sidul Açucarese/Commissione, C-456/13 P, […] p.to 48 e la giurisprudenza ivi citata).

65. Nell’ipotesi contraria, in cui detta autorità reputi fondate le censure sollevate dalla persona che l’ha investita di una domanda relativa alla protezione dei suoi diritti e libertà con riguardo al trattamento dei suoi dati personali, questa stessa autorità, ai sensi dell’art.28, §3, primo comma, terzo trattino, della direttiva 95/46, in combinato, segnatamente, con l’art.8, §3, della Carta, deve poter promuovere azioni giudiziarie. A tal riguardo, incombe al legislatore nazionale prevedere mezzi di ricorso che consentano all’autorità nazionale di controllo di cui trattasi di far valere le censure che essa reputa fondate dinanzi ai giudici nazionali, affinché questi ultimi procedano, qualora condividano i dubbi di tale autorità in ordine alla validità della decisione della Commissione, ad un rinvio pregiudiziale inteso all’esame della validità di tale decisione.

66. In virtù delle considerazioni che precedono, si deve rispondere alle questioni sollevate che l’art.25, §6, della direttiva 95/46, letto alla luce degli artt.7, 8 e 47 della Carta, deve essere interpretato nel senso che una decisione adottata in forza di tale disposizione, quale la decisione 2000/520, con la quale la Commissione constata che un paese terzo garantisce un livello di protezione adeguato, non osta a che un’autorità di controllo di uno Stato membro, ai sensi dell’art.28 di tale direttiva, esaminì la domanda di una persona relativa alla protezione dei suoi diritti e libertà con riguardo al trattamento di dati personali che la riguardano, i quali sono stati trasferiti da uno Stato membro verso tale paese terzo, qualora tale persona faccia valere che il diritto e la prassi in vigore in quest’ultimo non garantiscono un livello di protezione adeguato.

**Sulla validità della decisione 2000/520**

67. Come si evince dalle spiegazioni del giudice del rinvio relative alle questioni sollevate, il sig. Schrems fa valere, nel procedimento principale, che il diritto e la prassi degli Stati Uniti non assicurano un livello di protezione adeguato ai sensi dell’art.25 della direttiva 95/46. Come rilevato dall’avvocato generale ai §§123 e 124 delle sue conclusioni, il sig. Schrems esprime dubbi, che tale giudice sembra peraltro condividere nella sostanza, concernenti la validità della decisione 2000/520. In tali circostanze, in virtù delle constatazioni effettuate ai punti da 60 a 63 della presente sentenza, e al fine di fornire una risposta completa al detto giudice, occorre verificare se tale decisione sia conforme ai requisiti risultanti da detta direttiva, letta alla luce della Carta.

**Sui requisiti risultanti dall’art.25, §6, della direttiva 95/46**

68. Come è già stato rilevato ai p.ti 48 e 49 della presente sentenza, l’art.25, §1, della direttiva 95/46 vieta i trasferimenti di dati personali verso un paese terzo che non garantisce un livello di protezione adeguato.

69. Tuttavia, ai fini del controllo di tali trasferimenti, l’art.25, §6, primo comma, di tale direttiva, dispone che la Commissione «può constatare (…) che un paese terzo garantisce un livello di protezione adeguato ai sensi del §2 [di tale articolo], in considerazione della sua legislazione nazionale o dei suoi impegni internazionali (…), ai fini della tutela della vita privata o delle libertà e dei diritti fondamentali della persona».

70. È vero che né l’art.25, §2, della direttiva 95/46 né nessun’altra disposizione della medesima contengono una definizione della nozione di livello di protezione adeguato. In particolare, l’art.25, §2, di detta direttiva si limita ad enunciare che l’adeguatezza del livello di protezione garantito da un paese terzo «è valutata con riguardo a tutte le circostanze relative ad
un trasferimento o ad una categoria di trasferimenti di dati» ed elenca, in maniera non esaustiva, le circostanze che devono essere prese in considerazione in occasione di una siffatta valutazione.

71. Tuttavia, da un lato, come si evince dalla lettera stessa dell’art.25, §6, della direttiva 95/46, tale disposizione esige che un paese terzo «garantisca[1]» un livello di protezione adeguato in considerazione della sua legislazione nazionale o dei suoi impegni internazionali. Dall’altro, sempre secondo tale disposizione, l’adeguatezza della protezione assicurata dal paese terzo viene valutata «ai fini della tutela della vita privata o delle libertà e dei diritti fondamentali della persona».

72. In tal modo, l’art.25, §6, della direttiva 95/46 attua l’obbligo esplicito di protezione dei dati personali previsto all’art.8, §1, della Carta e mira ad assicurare, come rilevato dall’avvocato generale ai §§139 delle sue conclusioni, la continuità del livello elevato di tale protezione in caso di trasferimento di dati personali verso un paese terzo.

73. È vero che il termine «adeguato» figurante all’art.25, §6, della direttiva 95/46 implica che non possa esigersi che un paese terzo assicuri un livello di protezione identico a quello garantito nell’ordinamento giuridico dell’Unione. Tuttavia, come rilevato dall’avvocato generale ai §141 delle sue conclusioni, l’espressione «livello di protezione adeguato» deve essere intesa nel senso che esige che tale paese assicuri effettivamente, in considerazione della sua legislazione nazionale o dei suoi impegni internazionali, un livello di protezione delle libertà e dei diritti fondamentali sostanzialmente equivalente a quello garantito all’interno dell’Unione in forza della direttiva 95/46, letta alla luce della Carta. Infatti, in assenza di un siffatto requisito, l’obiettivo menzionato al punto precedente della presente sentenza sarebbe disatteso. Inoltre, il livello elevato di protezione garantito dalla direttiva 95/46, letta alla luce della Carta, potrebbe essere facilmente eluso da trasferimenti di dati personali dall’Unione verso paesi terzi ai fini del loro trattamento in tali paesi.

74. Si evince dalla formulazione espressa dell’art.25, §6, della direttiva 95/46 che è l’ordinamento giuridico del paese terzo interessato dalla decisione della Commissione che deve garantire un livello di protezione adeguato. Anche se gli strumenti dei quali tale paese terzo si avvale, al riguardo, per assicurare un siffatto livello di protezione, possono essere diversi da quelli attuati all’interno dell’Unione al fine di garantire il rispetto dei requisiti risultanti da tale direttiva, letta alla luce della Carta, tali strumenti devono cionondimeno rivelarsi efficaci, nella prassi, al fine di assicurare una protezione sostanzialmente equivalente a quella garantita all’interno dell’Unione.

75. In tali condizioni, in sede di esame del livello di protezione offerto da un paese terzo, la Commissione è tenuta a valutare il contenuto delle norme applicabili in tale paese risultanti dalla legislazione nazionale o dagli impegni internazionali di quest’ultimo, nonché la prassi intesa ad assicurare il rispetto di tali norme; al riguardo, tale istituzione deve prendere in considerazione, in conformità all’art.25, §2, della direttiva 95/46, tutte le circostanze relative ad un trasferimento di dati personali verso un paese terzo.

76. Analogamente, alla luce del fatto che il livello di protezione assicurato da un paese terzo può evolversi, incombe alla Commissione, successivamente all’adozione di una decisione in forza dell’art.25, §6, della direttiva 95/46, verificare periodicamente se la constatazione relativa al livello di protezione adeguato assicurato dal paese terzo in questione continui ad essere giustificata in fatto e in diritto. Una siffatta verifica è in ogni caso obbligatoria quando taluni indizi facciano sorgere un dubbio al riguardo.

77. Inoltre, come rilevato dall’avvocato generale ai §§134 e 135 delle sue conclusioni, in sede di esame della validità di una decisione della Commissione adottata in forza dell’art.25, §6, della direttiva 95/46, occorre anche tenere conto delle circostanze intervenute successivamente all’adozione di tale decisione.

78. A tal riguardo, occorre constatare che, alla luce, da un lato, del ruolo importante svolto dalla protezione dei dati personali sotto il profilo del diritto fondamentale al rispetto della vita privata e, dall’altro, del numero significativo di persone i cui diritti fondamentali possono essere violati in caso di trasferimento di dati personali verso un paese terzo che non assicura un livello di protezione adeguato, il potere discrezionale della Commissione in ordine all’adeguatezza del livello di protezione assicurato da un paese terzo risulta ridotto, cosicché è necessario procedere ad un controllo stretto dei requisiti risultanti dall’art.25 della direttiva 95/46, letto alla luce della Carta (v., per analogia, sentenza Digital Rights Ireland e a., C-293/12 e C-594/12, […] p.ti 47 e 48).

Sull’art.1 della decisione 2000/520

79. La Commissione ha considerato, all’art.1, §1, della decisione 2000/520, che i principi di cui all’allegato I della medesima, applicati in conformità agli orientamenti forniti dalle FAQ di cui all’allegato II di detta decisione, garantiscono un livello adeguato di protezione dei dati personali.
trasferiti dall'Unione a organizzazioni aventi sede negli Stati Uniti. Risulta da tale disposizione che sia tali principi sia tali FAQ sono stati pubblicati dal Dipartimento del commercio degli Stati Uniti.

80. L'adesione di un'organizzazione ai principi dell'approdo sicuro avviene sulla base di un sistema di autocertificazione, come si evince dall'art.1, §§2 e 3, di tale decisione, in combinato disposto con la FAQ 6 figurante all'allegato II a detta decisione.

81. Sebbene il ricorso, da parte di un paese terzo, ad un sistema di autocertificazione non sia di per sé contrario al requisito previsto dall'art.25, §6, della direttiva 95/46, secondo il quale il paese terzo di cui trattasi deve garantire un livello di protezione adeguato «in considerazione della (...) legislazione nazionale o [degli] impianti internazionali» di tale paese, l'affidabilità di un siffatto sistema, con riferimento a tale requisito, poggia essenzialmente sulla predisposizione di meccanismi efficaci di accertamento e di controllo che consentano di individuare e sanzionare, nella prassi, eventuali violazioni delle norme che assicurano la protezione dei diritti fondamentali, e segnatamente del diritto al rispetto della vita privata, nonché del diritto alla protezione dei dati personali.

82. Nella specie, in forza dell'allegato I, secondo comma, della decisione 2000/520, i principi dell'approdo sicuro sono «destinati unicamente ad organizzazioni americane che ricevono dati personali dall'Unione Europea, al fine di permettere a tali organizzazioni di ottemperare al principio di “approdo sicuro” e alla presunzione di “adeguatezza” che esso comporta». Tali principi sono dunque applicabili soltanto alle organizzazioni americane autocertificate che ricevono dati personali dall'Unione, mentre dalle autorità pubbliche americane non si esige il rispetto di detti principi.

83. Inoltre, ai sensi dell'art.2 della decisione 2000/520, quest'ultima «dispone soltanto in merito all'adeguatezza della protezione offerta negli Stati Uniti, in base ai principi [dell'approdo sicuro] applicati in conformità alle FAQ, al fine di quanto prescritto dall'art.25, §1, della direttiva [95/46]», senza tuttavia contenere le constatazioni sufficienti quanto alle misure tramite le quali gli Stati Uniti d'America assicurano un livello di protezione adeguato, ai sensi dell'art.25, §6, di tale direttiva, in considerazione della loro legislazione nazionale o dei loro impegni internazionali.

84. A ciò si aggiunge che, in conformità all'allegato I, quarto comma, della decisione 2000/520, l'applicabilità di detti principi può essere limitata, segnatamente, «se ed in quanto necessario per soddisfare esigenze di sicurezza nazionale, interesse pubblico o amministrazione della giustizia [degli Stati Uniti]», nonché da «disposizioni legislative o regolamentari ovvero decisioni giurisdizionali quando tali fonti comportino obblighi contrastanti od autorizzazioni esplicite, purché nell'avvalersi di un'autorizzazione siffatta un'organizzazione possa dimostrare in considerazione della loro legislazione nazionale o dei loro impegni internazionali.

85. A tal riguardo, al titolo B del suo allegato IV, la decisione 2000/520 sottolinea, per quanto attiene ai limiti ai quali è assoggettata l'applicabilità dei principi dell'approdo sicuro, che «[l] ovvio che quando la legge statunitense impone un'obbligazione conflittuale, le organizzazioni statunitensi, che aderiscano o no ai principi “approdo sicuro”, devono osservare la legge».

86. In tal modo, la decisione 2000/520 sancisce il primato delle «esigenze di sicurezza nazionale, interesse pubblico o amministrazione della giustizia [degli Stati Uniti]» sui principi dell'approdo sicuro, primato in forza del quale le organizzazioni americane autocertificate che ricevono dati personali dall'Unione sono tenute a disapplicare senza limiti tali principi allorché questi ultimi interferiscono con tali esigenze e risultano dunque incompatibili con le medesime.

87. Alla luce del carattere generale della deroga figurante all'allegato I, quarto comma, della decisione 2000/520, essa rende pertanto possibili ingerenze, fondate su esigenze connesse alla sicurezza nazionale e all'interesse pubblico o alla legislazione interna degli Stati Uniti, nei diritti fondamentali delle persone i cui dati personali sono o potrebbero essere trasferiti dall'Unione verso gli Stati Uniti. A tal riguardo, poco importa, per accertare l'esistenza di un'ingerenza nel diritto fondamentale al rispetto della vita privata, che le informazioni relative alla vita privata di cui trattasi abbiano o meno un carattere sensibile o che gli interessati abbiano o meno subito eventuali inconvenienti in seguito a tale ingerenza (sentenza Digital Rights Ireland e a., C-293/12 e C-594/12, [...], p.to 33 e la giurisprudenza ivi citata).

88. Inoltre, la decisione 2000/520 non contiene alcuna dichiarazione quanto all'esistenza, negli Stati Uniti, di norme statali destinate a limitare le eventuali ingerenze nei diritti fondamentali delle persone i cui dati vengono trasferiti dall'Unione verso gli Stati Uniti, ingerenze che entità
statali di tale paese sarebbero autorizzate a compiere laddove perseguano obiettivi legittimi, come la sicurezza nazionale.

89. A ciò si aggiunge il fatto che la decisione 2000/520 non menziona l'esistenza di una tutela giuridica efficace nei confronti delle ingiustizie di tale natura. Come rilevato dall'avvocato generale ai paragrafi da 204 a 206 delle sue conclusioni, i meccanismi di arbitrato privato e i procedimenti dinanzi alla Commissione federale per il commercio, i cui poteri, descritti segnatamente nelle FAQ 11 figuranti all'allegato II a tale decisione, sono limitati alle controversie in materia commerciale, riguardano il rispetto, da parte delle imprese americane, dei principi dell'approdo sicuro, e non possono essere applicati nell'ambito delle controversie concernenti la legittimità di ingiustizie nei diritti fondamentali risultanti da misure di origine statale.

90. Inoltre, la suesposta analisi della decisione 2000/520 è corroborata dalla valutazione della stessa Commissione quanto alla situazione risultante dall’esecuzione di tale decisione. Infatti, in particolare ai p.ti 2 e 3.2 della comunicazione COM(2013) 846 final, nonché ai p.ti 7.1, 7.2 e 8 della comunicazione COM(2013) 847 final, il cui contenuto viene illustrato rispettivamente ai punti da 13 a 16, nonché ai p.ti 22, 23 e 25 della presente sentenza, tale istituzione ha constatato che le autorità americane potevano accedere ai dati personali trasferiti dagli Stati membri verso gli Stati Uniti e trattarli in maniera incompatibile, segnatamente, con le finalità del loro trasferimento, e al di là di quanto era strettamente necessario e proporzionato per la protezione della sicurezza nazionale. Analogamente, la Commissione ha constatato che non esistevano, per le persone di cui trattasi, rimedi amministrativi o giurisdizionali che consentissero, segnatamente, di accedere ai dati che le riguardavano e, se del caso, di ottennerne la rettifica o la soppressione.

91. Quanto al livello di protezione delle libertà e dei diritti fondamentali garantito all’interno dell’Unione, una normativa della medesima che comporta un’ingerenza nei diritti fondamentali garantiti dagli artt.7 e 8 della Carta deve prevedere, secondo la giurisprudenza costante della Corte, regole chiare e precise che disciplinino la portata e l’applicazione della misura de qua e impongano requisiti minimi in modo che le persone i cui dati personali sono interessati dispongano di garanzie sufficienti che permettano di proteggere efficacemente i loro dati contro il rischio di abusi nonché contro eventuali accessi e usi illeciti dei suddetti dati. La necessità di disporre di siffatte garanzie è tanto più importante allorché i dati personali sono soggetti a trattamento automatico ed esiste un rischio considerevole di accesso illecito ai dati stessi (sentenza Digital Rights Ireland e a., C-293/12 e C-594/12, […] p.ti 54 e 55, nonché la giurisprudenza ivi citata).

92. Inoltre, è soprattutto, la protezione del diritto fondamentale al rispetto della vita privata a livello dell’Unione richiede che le deroghe e le restrizioni alla tutela dei dati personali operino entro i limiti dello stretto necessario (sentenza Digital Rights Ireland e a., C-293/12 e C-594/12, […] p.to 52 e la giurisprudenza ivi citata).

93. In tal senso, non è limitata allo stretto necessario una normativa che autorizza in maniera generale la conservazione di tutti i dati personali di tutte le persone i cui dati sono stati trasferiti dall’Unione verso gli Stati Uniti senza alcuna distinzione, limitazione o eccezione a seconda dell’obiettivo perseguito e senza che sia previsto alcun criterio oggettivo che permetta di delimitare l’accesso delle autorità pubbliche ai dati e il loro uso ulteriore a fini precisi, rigorosamente ristretti ed idonei a giustificare l’ingerenza che sia l’accesso sia l’utilizzazione di tali dati comporta [v. in tal senso, in relazione alla direttiva 2006/24/CE […]]. del 15 marzo 2006, riguardante la conservazione di dati generati o trattati nell’ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE, […]]. sentenza Digital Rights Ireland e a., C-293/12 e C-594/12, […] punti da 57 a 61].

94. In particolare, si deve ritenere che una normativa che consente alle autorità pubbliche di accedere in maniera generalizzata al contenuto di comunicazioni elettroniche pregiudichi il contenuto essenziale del diritto fondamentale al rispetto della vita privata, come garantito dall’art.7 della Carta (v., in tal senso, sentenza Digital Rights Ireland e a., C-293/12 e C-594/12, […] p.to 39).

95. Analogamente, una normativa che non preveda alcuna possibilità per il singolo di avvalersi di rimedi giuridici al fine di accedere a dati personali che lo riguardano, oppure di ottenere la rettifica o la soppressione di tali dati, non rispetta il contenuto essenziale del diritto fondamentale ad una tutela giurisdizionale effettiva, quale sancito all’art.47 della Carta. Infatti, l’art.47, primo comma, della Carta esige che ogni individuo i cui diritti e le cui libertà garantiti dal diritto dell’Unione siano stati violati abbia diritto ad un ricorso effettivo dinanzi ad un giudice, nel rispetto delle condizioni previste in tale articolo. A tal riguardo, l’esistenza stessa di un controllo
giurisdizionale effettivo, destinato ad assicurare il rispetto delle disposizioni del diritto dell’Unione, è inerente all’esistenza di uno Stato di diritto (v., in tal senso, sentenze Les Verts/Parlamento, 294/83, […], p.to 23; Johnston, 222/84, […], p.ti 18 e 19; Heylens e a., 222/86, […], p.to 14, nonché, UGT-Rioja e a., da C-428/06 a C-434/06, […], p.to 80).

96. Come è stato rilevato segnatamente ai p.ti 71, 73 e 74 della presente sentenza, l’adozione, da parte della Commissione, di una decisione in forza dell’art.25, §6, della direttiva 95/46 richiede la constatazione, debitamente motivata, da parte di tale istituzione, che il paese terzo di cui trattasi garantisce effettivamente, in considerazione della sua legislazione nazionale o dei suoi impegni internazionali, un livello di protezione dei diritti fondamentali sostanzialmente equivalente a quello garantito nell’ordinamento giuridico dell’Unione, come emerge segnatamente dai punti precedenti della presente sentenza.

97. Orbene, occorre rilevare che la Commissione, nella decisione 2000/520, non ha affermato che gli Stati Uniti d’America «garantiscono» effettivamente un livello di protezione adeguato in considerazione della loro legislazione nazionale o dei loro impegni internazionali.

98. Di conseguenza, e senza che occorra esaminare i principi dell’approdo sicuro sotto il profilo del loro contenuto, si deve considerare che l’art.1 di tale decisione viola i requisiti fissati all’art.25, §6, della direttiva 95/46, letto alla luce della Carta, e che esso è, per tale motivo, invalido.

Sull’art.3 della decisione 2000/520

99. Si evince dalle considerazioni svolte ai p.ti 53, 57 e 63 della presente sentenza che, considerato l’art.28 della direttiva 95/46, letto alla luce, segnatamente, dell’art.8 della Carta, le autorità nazionali di controllo devono poter esaminare, in piena indipendenza, ogni domanda relativa alla protezione dei diritti e delle libertà di una persona, nel rispetto dei dati personali che la riguardano. Ciò vale in particolare allorché, in occasione di una siffatta domanda, tale persona sollevi questioni attinenti alla compatibilità di una decisione della Commissione adottata in forza dell’art.25, §6, di tale direttiva, con la protezione della vita privata e delle libertà e dei diritti fondamentali della persona.

100. Tuttavia, l’art.3, §1, primo comma, della decisione 2000/520 contiene una disciplina specifica quanto ai poteri di cui dispongono le autorità nazionali di controllo con riferimento ad una constatazione effettuata dalla Commissione in relazione al livello di protezione adeguato, ai sensi dell’art.25 della direttiva 95/46.

101. Così, ai sensi di tale disposizione, tali autorità possono, «[f]atto salvo il loro potere di adottare misure per garantire l’ottemperanza alle disposizioni nazionali adottate in forza di disposizioni diverse dall’art.25 della direttiva [95/46], (…) sospendere flussi di dati diretti a un’organizzazione che ha autocertificato la sua adesione ai principi [della decisione 2000/520]», a condizioni restrittive che fissano una soglia elevata di intervento. Per quanto tale disposizione non pregiudichi i poteri di dette autorità di adottare misure intese ad assicurare il rispetto delle disposizioni nazionali adottate in applicazione di questa direttiva, cionondimeno essa esclude che le medesime possano adottare misure intese a garantire il rispetto dell’art.25 della direttiva medesima.

102. L’art.3, §1, primo comma, della decisione 2000/520 deve pertanto essere inteso nel senso che esso priva le autorità nazionali di controllo dei poteri che esse traggono dall’art.28 della direttiva 95/46, nel caso in cui una persona, in occasione di una domanda basata su tale disposizione, adduca elementi idonei a rimettere in discussione il fatto che una decisione della Commissione che ha constatato, sul fondamento dell’art.25, §6, di tale direttiva, che un paese terzo garantisce un livello di protezione adeguato, sia compatibile con la protezione della vita privata e delle libertà e dei diritti fondamentali della persona.

103. Orbene, il potere di esecuzione che il legislatore dell’Unione ha attribuito alla Commissione con l’art.25, §6, della direttiva 95/46 non conferisce a tale istituzione la competenza di limitare i poteri delle autorità nazionali di controllo previsti al punto precedente della presente sentenza.

104. Ciò premesso, occorre constatare che, adottando l’art.3 della decisione 2000/520, la Commissione ha ecceduto la competenza attribuitale all’art.25, §6, della direttiva 95/46, letto alla luce della Carta, e che, per questo motivo, esso è invalido.

105. Poiché gli artt.1 e 3 della decisione 2000/520 non possono essere separati dagli artt.2 e 4, nonché dagli allegati alla medesima, la loro invalidità inficia la validità di tale decisione nel suo complesso.
106. Alla luce di tutte le considerazioni che precedono, si deve concludere che la decisione 2000/520 è invalida.

Per questi motivi, la Corte (Grande Sezione) dichiara:

1) L’art.25, §6, della direttiva 95/46/CE [...], del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, come modificata dal regolamento (CE) n.1882/2003 [...], del 29 settembre 2003, letto alla luce degli artt.7, 8 e 47 della Carta dei diritti fondamentali dell’Unione Europea, deve essere interpretato nel senso che una decisione adottata in forza di tale disposizione, come la decisione 2000/520/CE [...] del 26 luglio 2000, a norma della direttiva 95/46 sull’adeguatezza della protezione offerta dai principi di approdo sicuro e dalle relative «Domande più frequenti» (FAQ) in materia di riservatezza pubblicate dal Dipartimento del commercio degli Stati Uniti, con la quale la Commissione europea constata che un paese terzo garantisce un livello di protezione adeguato, non osta a che un’autorità di controllo di uno Stato membro, ai sensi dell’art.28 di tale direttiva, come modificata, esamini la domanda di una persona relativa alla protezione dei suoi diritti e delle sue libertà con riguardo al trattamento di dati personali che la riguardano, i quali sono stati trasferiti da uno Stato membro verso tale paese terzo, qualora tale persona faccia valere che il diritto e la prassi in vigore in quest’ultimo non garantiscono un livello di protezione adeguato.

2) La decisione 2000/520 è invalida.

*****

DISCUSSIONE

1. Quali sono i principi della normativa in materia di protezione dei dati personali che si applicano al trasferimento di dati a Stati non membri dell’Unione europea?

2. Cosa si intende, nei rapporti tra Unione europea e Stati Uniti, per "approdo sicuro" ("safe harbor")?

3. Sotto quelli profili viene contestata la validità della decisione 2000/520/CE?

4. Quali poteri riconosce la Corte alle autorità nazionali di controllo, di fronte alla decisione 2000/520/CE?

5. Gli Stati Uniti assicurano un adeguato livello di protezione ai diritti delle persone (dell'Unione europea) in riferimento ai dati personali trasferiti da uno Stato membro?

*****

NORME

- artt.7, 8, 47 CDFUE
2.3. Tutela dei dati personali e stabilimento in altro Stato membro

Corte di Giustizia dell’Unione Europea, 1 ottobre 2015 (causa C-230/14)

1. La domanda di pronuncia pregiudiziale verte sull’interpretazione degli artt.4, §1, lett.a), e 28, §§1, 3 e 6, della direttiva 95/46/CE […] del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati […].

2. Tale domanda è stata presentata nell’ambito di una controversia tra la Weltimmo s. r. o. (in prosieguo: la «Weltimmo»), società la cui sede è in Slovacchia, e la Nemzeti Adatvédelmi és Információszabadság Hatóság (autorità nazionale incaricata della protezione dei dati e della libertà dell’informazione; in prosieguo: l’«autorità ungherese di controllo») in merito a un’amministrazione emanata da quest’ultima per violazione della legge n.CXII del 2011 sul diritto di autodeterminazione in materia di informazione e sulla libertà di informazione ([…]in prosieguo: la «legge sull’informazione»), che ha recepito la direttiva 95/46 nel diritto ungherese.

14. Nutrendo dubbi sull’individuazione del diritto applicabile e sulle competenze dell’autorità ungherese di controllo alla luce degli artt.4, §1, e 28 della direttiva 95/46, la Kúria (Corte suprema) ha deciso di sospendere il procedimento e di sottoporre alla Corte le seguenti questioni pregiudiziali:

«1) Se l’art.28, §1, della direttiva 95/46 debba essere interpretato nel senso che la normativa nazionale di uno Stato membro può applicarsi nel suo territorio a un responsabile del trattamento dei dati, stabilito esclusivamente in un altro Stato membro, che gestisce una pagina Internet di intermediazione immobiliare e che pubblicizza, tra l’altro, immobili situati nel territorio del primo Stato membro, i proprietari dei quali trasmettono dati personali a un dispositivo (server) per la memorizzazione e l’elaborazione di dati appartenente al gestore della pagina Internet e situato in un altro Stato membro.

2) Se, alla luce dei considerando da 18 a 20 e degli artt.1, §2, e 28, §1, l’art.4, §1, lett.a), della direttiva 95/46 debba essere interpretato nel senso che l’autorità ungherese di controllo non può applicare la legge ungherese sulla protezione dei dati, quale diritto nazionale, al gestore di una pagina Internet di intermediazione immobiliare stabilito esclusivamente in un altro Stato membro neppure qualora detto gestore pubblicizzi, tra l’altro, immobili situati in territorio di altro Stato membro, i proprietari dei quali trasmettono dati personali a un dispositivo (server) per la memorizzazione e l’elaborazione di dati appartenente al gestore della pagina Internet e situato in un altro Stato membro.

3) Se, a fini interpretativi, rilevi che il servizio fornito dal responsabile del trattamento di dati che gestisce la pagina Internet sia rivolto al territorio dell’altro Stato membro.

4) Se, a fini interpretativi, rilevi che i dati concernenti gli immobili situati nel territorio dell’altro Stato membro e i dati personali dei proprietari siano stati effettivamente caricati dal territorio di detto altro Stato membro.

5) Se, a fini interpretativi, rilevi che i dati personali trasmessi in relazione ai citati immobili riguardino cittadini dell’altro Stato membro.

6) Se, a fini interpretativi, rilevi che i titolari della società stabilita in Slovacchia abitino in Ungheria.

[…] Sulle questioni pregiudiziali

Osservazioni preliminari

15. Per quanto attiene, anzitutto, all’ambito fattuale della controversia nel procedimento principale, occorre menzionare alcuni elementi informativi integrativi, presentati dall’autorità ungherese di controllo nelle sue osservazioni scritte e all’udienza dinanzi alla Corte.

16. Si evince da tali elementi, in primo luogo, che tale autorità avrebbe appreso, informalmente, dalla sua omologa slovacca che la Weltimmo non svolgeva nessuna attività nel territorio della sua sede, in Slovacchia. Inoltre, la Weltimmo avrebbe più volte spostato la sede da uno
Stato a un altro. In secondo luogo, la Weltimmo avrebbe creato due siti di annunci immobiliari, scritti solamente in lingua ungherese, avrebbe aperto un conto bancario in Ungheria, destinato al recupero crediti, e avrebbe avuto una casella postale in tale Stato membro, per gli affari correnti. La posta sarebbe stata regolarmente prelevata e trasmessa alla Weltimmo per via elettronica. In terzo luogo, gli inserzionisti non soltanto devono essi stessi iscrivere i dati relativi ai loro immobili nel sito della Weltimmo, ma anche cancellare tali dati dal sito se non vogliono che continuino a figurarvi oltre il periodo di un mese sopra menzionato. La Weltimmo avrebbe avanzato un problema di gestione informatica per spiegare perché non aveva potuto cancellare i dati. In quarto luogo, la Weltimmo sarebbe una società composta di una o due persone soltanto. Il suo rappresentante in Ungheria avrebbe cercato di negoziare con gli inserzionisti il pagamento dei crediti insolventi.

17. Per quanto attiene, poi, alla formulazione delle questioni sottoposte, nonostante il giudice del rinvio utilizzi i termini «stabilito esclusivamente» nella prima e nella seconda questione, si evince dalla decisione di rinvio e dalle osservazioni scritte e orali presentate dall’autorità ungherese di controllo che, sebbene la Weltimmo sia registrata in Slovacchia e sia, di conseguenza, stabilita in tale Stato membro, ai sensi del diritto societario, sussistono dubbi sul fatto se sia «stabilita» unicamente in tale Stato membro, a norma dell’art.4, §1, lett.a), della direttiva 95/46. Chiedendo alla Corte di interpretare tale disposizione, il giudice del rinvio intende, infatti, sapere cosa rientri nella nozione di «stabilimento» utilizzata in detta disposizione.

18. Occorre, infine, rilevare che nella prima e nella seconda questione, il giudice del rinvio afferma che il server usato dalla Weltimmo è installato in Slovacchia, mentre, in un altro passo della decisione di rinvio, accenna che è possibile che i server di tale società si trovino in Germania o in Austria. Ciò detto, sembra opportuno considerare che non sia appurato in quale Stato membro si trova il server o si trovano i server usati da detta società.

Sulle questioni dalla prima alla sesta

19. Con le questioni dalla prima alla sesta, che occorre esaminare congiuntamente, il giudice del rinvio chiede in sostanza se gli artt.4, §1, lett.a), e 28, §1, della direttiva 95/46 devono essere interpretati nel senso che, in circostanze quali quelle del procedimento principale, essi consentono all’autorità di controllo di un solo Stato membro di applicare la sua normativa nazionale in materia di protezione dei dati nei confronti di un responsabile del trattamento, la cui società è registrata in un altro Stato membro e che gestisce un sito Internet di annunci immobiliari riguardanti beni immobili situati nel territorio del primo di tali due Stati. Detto giudice chiede in particolare se sia rilevante che tale Stato membro sia quello:

– verso il quale si rivolge l’attività del responsabile del trattamento dei dati personali,
– in cui sono situati i beni immobili interessati,
– a partire dal quale sono comunicati dati relativi ai proprietari di tali beni,
– del quale sono cittadini questi ultimi, e
– nel quale siano domiciliati i titolari di tale società.

20. Per quanto riguarda il diritto applicabile, il giudice del rinvio cita in particolare gli ordinamenti slovacco e ungherese; nel primo è il diritto dello Stato membro in cui è registrato il responsabile del trattamento dei dati personali di cui trattasi, mentre nel secondo è quello del Stato membro cui si rivolgono i siti Internet di cui è causa nel procedimento principale, nel territorio del quale sono situati i beni immobili oggetto degli annunci pubblicati.


22. L’art.28 della direttiva 95/46, rubricato «Autorità di controllo», è, invece, dedicato al ruolo e ai poteri di tale autorità. In forza di tale art.28, §1, essa è incaricata di sorvegliare, nel territorio del suo Stato membro, l’applicazione delle disposizioni di attuazione della direttiva adottate dagli Stati membri. Ai sensi dell’art.28, §6, di detta direttiva, l’autorità di controllo esercita i poteri attribuiti, indipendentemente dalla legge nazionale applicabile al trattamento dei dati personali.

23. Occorre dunque determinare il diritto nazionale applicabile al responsabile di tale trattamento alla luce non dell’art.28 della direttiva 95/46, ma dell’art.4 della medesima.

24. Ai termini dell’art.4, §1, lett.a), della direttiva 95/46, ciascuno Stato membro applica le disposizioni nazionali adottate per l’attuazione della presente direttiva al trattamento di dati personali effettuato nel contesto delle attività di uno stabilimento del responsabile del trattamento nel territorio dello Stato membro.
25. Alla luce dell’obiettivo perseguito dalla direttiva 95/46, consistente nel garantire una tutela efficace e completa delle libertà e dei diritti fondamentali delle persone fisiche, segnatamente del diritto alla vita privata, con riguardo al trattamento dei dati personali, l’espressione «nel contesto delle attività di uno stabilimento» non può ricevere un’interpretazione restrittiva (v., in tal senso, sentenza Google Spain e Google, C-131/12, […], p.to 53).

26. Per conseguire tale obiettivo ed evitare che una persona venga privata della tutela cui ha diritto in forza della direttiva in parola, il considerando 18 della medesima direttiva enuncia che è necessario che qualsiasi trattamento di dati personali effettuato nell’Unione Europea rispetti la legislazione di uno degli Stati membri e che è opportuno assoggettare i trattamenti effettuati da chiunque operi sotto l’autorità del responsabile del trattamento stabilito in uno Stato membro alla legge di tale Stato.

27. Il legislatore dell’Unione ha quindi previsto un ambito di applicazione territoriale della direttiva 95/46 particolarmente esteso, che ha inserito all’art.4 della stessa (v., in tal senso, sentenza Google Spain e Google, C-131/12, […], p.to 54).

28. Per quanto attiene, in primo luogo, alla nozione di «stabilimento», va ricordato che il considerando 19 della direttiva 95/46 enuncia che lo stabilimento nel territorio di uno Stato membro implica l’esercizio effettivo e reale dell’attività mediante un’organizzazione stabile e che la forma giuridica di siffatto stabilimento, si tratti di una semplice succursale o di una filiale dotata di personalità giuridica, non è il fattore determinante a questo riguardo (sentenza Google Spain e Google, C-131/12, […], p.to 48). Detto considerando precisa, inoltre, che, quando un unico responsabile del trattamento è stabilito nel territorio di diversi Stati membri, esso deve assicurare, segnatamente per evitare che le disposizioni vengano eluse, che ognuno degli stabilimenti adempia gli obblighi previsti dalla legge nazionale applicabile alle attività di ciascuno di essi.

29. Ne consegue, come ha sostanzialmente rilevato l’avvocato generale ai §§28 e da 32 a 34 delle sue conclusioni, una concezione flessibile della nozione di stabilimento, che si discosta dall’impostazione formale secondo cui un’impresa sarebbe stabilita esclusivamente nel luogo in cui è registrata. Infatti, per determinare se una società, responsabile di un trattamento dei dati, dispone di uno stabilimento, ai sensi della direttiva, 95/46, in uno Stato membro diverso dallo Stato membro o dal paese terzo in cui è registrata, occorre valutare sia il grado di stabilità dell’organizzazione sia l’esercizio effettivo delle attività in tale altro Stato membro, prendendo in considerazione la natura specifica delle attività economiche e delle prestazioni di servizi in questione. Ciò vale soprattutto per imprese che offrono servizi esclusivamente tramite Internet.

30. A questo proposito, occorre segnatamente considerare, alla luce dell’obiettivo perseguito da tale direttiva, consistente nel garantire una tutela efficace e completa del diritto alla vita privata e nell’evitare che le disposizioni vengano eluse, che la presenza di un unico rappresentante, in talune circostanze, può essere sufficiente a costituire un’organizzazione stabile se il medesimo opera con un grado di stabilità sufficiente con l’ausilio dei mezzi necessari per la fornitura dei servizi concreti di cui trattasi nello Stato membro in questione. Ciò vale soprattutto per imprese che offrono servizi esclusivamente tramite Internet.

31. Inoltre, per realizzare detto obiettivo, occorre considerare che la nozione di «stabilimento», ai sensi della direttiva 95/46, si estende a qualsiasi attività reale ed effettiva, anche minima, esercitata tramite un’organizzazione stabile.

32. Nel caso di specie, l’attività esercitata dalla Weltimmo consiste, quantomeno, nella gestione di uno dei vari siti Internet di annunci immobiliari riguardanti beni situati in Ungheria, scritti in lingua ungherese e i cui annunci diventano a pagamento dopo un mese. Occorre dunque affermare che tale società svolge un’attività concreta ed effettiva che è opportuno assoggettare i trattamenti effettuati da chiunque operi sotto l’autorità del responsabile del trattamento stabilito in uno Stato membro alla legge di tale Stato.

33. Per conseguire tale obiettivo ed evitare che una persona venga privata della tutela cui ha diritto in forza della direttiva in parola, il considerando 18 della medesima direttiva enuncia che è necessario che qualsiasi trattamento di dati personali effettuato nell’Unione Europea rispetti la legislazione di uno degli Stati membri e che è opportuno assoggettare i trattamenti effettuati da chiunque operi sotto l’autorità del responsabile del trattamento stabilito in uno Stato membro alla legge di tale Stato.

34. Occorre, in secondo luogo, sapere se il trattamento dei dati personali di cui trattasi è fatto «nel contesto delle attività» di tale stabilimento.
35. La Corte ha già considerato che l’art.4, §1, lett.a), della direttiva 95/46 non esige che il trattamento di dati personali in questione venga effettuato «dallo» stesso stabilimento interessato, bensì soltanto che venga effettuato «nel contesto delle attività» di quest’ultimo (sentenza Google Spain e Google, C-131/12, […] p.to 52).

36. Nel caso di specie, il trattamento controverso nel procedimento principale consiste, in particolare, nel pubblicare, sui siti Internet di annunci immobiliari della Weltimmo, dati personali relativi ai titolari di tali beni e, eventualmente, nell’utilizzare tali dati per esigenze di fatturazione degli annunci allo scadere del termine di un mese.

37. A tal proposito, occorre ricordare che, per quanto riguarda in particolare Internet, la Corte ha già avuto modo di constatare che l’operazione consistente nel far comparire su una pagina Internet dati personali va considerata come un «trattamento» ai sensi dell’art.2, lett.b), della direttiva 95/46 (v. sentenze Lindqvist, C-101/01, […], p.to 25, nonché Google Spain e Google, C-131/12, […], p.to 26).

38. Orbene, è indubbio che tale trattamento è avvenuto nel contesto delle attività, descritte al p.to 32 della presente sentenza, che la Weltimmo svolge in Ungheria.

39. Pertanto, fatte salve le verifiche rammentate al p.to 33 della presente sentenza, che spetta compiere al giudice del rinvio ai sensi dell’art.2, lett.b), della direttiva 96/46 consente, in una situazione quale quella controversa nel procedimento principale, l’applicazione del diritto ungherese in materia di protezione dei dati personali.

40. Il fatto che i titolari dei beni oggetto degli annunci immobiliari siano cittadini ungheresi, invece, non è assolutamente rilevante al fine di determinare il diritto nazionale applicabile al trattamento dei dati di cui è causa nel procedimento principale.

41. Tenuto conto di tutte le considerazioni che precedono, occorre rispondere alle questioni dalla prima alla sesta nei seguenti termini:

– l’art.4, §1, lett.a), della direttiva 95/46 deve essere interpretato nel senso che esso consente l’applicazione della legge in materia di protezione dei dati personali di uno Stato membro diverso da quello nel quale il responsabile del trattamento in Ungheria, occorre considerare che tale trattamento si svolge nel contesto delle attività di tale stabilimento e che l’art.4, §1, lett.a), della direttiva 96/46 consente, in una situazione quale quella controversa nel procedimento principale, l’applicazione del diritto ungherese in materia di protezione dei dati personali.

– per determinare se ciò si verifichi, in circostanze quali quelle controverso nel procedimento principale, il giudice del rinvio può tener conto, in particolare, del fatto, da un lato, che l’attività del responsabile del trattamento in Ungheria, occorre considerare che tale trattamento si svolge nel contesto delle attività di tale stabilimento, ai sensi dell’art.4, §1, lett.a), della direttiva 95/46, che svolge attività nel contesto delle quali è effettuato il trattamento dei dati personali interessati.

– è, invece, inconferente la questione della cittadinanza delle persone interessate da tale trattamento.

**Sulla settima questione**

42. La settima questione viene sottoposta soltanto nell’ipotesi in cui l’autorità ungherese di controllo consideri che la Weltimmo abbia, non in Ungheria, ma in un altro Stato membro, uno stabilimento, ai sensi dell’art.4, §1, lett.a), della direttiva 95/46, che svolge attività nel contesto delle quali è effettuato il trattamento dei dati personali interessati.

43. Con tale questione, il giudice del rinvio chiede, in sostanza, se, nel caso in cui l’autorità ungherese di controllo giungesse alla conclusione che il diritto applicabile al trattamento dei dati personali non è il diritto ungherese, ma il diritto di un altro Stato membro, l’art.28, §§1, 3 e 6, della direttiva 95/46 debba essere interpretato nel senso che detta autorità può esercitare soltanto i poteri previsti all’art.28, §3, di tale direttiva, conformemente al diritto tale altro Stato membro, e non può imporre sanzioni.

44. Per quanto attiene, in primo luogo, alla competenza di un’autorità di controllo ad agire in un simile caso, occorre rilevare che, in forza dell’art.28, §4, della direttiva 95/46, qualsiasi persona può presentare a ciascuna autorità di controllo, una domanda relativa alla tutela dei suoi diritti e libertà con riguardo al trattamento di dati personali.
45. Di conseguenza, in una situazione quale quella controversa nel procedimento principale, l’autorità ungherese di controllo può essere adatta da persone, quali gli inserzionisti di beni immobili di cui trattasi nel procedimento principale, che si ritengono vittime di un trattamento illegale dei dati personali che le riguardano nello Stato membro nel quale possiedono tali beni.

46. Occorre esaminare, in secondo luogo, quali siano i poteri di tale autorità di controllo alla luce dell’art.28, §§1, 3 e 6, della direttiva 95/46.

47. Si evince dall’art.28, §1, di tale direttiva che ciascuna autorità di controllo creato da uno Stato membro sorveglia, nel territorio di tale Stato membro, l’osservanza delle disposizioni di attuazione della direttiva 95/46, adottate dagli Stati membri.

48. In forza dell’art.28, §3, della direttiva 95/46, tali autorità di controllo dispongono in particolare di poteri investigativi, come il diritto di raccolta di qualsiasi informazione necessaria all’esercizio della loro funzione di controllo, e di poteri effettivi d’intervento come quello di ordinare il congelamento, la cancellazione o la distruzione dei dati, oppure di vietare a titolo provvisorio o definitivo un trattamento, ovvero quello di rivolgersi un avvertimento o un monito al responsabile del trattamento.

49. Tenuto conto della non tassatività dei poteri appena elencati e del tipo di poteri di intervento menzionati in tale disposizione, nonché del margine di manovra di cui dispongono gli Stati membri per il recepimento della direttiva 95/46, occorre considerare che tali poteri di intervento possono comprendere quello di sanzionare il responsabile del trattamento di dati, eventualmente imponendogli un’amenda.

50. I poteri conferiti alle autorità di controllo devono essere esercitati nel rispetto del diritto procedurale dello Stato membro cui esse appartengono.

51. Si evince dall’art.28, §§1 e 3, della direttiva 95/46 che ciascuna autorità di controllo esercita tutti i poteri che le sono stati conferiti nel territorio dello Stato membro cui appartiene, per assicurare in tale territorio il rispetto delle norme in materia di protezione dei dati.

52. Tale applicazione territoriale dei poteri di ciascuna autorità di controllo è conforme all’art.28, §6, di tale direttiva, ai sensi del quale ciascuna autorità di controllo è competente a esercitare, nel territorio del suo Stato membro, i poteri attribuiti a norma dell’art.28, §3, di detta direttiva e ciò indipendentemente dalla legge nazionale applicabile. Tale art.28, §6, precisa anche che ciascuna autorità può essere invitata ad esercitare i suoi poteri su domanda dell’autorità di un altro Stato membro e che le autorità di controllo collaborano tra loro nella misura necessaria allo svolgimento dei propri compiti, in particolare scambiandosi ogni informazione utile.

53. Tale disposizione è necessaria per garantire la libera circolazione dei dati personali in tutta l’Unione, continuando a sorvegliare il rispetto delle norme dirette a tutelare la vita privata delle persone fisiche di cui alla direttiva 95/46. Infatti, in mancanza di detta disposizione, nel caso in cui il responsabile del trattamento dei dati personali fosse soggetto alla legge di uno Stato membro, ma violasse il diritto alla tutela della vita privata delle persone fisiche in un altro Stato membro, in particolare rivolgendola la sua attività verso tale altro Stato membro senza però esservi stabilito, ai sensi di tale direttiva, sarebbe difficile, se non impossibile, per tali persone far rispettare il loro diritto a detta tutela.

54. Si evince quindi dall’art.28, §6, della direttiva 95/46 che l’autorità di controllo di uno Stato membro alla quale persone fisiche presentano un reclamo relativo al trattamento di dati personali che le riguardano, in base all’art.28, §4, di tale direttiva, può esaminare tale reclamo indipendentemente dalla legge applicabile e, di conseguenza, anche se il diritto applicabile al trattamento dei dati interessati è quello di un altro Stato membro.

55. Tuttavia, in tale ipotesi, i poteri di tale autorità non comprendono necessariamente tutti quelli di cui è investita secondo il diritto dello suo Stato membro.

56. Infatti, come rilevato dall’avvocato generale al §50 delle sue conclusioni, dalle esigenze derivanti dalla sovranità territoriale dello Stato membro, dal principio di legalità e dalla nozione di Stato di diritto discende che il potere sanzionatorio non può avere luogo, in linea di principio, al di fuori dei limiti legali entro cui un’autorità amministrativa è autorizzata ad agire secondo il diritto nazionale del suo Stato membro.

57. Così, quando ad un’autorità di controllo viene presentato un reclamo, secondo l’art.28, §4, della direttiva 95/46, essa può esercitare i suoi poteri investigativi indipendentemente dai diritto applicabile e ancor prima di sapere quale sia il diritto nazionale che si applica al trattamento controverso. Tuttavia, essa, qualora giunga alla conclusione che si applica il diritto di un altro Stato membro, non può imporre sanzioni al di fuori del territorio del suo Stato membro. In una situazione
del genere, essa è tenuta, in virtù dell’obbligo di collaborazione di cui all’art.28, §6, di tale direttiva, a chiedere all’autorità di controllo di tale altro Stato membro di accertare un’eventuale violazione di tale diritto e di imporre sanzioni se questo lo consente, appoggiandosi, se del caso, sulle informazioni che essa le avrà comunicato.

58. L’autorità di controllo cui è proposto un reclamo, nell’ambito di tale collaborazione può essere indotta a svolgere altre indagini, su istruzione dell’autorità di controllo dell’altro Stato membro.

59. Ne consegue che, in una situazione quale quella controversa nel procedimento principale, nell’ipotesi in cui il diritto applicabile sia quello di uno Stato membro diverso dall’Ungheria, l’autorità ungherese di controllo non potrebbe esercitare i poteri sanzionatori attribuiti dalla legge ungherese.

60. Risulta dalle considerazioni sopra esposte che occorre rispondere alla settima questione dichiarando che, nell’ipotesi in cui l’autorità di controllo di uno Stato membro cui sia proposto un reclamo, ai sensi dell’art.28, §4, della direttiva 95/46, giunga alla conclusione che il diritto applicabile al trattamento dei dati personali interessati non è il diritto di tale Stato membro, ma quello di un altro Stato membro, l’art.28, §§1, 3 e 6, di tale direttiva deve essere interpretato nel senso che tale autorità di controllo potrebbe esercitare i poteri effettivi d’intervento attribuiti in base all’art.28, §3, di detta direttiva solamente nel territorio del suo Stato membro. Pertanto, essa non può imporre sanzioni sulla base del diritto di tale Stato membro nei confronti del responsabile del trattamento di tali dati che non è stabilito in tale territorio, ma, secondo l’art.28, §6, della medesima direttiva, dovrebbe chiedere all’autorità di controllo dello Stato membro del quale si applica legge d’intervenire.

Per questi motivi, la Corte (Terza Sezione) dichiara:

1) L’art.4, §1, lett.a), della direttiva 95/46/CE […] del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, deve essere interpretato nel senso che esso consente l’applicazione della legge in materia di protezione dei dati personali di uno Stato membro diverso da quello nel quale il responsabile del trattamento di tali dati è registrato, purché il medesimo svolga, tramite un’organizzazione stabile nel territorio di tale Stato membro, un’attività effettiva e reale, anche minima, nel contesto della quale si svolge tale trattamento.

Per determinare se ciò si verifichi, in circostanze quali quelle controversa nel procedimento principale, il giudice del rinvio può tener conto, in particolare, del fatto, da un lato, che l’attività del responsabile di detto trattamento, nell’ambito della quale il medesimo ha luogo, consiste nella gestione di siti Internet di annunci immobiliari riguardanti beni immobili situati nel territorio di tale Stato membro e redatti nella lingua di quest’ultimo e che essa, di conseguenza, è principalmente, ovvero interamente, rivolta verso detto Stato membro e, dall’altro, che tale responsabile ha un rappresentante in detto Stato membro, il quale è incaricato di recuperare i crediti risultanti da tale attività nonché di rappresentarlo nei procedimenti amministrativo e giudiziario relativi al trattamento dei dati interessati.

È, invece, inconferente la questione della cittadinanza delle persone interessate da tale trattamento.

2) Nell’ipotesi in cui l’autorità di controllo di uno Stato membro cui sia proposto un reclamo, ai sensi dell’art.28, §4, della direttiva 95/46, giunga alla conclusione che il diritto applicabile al trattamento dei dati personali interessati non è il diritto di tale Stato membro, ma quello di un altro Stato membro, l’art.28, §§1, 3 e 6, di tale direttiva deve essere interpretato nel senso che tale autorità di controllo potrebbe esercitare i poteri effettivi d’intervento attribuiti in base all’art.28, §3, di detta direttiva solamente nel territorio del suo Stato membro. Pertanto, essa non può imporre sanzioni sulla base del diritto di tale Stato membro nei confronti del responsabile del trattamento di tali dati che non è stabilito in tale territorio, ma, secondo l’art.28, §6, della medesima direttiva, dovrebbe chiedere all’autorità di controllo dello Stato membro del quale si applica legge d’intervenire.

[...]
DISCUSSIONE

1. Quale è la nozione di “stabilimento” che deve essere applicata alla normativa in materia di protezione dei dati personali?

2. Qualora l’attività si basi anche su un sito Internet, quali sono gli elementi utili per verificare lo Stato di “stabilimento”?

3. Quali è il rapporto tra diritto applicabile e poteri delle autorità nazionali di controllo?
3. LE REGOLE DI INTERNET
3.1. Analogia, metafore, cyberspace

Supreme Court of California, 30 June 2003, n.S103781 (Intel v. Hamidi)

[...]

Hamidi, a former Intel engineer, together with others, formed an organization named Former and Current Employees of Intel (FACE-Intel) to disseminate information and views critical of Intel's employment and personnel policies and practices. FACE-Intel maintained a website (which identified Hamidi as webmaster and as the organization's spokesperson) containing such material. In addition, over a 21-month period Hamidi, on behalf of FACE-Intel, sent six mass e-mails to employee addresses on Intel's electronic mail system. The messages criticized Intel's employment practices, warned employees of the dangers those practices posed to their careers, suggested employees consider moving to other companies, solicited employees' participation in FACE-Intel, and urged employees to inform themselves further by visiting FACE-Intel's website. The messages stated that recipients could, by notifying the sender of their wishes, be removed from FACE-Intel's mailing list; Hamidi did not subsequently send messages to anyone who requested removal.

Each message was sent to thousands of addresses (as many as 35,000 according to FACE-Intel's website), though some messages were blocked by Intel before reaching employees. Intel's attempt to block internal transmission of the messages succeeded only in part; Hamidi later admitted he evaded blocking efforts by using different sending computers. When Intel, in March 1998, demanded in writing that Hamidi and FACE-Intel stop sending e-mails to Intel's computer system, Hamidi asserted the organization had a right to communicate with willing Intel employees; he sent a new mass mailing in September 1998.

The summary judgment record contains no evidence Hamidi breached Intel's computer security in order to obtain the recipient addresses for his messages; indeed, internal Intel memoranda show the company's management concluded no security breach had occurred. Hamidi stated he created the recipient address list using an Intel directory on a floppy disk anonymously sent to him. Nor is there any evidence that the receipt or internal distribution of Hamidi's electronic messages damaged Intel's computer system or slowed or impaired its functioning. Intel did present uncontradicted evidence, however, that many employee recipients asked a company official to stop the messages and that staff time was consumed in attempts to block further messages from FACE-Intel. According to the FACE-Intel website, moreover, the messages had prompted discussions between "[e]xcited and nervous managers" and the company's human resources department.

Intel sued Hamidi and FACE-Intel, pleading causes of action for trespass to chattels and nuisance, and seeking both actual damages and an injunction against further e-mail messages. Intel later voluntarily dismissed its nuisance claim and waived its demand for damages.

[...]

Discussion
I. Current California Tort Law
[...]

Relying on a line of decisions, most from federal district courts, applying the tort of trespass to chattels to various types of unwanted electronic contact between computers, Intel contends that, while its computers were not damaged by receiving Hamidi's messages, its interest in the "physical condition, quality or value" [...] of the computers was harmed. We disagree. The cited line of decisions does not persuade us that the mere sending of electronic communications that assertedly cause injury only because of their contents constitutes an actionable trespass to a computer system through which the messages are transmitted. Rather, the decisions finding electronic contact to be a trespass to computer systems have generally involved some actual or threatened interference with the computers' functioning.

[...]

A series of federal district court decisions held that sending UCE through an ISP's equipment may constitute trespass to the ISP's computer system. The lead case, CompuServe, Inc. v. Cyber Promotions, Inc., [...] was followed by Hotmail Corp. v. Van$h Money Pie, Inc. [...], America Online, Inc. v. IMS [...], and America Online, Inc. v. LCGM, Inc. [...].
In each of these spamming cases, the plaintiff showed, or was prepared to show, some interference with the efficient functioning of its computer system. In CompuServe, the plaintiff ISP's mail equipment monitor stated that mass UCE mailings, especially from nonexistent addresses such as those used by the defendant, placed "a tremendous burden" on the ISP's equipment, using "disk space and drain[ing] the processing power," making those resources unavailable to serve subscribers [...]. Similarly, in Hotmail Corp. v. Van$ Money Pie, Inc., [...], the Court found the evidence supported a finding that the defendant's mailings "fill[ed] up Hotmail's computer storage space and threaten[ed] to damage Hotmail's ability to service its legitimate customers". [...] That Intel does not claim the type of functional impact that spammers and robots have been alleged to cause is not surprising in light of the differences between Hamidi's activities and those of a commercial enterprise that uses sheer quantity of messages as its communications strategy. Though Hamidi sent thousands of copies of the same message on six occasions over 21 months, that number is minuscule compared to the amounts of mail sent by commercial operations. The individual advertisers sued in America Online, Inc. v. IMS, [...], and America Online, Inc. v. LCGM, Inc., [...], were alleged to have sent more than 60 million messages over 10 months and more than 92 million messages over seven months, respectively. Collectively, UCE has reportedly come to constitute about 45 percent of all e-mail [...]. The functional burden on Intel's computers, or the cost in time to individual recipients, of receiving Hamidi's occasional advocacy messages cannot be compared to the burdens and costs caused ISP's and their customers by the ever-rising deluge of commercial e-mail. [...] In addition to impairment of system functionality, CompuServe and its progeny also refer to the ISP's loss of business reputation and customer goodwill, resulting from the inconvenience and cost that spam mailings to its customers, as harm to the ISP's legally protected interests in its personal property [...] Intel argues that its own interest in employee productivity, assertedly disrupted by Hamidi's messages, is a comparable protected interest in its computer system. We disagree. [...] CompuServe's customers were annoyed because the system was inundated with unsolicited commercial messages, making its use for personal communication more difficult and costly [...]. Their complaint, which allegedly led some to cancel their CompuServe service, was about the functioning of CompuServe's electronic mail service. Intel's workers, in contrast, were allegedly distracted from their work not because of the frequency or quantity of Hamidi's messages, but because of assertions and opinions the messages conveyed. Intel's complaint is thus about the contents of the messages rather than the functioning of the company's e-mail system. Even accepting CompuServe's economic injury rationale, therefore, Intel's position represents a further extension of the trespass to chattels tort, fictionally recharacterizing the allegedly injurious effect of a communication's contents on recipients as an impairment to the device which transmitted the message. [...] Intel's theory would expand the tort of trespass to chattels to cover virtually any unconsented-to communication that, solely because of its content, is unwelcome to the recipient or intermediate transmitter [...]. While unwelcome communications, electronic or otherwise, can cause a variety of injuries to economic relations, reputation and emotions, those interests are protected by other branches of tort law; in order to address them, we need not create a fiction of injury to the communication system. Nor may Intel appropriately assert a property interest in its employees' time. [...] Whatever interest Intel may have in preventing its employees from receiving disruptive communications, it is not an interest in personal property, and trespass to chattels is therefore not an action that will lie to protect it. Nor, finally, can the fact Intel staff spent time attempting to block Hamidi's messages be bootstrapped into an injury to Intel's possessor interest in its computers. [...] Intel connected its e-mail system to the Internet and permitted its employees to make use of this connection both for business and, to a reasonable extent, for their own purposes. In doing so, the company necessarily contemplated the employees' receipt of unsolicited as well as solicited communications from other companies and individuals. That some communications would, because of their contents, be unwelcome to Intel management was virtually inevitable. Hamidi did nothing but use the e-mail system for its intended purpose - to communicate with employees. The
system worked as designed, delivering the messages without any physical or functional harm or disruption. These occasional transmissions cannot reasonably be viewed as impairing the quality or value of Intel's computer system. We conclude, therefore, that Intel has not presented undisputed facts demonstrating an injury to its personal property, or to its legal interest in that property, that support, under California tort law, an action for trespass to chattels.

II. Proposed Extension of California Tort Law

We next consider whether California common law should be extended to cover, as a trespass to chattels, an otherwise harmless electronic communication whose contents are objectionable. We decline to so expand California law. […]

Writing on behalf of several industry groups appearing as amici curiae, Professor Richard A. Epstein […] urges us to excuse the required showing of injury to personal property in cases of unauthorized electronic contact between computers, "extending the rules of trespass to real property to all interactive Web sites and servers". The court is thus urged to recognize, for owners of a particular species of personal property, computer servers, the same interest in inviolability as is generally accorded a possessor of land. In effect, Professor Epstein suggests that a company's server should be its castle, upon which any unauthorized intrusion, however harmless, is a trespass.

Epstein's argument derives, in part, from the familiar metaphor of the Internet as a physical space, reflected in much of the language that has been used to describe it: "cyberspace," "the information superhighway," e-mail "addresses," and the like. Of course, the Internet is also frequently called simply the "Net," a term, Hamidi points out, "evoking a fisherman's chattel". A major component of the Internet is the World Wide "Web," a descriptive term suggesting neither personal nor real property, and "cyberspace" itself has come to be known by the oxymoronic phrase "virtual reality," which would suggest that any real property "located" in "cyberspace" must be "virtually real" property. Metaphor is a two-edged sword.

Indeed, the metaphorical application of real property rules would not, by itself, transform a physically harmless electronic intrusion on a computer server into a trespass. That is because, under California law, intangible intrusions on land, including electromagnetic transmissions, are not actionable as trespasses (though they may be as nuisances) unless they cause physical damage to the real property. (San Diego Gas & Electric Co. v. Superior Court […] Since Intel does not claim Hamidi's electronically transmitted messages physically damaged its servers, it could not prove a trespass to land even were we to treat the computers as a type of real property. Some further extension of the concept would be required, under which the electronic signals Hamidi sent would be recast as tangible intruders, perhaps as tiny messengers rushing through the "hallways" of Intel's computers and bursting out of employees' computers to read them Hamidi's missives. But such fictions promise more confusion than clarity in the law […].

The plain fact is that computers, even those making up the Internet, are - like such older communications equipment as telephones and fax machines - personal property, not realty. Professor Epstein observes that "although servers may be moved in real space, they cannot be moved in cyberspace," because an Internet server must, to be useful, be accessible at a known address. But the same is true of the telephone: to be useful for incoming communication, the telephone must remain constantly linked to the same number (or, when the number is changed, the system must include some forwarding or notification capability, a qualification that also applies to computer addresses). Does this suggest that an unwelcome message delivered through a telephone or fax machine should be viewed as a trespass to a type of real property? We think not: as already discussed, the contents of a telephone communication may cause a variety of injuries and may be the basis for a variety of tort actions (e.g., defamation, intentional infliction of emotional distress, invasion of privacy), but the injuries are not to an interest in property, much less real property, and the appropriate tort is not trespass.

More substantively, Professor Epstein argues that a rule of computer server inviolability will, through the formation or extension of a market in computer-to-computer access, create "the right social result". In most circumstances, he predicts, companies with computers on the Internet will continue to authorize transmission of information through e-mail, website searching, and page linking because they benefit by that open access. When a website owner does deny access to a particular sending, searching, or linking computer, a system of "simple one-on-one negotiations" will arise to provide the necessary individual licenses.
Other scholars are less optimistic about such a complete propertization of the Internet. Professor Mark Lemley [...], writing on behalf of an *amicus curiae* group of professors of intellectual property and computer law, observes that under a property rule of server inviolability, "*each of the hundreds of millions of [Internet] users must get permission in advance from anyone with whom they want to communicate and anyone who owns a server through which their message may travel*". The consequence for e-mail could be a substantial reduction in the freedom of electronic communication, as the owner of each computer through which an electronic message passes could impose its own limitations on message content or source. […]

[...] A leading scholar of Internet law and policy, Professor Lawrence Lessig [...], has criticized Professor Epstein's theory of the computer server as quasi-real property, previously put forward in the *eBay* case […], on the ground that it ignores the costs to society in the loss of network benefits […].

We discuss this debate among the *amicus curiae* and academic writers only to note its existence and contours, not to attempt its resolution. Creating an absolute property right to exclude undesired communications from one's e-mail and web servers might help force spammers to internalize the costs they impose on ISP's and their customers. But such a property rule might also create substantial new costs, to e-mail and e-commerce users and to society generally, in lost ease and openness of communication and in lost network benefits. In light of the unresolved controversy, we would be acting rashly to adopt a rule treating computer servers as real property for purposes of trespass law.

The Legislature has already adopted detailed regulations governing UCE […]. It may see fit in the future also to regulate non-commercial e-mail, such as that sent by Hamidi, or other kinds of unwanted contact between computers on the Internet […]. But we are not persuaded that these perceived problems call at present for judicial creation of a rigid property rule of computer server inviolability. We therefore decline to create an exception, covering Hamidi's unwanted electronic messages to Intel employees, to the general rule that a trespass to chattels is not actionable if it does not involve actual or threatened injury to the personal property or to the possessor's legally protected interest in the personal property. No such injury having been shown on the undisputed facts, Intel was not entitled to summary judgment in its favor.

**DISCUSSIONE**

1. *Quali tipi di comunicazione, per mezzo e per contenuto, erano inviate da Hamidi?*
2. *In cosa consiste il trespass to chattels e su quali basi è stato richiamato da Intel?*
3. *Intel ha subito un danno in conseguenza delle azioni di Hamidi? Di che tipo?*
   *Perché?*
5. *Le e-mail di Hamidi potevano essere considerate come spam?*
6. *Secondo la Corte suprema della California sarebbe stato auspicabile estendere l’ambito del trespass to chattels per includervi la fattispecie in esame? Perché?*
7. *Quali sono le alternative?*
8. *Quali sono le metafore discusse nella sentenza? Quali sono i possibili effetti dell’uso di tali metafore?*
9. *Quale è il ruolo dell’analogia in un ordinamento giuridico? Quali i limiti?*
10. *Quali sono i vantaggi e gli svantaggi dell’uso dell’analogia, nel diritto, ma anche al di fuori del diritto (con l’uso di metafore)?*
3.2. Reati commessi a mezzo Internet e analogie

Corte di Cassazione, sez. I penale, 28 aprile 2015, n.24431

[...], ritenuto in fatto e considerato in diritto

1. Il 18 luglio 2013 il Giudice di pace di Roma, chiamato a giudicare una fattispecie diffamatoria, dichiarava la sua incompetenza per materia a decidere in ordine al reato di cui all'art.595 c.p., comma 3, precisando che, ancorché non contestata, quella al suo esame integrava fattispecie aggravata ai sensi del terzo comma della norma incriminatrice.

Il Tribunale di Roma, monocraticamente composto, non ritenendo configurabile l'aggravante viceversa considerata dal giudice di pace sul rilievo che postare un commento sulla bacheca Facebook della p.o. non implica pubblicazione né diffusione del relativo contenuto offensivo, possibile soltanto se non attivati, dalla stessa p.o., meccanismi di protezione della privacy, declinava anch'esso la propria competenza a giudicare della fattispecie dedotta in favore del Giudice di pace di Roma e rimetteva pertanto gli atti alla Corte di Cassazione per la risoluzione del conflitto.

2. Il conflitto sussiste, in quanto due giudici ordinari, contemporaneamente, ricusano di giudicare in ordine alla medesima vicenda giurisdizionale, dando così luogo a quella situazione di stallo processuale prevista dall'art.28 c.p.p., la cui risoluzione è demandata a questa Corte dalla norme successive.

Tanto premesso ritiene il Collegio che competente a conoscere del fatto dedotto in giudizio è il Tribunale di Roma, in composizione monocratica.


È pur vero che la fattispecie dedotta si appalesa sotto più profili diversa da quelle delibate dalla Corte con i citati arresti, giacché diverso l'utilizzo di internet, di cui si è occupato il giudice di legittimità, da quello relativo ad una bacheca Facebook, ma v'è tra esse, e non solo perché in entrambi i casi v'è l'applicazione di risorse informatiche, un decisivo fondamento comune.

Ed infatti, il reato tipizzato al terzo comma dell'art.595 c.p. quale ipotesi aggravata del delitto di diffamazione trova il suo fondamento nella potenzialità, nella idoneità e nella capacità del mezzo utilizzato per la consumazione del reato a coinvolgere e raggiungere una pluralità di persone, ancorché non individuate nello specifico ed apprezzabili soltanto in via potenziale, con ciò cagionando un maggiore e più diffuso danno alla persona offesa. D'altra parte lo strumento principe della fattispecie criminosa in esame è quello della stampa, al quale il codificatore ha giustapposto "qualsiasi altro mezzo di pubblicità", giacché anche in questo caso, per definizione, si determina una diffusione dell'offesa ed in tale tipologia, quella appunto del mezzo di pubblicità, ha fatto rientrare la lezione ermeneutica della corte, ad esempio, un pubblico comizio (sez.V, n.9384 del 28 maggio 1998, Forzano, […] ovvero (sez.V, 6 aprile 2011, n.29221 […] l'utilizzo, al fine di inviare un messaggio, della posta elettronica secondo le modalità del "forward" e cioè verso una pluralità di destinatari. Detti arresti risultano infatti argomentati con il rilievo che, sia un comizio che la posta elettronica, vanno considerati mezzi di pubblicità, giacché idonei a provocare una ampia e indiscriminata diffusione della notizia tra un numero indeterminato di persone.

Tornando ora, come di necessità, alla fattispecie dedotta, osserva il Collegio che anche la diffusione di un messaggio con le modalità consentite dall'utilizzo per questo di una bacheca Facebook, ha potenzialmente la capacità di raggiungere un numero indeterminato di persone, sia perché, per comune esperienza, bacheche di tal natura racchioduo un numero apprezzabile di persone (senza le quali la bacheca Facebook non avrebbe senso), sia perché l'utilizzo di Facebook integra una delle modalità attraverso le quali gruppi di soggetti socializzano le rispettive esperienze di vita, valorizzando in primo luogo il rapporto interpersonale, che, proprio per il mezzo
utilizzato, assume il profilo del rapporto interpersonale allargato ad un gruppo indeterminato di aderenti al fine di una costante socializzazione.

Identificata nei termini detti, la condotta di postare un commento sulla bacheca facebook realizza, pertanto, la pubblicizzazione e la diffusione di esso, per la idoneità del mezzo utilizzato a determinare la circolazione del commento tra un gruppo di persone comunque apprezzabile per composizione numerica, di guisa che, se offensivo tale commento, la relativa condotta rientra nella tipizzazione codicistica descritta dal terzo comma dell’art.595 c.p..<

[...]

P.Q.M.
la Corte dichiara la competenza del Tribunale di Roma, cui dispone trasmettersi gli atti.

[...]

*****

DISCUSSIONE

1. Quale analogia è stata utilizzata per la posta elettronica? Sulla base di quali considerazioni? Vi convince?
2. Quale analogia è stata utilizzata per la bacheca Facebook? Sulla base di quali considerazioni? Vi convince?
3. Sono possibili distinzioni nell’ambito della pubblicazione di contenuti su una bacheca Facebook? Se sì, possono essere giuridicamente rilevanti?
4. Quale è il ruolo dell’analogia in un ordinamento giuridico? Quali i limiti?
5. Quali sono i vantaggi e gli svantaggi dell’uso dell’analogia, nel diritto, ma anche al di fuori del diritto (con l’uso di metafore)?

*****

NORME

- art.595 c.p.
Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.

We have no elected government, nor are we likely to have one, so I address you with no greater authority than that with which liberty itself always speaks. I declare the global social space we are building to be naturally independent of the tyrannies you seek to impose on us. You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear.

Governments derive their just powers from the consent of the governed. You have neither solicited nor received ours. We did not invite you. You do not know us, nor do you know our world. Cyberspace does not lie within your borders. Do not think that you can build it, as though it were a public construction project. You cannot. It is an act of nature and it grows itself through our collective actions.

You have not engaged in our great and gathering conversation, nor did you create the wealth of our marketplaces. You do not know our culture, our ethics, or the unwritten codes that already provide our society more order than could be obtained by any of your impositions.

You claim there are problems among us that you need to solve. You use this claim as an excuse to invade our precincts. Many of these problems don't exist. Where there are real conflicts, where there are wrongs, we will identify them and address them by our means. We are forming our own Social Contract. This governance will arise according to the conditions of our world, not yours. Our world is different.

Cyberspace consists of transactions, relationships, and thought itself, arrayed like a standing wave in the web of our communications. Ours is a world that is both everywhere and nowhere, but it is not where bodies live.

We are creating a world that all may enter without privilege or prejudice accorded by race, economic power, military force, or station of birth.

We are creating a world where anyone, anywhere may express his or her beliefs, no matter how singular, without fear of being coerced into silence or conformity.

Your legal concepts of property, expression, identity, movement, and context do not apply to us. They are based on matter, and there is no matter here.

Our identities have no bodies, so, unlike you, we cannot obtain order by physical coercion. We believe that from ethics, enlightened self-interest, and the commonweal, our governance will emerge. Our identities may be distributed across many of your jurisdictions. The only law that all our constituent cultures would generally recognize is the Golden Rule. We hope we will be able to build our particular solutions on that basis. But we cannot accept the solutions you are attempting to impose.

In the United States, you have today created a law, the Telecommunications Reform Act, which repudiates your own Constitution and insults the dreams of Jefferson, Washington, Mill, Madison, De Tocqueville, and Brandeis. These dreams must now be born anew in us.

You are terrified of your own children, since they are natives in a world where you will always be immigrants. Because you fear them, you entrust your bureaucracies with the parental responsibilities you are too cowardly to confront yourselves. In our world, all the sentiments and expressions of humanity, from the debasing to the angelic, are parts of a seamless whole, the global conversation of bits. We cannot separate the air that chokes from the air upon which wings beat.

In China, Germany, France, Russia, Singapore, Italy and the United States, you are trying to ward off the virus of liberty by erecting guard posts at the frontiers of Cyberspace. These may keep out the contagion for a small time, but they will not work in a world that will soon be blanketeted in bit-bearing media.

Your increasingly obsolete information industries would perpetuate themselves by proposing laws, in America and elsewhere, that claim to own speech itself throughout the world. These laws
would declare ideas to be another industrial product, no more noble than pig iron. In our world, whatever the human mind may create can be reproduced and distributed infinitely at no cost. The global conveyance of thought no longer requires your factories to accomplish.

These increasingly hostile and colonial measures place us in the same position as those previous lovers of freedom and self-determination who had to reject the authorities of distant, uninformed powers. We must declare our virtual selves immune to your sovereignty, even as we continue to consent to your rule over our bodies. We will spread ourselves across the Planet so that no one can arrest our thoughts.

We will create a civilization of the Mind in Cyberspace. May it be more humane and fair than the world your governments have made before.

_Davos, Switzerland, February 8, 1996_

*****

**DISCUSSIONE**

1. _Quale pensate sia il valore di questo documento?_
2. _Cosa è il cyberspace? Cyberspace e Internet sono sinonimi?_
3. _L’indipendenza del cyberspace dai Governi nazionali e dalle organizzazioni internazionali è possibile? Perché?_
4. _La Rete può essere anarchica? In caso negativo, quali sono le regole che la governano? Come sono generate?_
5. _Quali sono le dinamiche che portano una comunità a individuare regole? Quali sono state, o sono, quelle relative alla Rete?_
3.4. Le norme sociali

RFC 1855 – Netiquette guidelines, 28 October 1995

Status of This Memo
This memo provides information for the Internet community. This memo does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

Abstract
This document provides a minimum set of guidelines for Network Etiquette (Netiquette) which organizations may take and adapt for their own use. As such, it is deliberately written in a bulleted format to make adaptation easier and to make any particular item easy (or easier) to find. It also functions as a minimum set of guidelines for individuals, both users and administrators. This memo is the product of the Responsible Use of the Network (RUN) Working Group of the IETF.

1.0 Introduction
In the past, the population of people using the Internet had "grown up" with the Internet, were technically minded, and understood the nature of the transport and the protocols. Today, the community of Internet users includes people who are new to the environment. These "Newbies" are unfamiliar with the culture and don't need to know about transport and protocols. In order to bring these new users into the Internet culture quickly, this Guide offers a minimum set of behaviors which organizations and individuals may take and adapt for their own use. Individuals should be aware that no matter who supplies their Internet access, be it an Internet Service Provider through a private account, or a student account at a University, or an account through a corporation, that those organizations have regulations about ownership of mail and files, about what is proper to post or send, and how to present yourself. Be sure to check with the local authority for specific guidelines.

2.0 One-to-One Communication (electronic mail, talk)
We define one-to-one communications as those in which a person is communicating with another person as if face-to-face: a dialog. In general, rules of common courtesy for interaction with people should be in force for any situation and on the Internet it's doubly important where, for example, body language and tone of voice must be inferred [...].

2.1 User Guidelines
2.1.1 For mail
- Unless you have your own Internet access through an Internet provider, be sure to check with your employer about ownership of electronic mail. Laws about the ownership of electronic mail vary from place to place.
- Unless you are using an encryption device (hardware or software), you should assume that mail on the Internet is not secure. Never put in a mail message anything you would not put on a postcard.
- Respect the copyright on material that you reproduce. Almost every country has copyright laws.
- If you are forwarding or re-posting a message you've received, do not change the wording. If the message was a personal message to you and you are re-posting to a group, you should ask permission first. You may shorten the message and quote only relevant parts, but be sure you give proper attribution.
- Never send chain letters via electronic mail. Chain letters are forbidden on the Internet. Your network privileges will be revoked. Notify your local system administrator if you ever receive one.
- A good rule of thumb: Be conservative in what you send and liberal in what you receive. You should not send heated messages (we call these "flames") even if you are provoked. On the other hand, you shouldn't be surprised if you get flamed and it's prudent not to respond to flames.
- Make things easy for the recipient. Many mailers strip header information which includes your return address. In order to ensure that people know who you are, be sure to include a line or two at the end of your message with contact information. You can create this file ahead of time and add it to the end of your messages. (Some mailers do this automatically). In Internet parlance, this is known as a ".sig" or "signature" file. Your .sig file takes the place of your business card. (And you can have more than one to apply in different circumstances).

- Watch cc’s when replying. Don’t continue to include people if the messages have become a 2-way conversation.

- Remember that the recipient is a human being whose culture, language, and humor have different points of reference from your own. Remember that date formats, measurements, and idioms may not travel well. Be especially careful with sarcasm.

- Use mixed case. UPPER CASE LOOKS AS IF YOU'RE SHOUTING.

- Use symbols for emphasis. That *is* what I meant. Use underscores for underlining. _War and Peace_ is my favourite book.

- Use smileys to indicate tone of voice, but use them sparingly. :-) is an example of a smiley (Look sideways). Don’t assume that the inclusion of a smiley will make the recipient happy with what you say or wipe out an otherwise insulting comment.

- Wait overnight to send emotional responses to messages. If you have really strong feelings about a subject, indicate it via FLAME ON/OFF enclosures. For example: FLAME ON: This type of argument is not worth the bandwidth it takes to send it. It’s illogical and poorly reasoned. The rest of the world agrees with me. FLAME OFF

- Be brief without being overly terse. When replying to a message, include enough original material to be understood but no more. It is extremely bad form to simply reply to a message by including all the previous message: edit out all the irrelevant material.

- Limit line length to fewer than 65 characters and end a line with a carriage return.

- Mail should have a subject heading which reflects the content of the message.

- If you include a signature keep it short. Rule of thumb is no longer than 4 lines. Remember that many people pay for connectivity by the minute, and the longer your message is, the more they pay.

- Just as mail (today) may not be private, mail (and news) are (today) subject to forgery and spoofing of various degrees of detectability. Apply common sense "reality checks" before assuming a message is valid.

- If you think the importance of a message justifies it, immediately reply briefly to an e-mail message to let the sender know you got it, even if you will send a longer reply later.

- "Reasonable" expectations for conduct via e-mail depend on your relationship to a person and the context of the communication. Norms learned in a particular e-mail environment may not apply in general to your e-mail communication with people across the Internet. Be careful with slang or local acronyms.

- The cost of delivering an e-mail message is, on the average, paid about equally by the sender and the recipient (or their organizations). This is unlike other media such as physical mail, telephone, TV, or radio. Sending someone mail may also cost them in other specific ways like network bandwidth, disk space or CPU usage. This is a fundamental economic reason why unsolicited e-mail advertising is unwelcome (and is forbidden in many contexts).

- Know how large a message you are sending. Including large files such as Postscript files or programs may make your message so large that it cannot be delivered or at least consumes excessive resources. A good rule of thumb would be not to send a file larger than 50 Kilobytes. Consider file transfer as an alternative, or cutting the file into smaller chunks and sending each as a separate message.

2.1.2 For talk

Talk is a set of protocols which allow two people to have an interactive dialogue via computer.

- Use mixed case and proper punctuation, as though you were typing a letter or sending mail.
Always say goodbye, or some other farewell, and wait to see a farewell from the other person before killing the session. This is especially important when you are communicating with someone a long way away. Remember that your communication relies on both bandwidth (the size of the pipe) and latency (the speed of light).

- Remember that talk is an interruption to the other person. Only use as appropriate. And never talk to strangers.
- The reasons for not getting a reply are many. Don’t assume that everything is working correctly. Not all versions of talk are compatible.

- Talk shows your typing ability. If you type slowly and make mistakes when typing it is often not worth the time of trying to correct, as the other person can usually see what you meant.
- Be careful if you have more than one talk session going!

3.0 One-to-Many Communication (Mailing Lists, NetNews)

Any time you engage in One-to-Many communications, all the rules for mail should also apply. After all, communicating with many people via one mail message or post is quite analogous to communicating with one person with the exception of possibly offending a great many more people than in one-to-one communication. Therefore, it’s quite important to know as much as you can about the audience of your message.

3.1 User Guidelines

3.1.1 General Guidelines for mailing lists and NetNews

- Read both mailing lists and newsgroups for one to two months before you post anything. This helps you to get an understanding of the culture of the group.

- Consider that a large audience will see your posts. That may include your present or your next boss. Take care in what you write. Remember too, that mailing lists and News groups are frequently archived, and that your words may be stored for a very long time in a place to which many people have access.
- Assume that individuals speak for themselves, and what they say does not represent their organization (unless stated explicitly).
- Remember that both mail and news take system resources. Pay attention to any specific rules covering their uses your organization may have.
- Messages and articles should be brief and to the point. Don’t wander off-topic, don’t ramble and don’t send mail or post messages solely to point out other people’s errors in typing or spelling. These, more than any other behavior, mark you as an immature beginner.

- Advertising is welcomed on some lists and Newsgroups, and abhorred on others! This is another example of knowing your audience before you post. Unsolicited advertising which is completely off-topic will most certainly guarantee that you get a lot of hate mail.

- Don’t get involved in flame wars. Neither post nor respond to incendiary material.

- There are Newsgroups and Mailing Lists which discuss topics of wide varieties of interests. These represent a diversity of lifestyles, religions, and cultures. Posting articles or sending messages to a group whose point of view is offensive to you simply to tell them they are offensive is not acceptable.

Sexually and racially harassing messages may also have legal implications. There is software available to filter items you might find objectionable.

3.1.2 Mailing List Guidelines

- The auto-reply feature of many mailers is useful for in-house communication, but quite annoying when sent to entire mailing lists. Examine "Reply-To" addresses when replying to messages from lists. Most auto-replies will go to all members of the list.
- Consider unsubscribing or setting a "nomail" option (when it’s available) when you cannot check your mail for an extended period.
4.1 User Guidelines

4.1.1. General guidelines
- Remember that all these services belong to someone else. The people who pay the bills get to make the rules governing usage. Information may be free - or it may not be! Be sure you check.

[...]

4.1.2 Real Time Interactive Services Guidelines (MUDs MOOs IRC)
- As in other environments, it is wise to "listen" first to get to know the culture of the group.
- It's not necessary to greet everyone on a channel or room personally. Usually one "Hello" or the equivalent is enough. Using the automation features of your client to greet people is not acceptable behavior.
[...]
- Don’t assume that people who you don’t know will want to talk to you. If you feel compelled to send private messages to people you don’t know, then be willing to accept gracefully the fact that they might be busy or simply not want to chat with you.
- Respect the guidelines of the group. Look for introductory materials for the group. These may be on a related ftp site.
- Don’t badger other users for personal information such as sex, age, or location. After you have built an acquaintance with another user, these questions may be more appropriate, but many people hesitate to give this information to people with whom they are not familiar.
- If a user is using a nickname alias or pseudonym, respect that user’s desire for anonymity. Even if you and that person are close friends, it is more courteous to use his nickname. Do not use that person’s real name on-line without permission.
[...]

*****

DISCUSSIONE

1. Che valore ha la Netiquette? Cosa rappresenta?
2. Quali pensate siano gli aspetti ancora attuali, quali quelli ormai superati e quali le lacune?
3. Quali “norme” vi hanno sorpreso?
4. Quali norme non seguite nella vostra esperienza on-line?
5. Pensate che la Netiquette possa essere ancora utile, che dovrebbe essere aggiornata o che ormai abbia perso ogni utilità?
3.5. Internet e principi

Dichiarazione dei diritti in Internet (Camera dei Deputati, luglio 2015)

Preambolo

Internet ha contribuito in maniera decisiva a ridefinire lo spazio pubblico e privato, a strutturare i rapporti tra le persone e tra queste e le Istituzioni. Ha cancellato confini e ha costruito modalità nuove di produzione e utilizzazione della conoscenza. Ha ampliato le possibilità di intervento diretto delle persone nella sfera pubblica. Ha modificato l’organizzazione del lavoro. Ha consentito lo sviluppo di una società più aperta e libera. Internet deve essere considerata come una risorsa globale e che risponde al criterio della universalità.

L’Unione Europea è oggi la regione del mondo dove è più elevata la tutela costituzionale dei dati personali, esplicitamente riconosciuta dall’art.8 della Carta dei diritti fondamentali, che costituisce il riferimento necessario per una specificazione dei principi riguardanti il funzionamento di Internet, anche in una prospettiva globale.

Questa Dichiarazione dei diritti in Internet è fondata sul pieno riconoscimento di libertà, eguaglianza, dignità e diversità di ogni persona. La garanzia di questi diritti è condizione necessaria perché sia assicurato il funzionamento democratico delle Istituzioni, e perché si eviti il prevalere di poteri pubblici e privati che possano portare ad una società della sorveglianza, del controllo e della selezione sociale. Internet si configura come uno spazio sempre più importante per l’autorganizzazione delle persone e dei gruppi e come uno strumento essenziale per promuovere la partecipazione individuale e collettiva ai processi democratici e l’eguaglianza sostanziale.

I principi riguardanti Internet tengono conto anche del suo configurarsi come uno spazio economico che rende possibili innovazione, corretta competizione e crescita in un contesto democratico.

Una Dichiarazione dei diritti di Internet è strumento indispensabile per dare fondamento costituzionale a principi e diritti nella dimensione sovranazionale.

Art.1 (Riconoscimento e garanzia dei diritti)

1. Sono garantiti in Internet i diritti fondamentali di ogni persona riconosciuti dalla Dichiarazione universale dei diritti umani delle Nazioni Unite, dalla Carta dei diritti fondamentali dell’Unione Europea, dalle costituzioni nazionali e dalle dichiarazioni internazionali in materia.

2. Tali diritti devono essere interpretati in modo da assicurarne l’effettività nella dimensione della Rete.

3. Il riconoscimento dei diritti in Internet deve essere fondato sul pieno rispetto della dignità, della libertà, dell’eguaglianza e della diversità di ogni persona, che costituiscono i principi in base ai quali si effettua il bilanciamento con altri diritti.

Art.2 (Diritto di accesso)

1. L’accesso ad Internet è diritto fondamentale della persona e condizione per il suo pieno sviluppo individuale e sociale.

2. Ogni persona ha eguale diritto di accedere a Internet in condizioni di parità, con modalità tecnologicamente adeguate e aggiornate che rimuovano ogni ostacolo di ordine economico e sociale.

3. Il diritto fondamentale di accesso a Internet deve essere assicurato nei suoi presupposti sostanziali e non solo come possibilità di collegamento alla Rete.

4. L’accesso comprende la libertà di scelta per quanto riguarda dispositivi, sistemi operativi e applicazioni anche distribuite.

5. Le Istituzioni pubbliche garantiscono i necessari interventi per il superamento di ogni forma di divario digitale tra cui quelli determinati dal genere, dalle condizioni economiche oltre che da situazioni di vulnerabilità personale e disabilità.

Art.3 (Diritto alla conoscenza e all’educazione in rete)
1. Le istituzioni pubbliche assicurano la creazione, l'uso e la diffusione della conoscenza in rete intesa come bene accessibile e fruibile da parte di ogni soggetto.

2. Debbono essere presi in considerazione i diritti derivanti dal riconoscimento degli interessi morali e materiali legati alla produzione di conoscenze.

3. Ogni persona ha diritto ad essere posta in condizione di acquisire e di aggiornare le capacità necessarie ad utilizzare Internet in modo consapevole per l'esercizio dei propri diritti e delle proprie libertà fondamentali.

4. Le Istituzioni pubbliche promuovono, in particolare attraverso il sistema dell'istruzione e della formazione, l'educazione all'uso consapevole di Internet e intervengono per rimuovere ogni forma di ritardo culturale che precluda o limiti l’utilizzo di Internet da parte delle persone.

5. L'uso consapevole di Internet è fondamentale garanzia per lo sviluppo di uguali possibilità di crescita individuale e collettiva, il riequilibrio democratico delle differenze di potere sulla Rete tra attori economici, Istituzioni e cittadini, la prevenzione delle discriminazioni e dei comportamenti a rischio e di quelli lesivi delle libertà altrui.

Art.4 (Neutralità della rete)

1. Ogni persona ha il diritto che i dati trasmessi e ricevuti in Internet non subiscano discriminazioni, restrizioni o interferenze in relazione al mittente, ricevente, tipo o contenuto dei dati, dispositivo utilizzato, applicazioni o, in generale, legittime scelte delle persone.

2. Il diritto ad un accesso neutrale ad Internet nella sua interezza è condizione necessaria per l'effettività dei diritti fondamentali della persona.

Art.5 (Tutela dei dati personali)

1. Ogni persona ha diritto alla protezione dei dati che la riguardano, per garantire il rispetto della sua dignità, identità e riservatezza.

2. Tali dati sono quelli che consentono di risalire all’identità di una persona e comprendono anche i dati dei dispositivi e quanto da essi generato e le loro ulteriori acquisizioni e elaborazioni, come quelle legate alla produzione di profili.

3. Ogni persona ha diritto di accedere ai dati raccolti che la riguardano, di ottenerne la rettifica e la cancellazione per motivi legittimi.

4. I dati devono esser trattati rispettando i principi di necessità, finalità, pertinenza, proporzionalità e, in ogni caso, prevale il diritto di ogni persona all'autodeterminazione informativa.

5. I dati possono essere raccolti e trattati con il consenso effettivamente informato della persona interessata o in base a altro fondamento legittimo previsto dalla legge. Il consenso è in via di principio revocabile. Per il trattamento di dati sensibili la legge può prevedere che il consenso della persona interessata debba essere accompagnato da specifiche autorizzazioni.

6. Il consenso non può costituire una base legale per il trattamento quando vi sia un significativo squilibrio di potere tra la persona interessata e il soggetto che effettua il trattamento.

7. Sono vietati l’accesso e il trattamento dei dati con finalità anche indirettamente discriminatorie.

Art.6 (Diritto all’autodeterminazione informativa)

1. Ogni persona ha diritto di accedere ai propri dati, quale che sia il soggetto che li detiene e il luogo dove sono conservati, per chiederne l’integrazione, la rettifica, la cancellazione secondo le modalità previste dalla legge. Ogni persona ha diritto di conoscere le modalità tecniche di trattamento dei dati che la riguardano.

2. La raccolta e la conservazione dei dati devono essere limitate al tempo necessario, rispettando in ogni caso i principi di finalità e di proporzionalità e il diritto all’autodeterminazione della persona interessata.

Art.7 (Diritto all’inviolabilità dei sistemi, dei dispositivi e domicili informatici)

1. I sistemi e i dispositivi informatici di ogni persona e la libertà e la segretezza delle sue informazioni e comunicazioni elettroniche sono inviolabili. Deroghe sono possibili nei soli casi e modi stabiliti dalla legge e con l'autorizzazione motivata dell'autorità giudiziaria.

Art.8 (Trattamenti automatizzati)
1. Nessun atto, provvedimento giudiziario o amministrativo, decisione comunque destinata ad incidere in maniera significativa nella sfera delle persone possono essere fondati unicamente su un trattamento automatizzato di dati personali volto a definire il profilo o la personalità dell’interessato.

**Art.9 (Diritto all’identità)**

1. Ogni persona ha diritto alla rappresentazione integrale e aggiornata delle proprie identità in Rete.
2. La definizione dell’identità riguarda la libera costruzione della personalità e non può essere sottratta all’intervento e alla conoscenza dell’interessato.
3. L’uso di algoritmi e di tecniche probabilistiche deve essere portato a conoscenza delle persone interessate, che in ogni caso possono opporsi alla costruzione e alla diffusione di profili che le riguardino.
4. Ogni persona ha diritto di fornire solo i dati strettamente necessari per l’adempimento di obblighi previsti dalla legge, per la fornitura di beni e servizi, per l’accesso alle piattaforme che operano in Internet.
5. L’attribuzione e la gestione dell’Identità digitale da parte delle Istituzioni Pubbliche devono essere accompagnate da adeguate garanzie, in particolare in termini di sicurezza.

**Art.10 (Protezione dell’anonimato)**

1. Ogni persona può accedere alla rete e comunicare elettronicamente usando strumenti anche di natura tecnica che proteggano l’anonimato ed evitino la raccolta di dati personali, in particolare per esercitare le libertà civili e politiche senza subire discriminazioni o censure.
2. Limitazioni possono essere previste solo quando siano giustificate dall’esigenza di tutelare rilevanti interessi pubblici e risultino necessarie, proporzionate, fondate sulla legge e nel rispetto dei caratteri propri di una società democratica.
3. Nei casi di violazione della dignità e dei diritti fondamentali, nonché negli altri casi previsti dalla legge, l’autorità giudiziaria, con provvedimento motivato, può disporre l’identificazione dell’autore della comunicazione.

**Art.11 (Diritto all’oblio)**

1. Ogni persona ha diritto di ottenere la cancellazione dagli indici dei motori di ricerca dei riferimenti ad informazioni che, per il loro contenuto o per il tempo trascorso dal momento della loro raccolta, non abbiano più rilevanza pubblica.
2. Il diritto all’oblio non può limitare la libertà di ricerca e il diritto dell’opinione pubblica a essere informati, che costituiscono condizioni necessarie per il funzionamento di una società democratica. Tale diritto può essere esercitato dalle persone note o alle quali sono affidate funzioni pubbliche solo se i dati che le riguardano non hanno alcun rilievo in relazione all’attività svolta o alle funzioni pubbliche esercitate.
3. Se la richiesta di cancellazione dagli indici dei motori di ricerca dei dati è stata accolta, chiunque può impugnare la decisione davanti all’autorità giudiziaria per garantire l’interesse pubblico all’informazione.

**Art.12 (Diritti e garanzie delle persone sulle piattaforme)**

1. I responsabili delle piattaforme digitali sono tenuti a comportarsi con lealtà e correttezza nei confronti di utenti, fornitori e concorrenti.
2. Ogni persona ha il diritto di ricevere informazioni chiare e semplificate sul funzionamento della piattaforma, a non veder modificate in modo arbitrario le condizioni contrattuali, a non subire comportamenti che possono determinare difficoltà o discriminazioni nell’accesso. Ogni persona deve in ogni caso essere informato del mutamento delle condizioni contrattuali. In questo caso ha diritto di interrompere il rapporto, di avere copia dei dati che la riguardano in forma interoperabile, di ottenere la cancellazione dalla piattaforma dei dati che la riguardano.
3. Le piattaforme che operano in Internet, qualora si presentino come servizi essenziali per la vita e l’attività delle persone, assicurano, anche nel rispetto del principio di concorrenza, condizioni per una adeguata interoperabilità, in presenza di parità di condizioni contrattuali, delle loro principali tecnologie, funzioni e dati verso altre piattaforme.
Art.13 (Sicurezza in rete)
1. La sicurezza in Rete deve essere garantita come interesse pubblico, attraverso l’integrità delle infrastrutture e la loro tutela da attacchi, e come interesse delle singole persone.

Art.14 (Governo della Rete)
1. Ogni persona ha diritto di vedere riconosciuti i propri diritti in Rete sia a livello nazionale che internazionale.
2. Internet richiede regole conformi alla sua dimensione universale e sovranazionale, volte alla piena attuazione dei principi e diritti prima indicati, per garantire il suo carattere aperto e democratico, impedire ogni forma di discriminazione e evitare che la sua disciplina dipenda dal potere esercitato da soggetti dotati di maggiore forza economica.
3. Le regole riguardanti la Rete devono tenere conto dei diversi livelli territoriali (sovranazionale, nazionale, regionale), delle opportunità offerte da forme di autoregolamentazione conformi ai principi indicati, della necessità di salvaguardare la capacità di innovazione anche attraverso la concorrenza, della molteplicità di soggetti che operano in Rete, promovendone il coinvolgimento in forme che garantiscono la partecipazione diffusa di tutti gli interessati. Le istituzioni pubbliche adottano strumenti adeguati per garantire questa forma di partecipazione.
4. In ogni caso, l’innovazione normativa in materia di Internet è sottoposta a valutazione di impatto sull’ecosistema digitale.
5. La gestione della Rete deve assicurare il rispetto del principio di trasparenza, la responsabilità delle decisioni, l’accessibilità alle informazioni pubbliche, la rappresentanza dei soggetti interessati.
6. L’accesso e il riutilizzo dei dati generati e detenuti dal settore pubblico debbono essere garantiti.
7. La costituzione di autorità nazionali e sovranazionali è indispensabile per garantire effettivamente il rispetto dei criteri indicati, anche attraverso una valutazione di conformità delle nuove norme ai principi di questa Dichiarazione.

*****

DISCUSSIONE

1. Quale pensate sia il valore di questo documento? Perché?
2. Cosa pensate della distribuzione degli articoli, in relazione ai singoli diritti? Vi sembra che ci siano diritti maggiormente tutelati e che alcuni diritti siano stati invece un poco dimenticati?
3. Quali sono gli articoli che vi hanno colpito, stupito o lasciato perplessi?
4. RESPONSABILITÀ DELL’INTERNET SERVICE PROVIDER
4.1. Responsabilità dell’Internet service provider per commenti di utenti

European Court of Human Rights, Grand Chamber, 16 June 2015, appl. n.64569/09 (Delfi v. Estonia)

In the case of Delfi AS v. Estonia, the European Court of Human Rights [...] delivers the following judgment [...].

Procedure
1. The case originated in an application (n.64569/09) against the Republic of Estonia lodged with the Court under Article 34 of the Convention for the Protection of Human Rights and Fundamental Freedoms (“the Convention”) by Delfi AS, a public limited liability company registered in Estonia (“the applicant company”), on 4 December 2009.

3. The applicant company alleged that its freedom of expression had been violated, in breach of Article 10 of the Convention, by the fact that it had been held liable for the third-party comments posted on its Internet news portal.

The facts
I. The circumstances of the case

A. Background to the case
11. The applicant company is the owner of Delfi, an Internet news portal that published up to 330 news articles a day at the time of the lodging of the application. Delfi is one of the largest news portals on the Internet in Estonia. It publishes news in Estonian and Russian in Estonia and also operates in Latvia and Lithuania.

12. At the material time, at the end of the body of the news articles there were the words “add your comment” and fields for comments, the commenter’s name and his or her e-mail address (optional). Below these fields there were buttons labelled “publish the comment” and “read comments”. The part for reading comments left by others was a separate area which could be accessed by clicking on the “read comments” button. The comments were uploaded automatically and were, as such, not edited or moderated by the applicant company. The articles received about 10,000 readers’ comments daily, the majority posted under pseudonyms.

13. Nevertheless, there was a system of notice-and-take-down in place: any reader could mark a comment as leim (an Estonian word for an insulting or mocking message or a message inciting hatred on the Internet) and the comment was removed expeditiously. Furthermore, there was a system of automatic deletion of comments that included certain stems of obscene words. In addition, a victim of a defamatory comment could directly notify the applicant company, in which case the comment was removed immediately.

14. The applicant company had made efforts to advise users that the comments did not reflect its own opinion and that the authors of comments were responsible for their content. On Delfi’s Internet site there were “Rules of comment” which included the following:

“The Delfi message board is a technical medium allowing users to publish comments. Delfi does not edit comments. An author of a comment is liable for his or her comment. It is worth noting that there have been cases in the Estonian courts where authors have been punished for the contents of a comment ...

Delfi prohibits comments whose content does not comply with good practice.
These are comments that:
– contain threats;
– contain insults;
– incite hostility and violence;
– incite illegal activities ... 
– contain off-topic links, spam or advertisements;
– are without substance and/or off-topic;
– contain obscene expressions and vulgarities ...
Delfi has the right to remove such comments and restrict their authors’ access to the writing of comments …”
The functioning of the notice-and-take-down system was also explained in the “Rules of comment”.
15. The Government submitted that in Estonia Delfi had a notorious history of publishing defamatory and degrading comments. Thus, on 22 September 2005 the weekly newspaper Eesti Ekspress had published an open letter from its editorial board to the Minister of Justice, the Chief Public Prosecutor and the Chancellor of Justice in which concern was expressed about incessant taunting of people on public websites in Estonia. Delfi was named as a source of brutal and arrogant mockery. The addresssees of the public letter responded to it in the 29 September 2005 edition of Eesti Ekspress. The Minister of Justice emphasised that the insulted persons had the right to defend their honour and reputation in court by bringing a suit against Delfi and claiming damages. The Chief Public Prosecutor referred to the legal grounds which made threats, incitement to social hatred, and sexual abuse of minors punishable under criminal law, and noted that liability for defamation and insults was dealt with under civil procedure. The Chancellor of Justice referred to the legal provisions designed to ensure the freedom of expression as well as the protection of everyone’s honour and good name, including sections 1043 and 1046 of the Obligations Act (Võlaõigusseadus).

B. Article and comments published on the Internet news portal
16. On 24 January 2006 the applicant company published an article on the Delfi portal under the heading “SLK Destroyed Planned Ice Road”. Ice roads are public roads over the frozen sea which are open between the Estonian mainland and some islands in winter. The abbreviation “SLK” stands for AS Saaremaa Laevakompanii (Saaremaa Shipping Company, a public limited liability company). SLK provides a public ferry transport service between the mainland and certain islands. L. was a member of the supervisory board of SLK and the company’s sole or majority shareholder at the material time.
17. On 24 and 25 January 2006 the article attracted 185 comments. About twenty of them contained personal threats and offensive language directed against L.
18. On 9 March 2006 L.’s lawyers requested the applicant company to remove the offensive comments and claimed 500,000 Estonian kroons (EEK) (approximately 32,000 euros (EUR)) in compensation for non-pecuniary damage. The request concerned the following twenty comments:
…
20. On 23 March 2006 the applicant company responded to the request from L.’s lawyers. It informed L. that the comments had been removed under the notice-and-take-down obligation, and refused the claim for damages.

D. Subsequent developments
32. On 1 October 2009 Delfi announced on its Internet portal that persons who had posted offensive comments were not allowed to post a new comment until they had read and accepted the rules of commenting. Furthermore, it was announced that Delfi had set up a team of moderators who carried out follow-up moderation of comments posted on the portal. First of all, the moderators reviewed all user notices of inappropriate comments. The compliance of comments with the rules of commenting was monitored as well. According to the information published, the number of comments posted by Delfi’s readers in August 2009 had been 190,000. Delfi’s moderators had removed 15,000 comments (about 8%), mainly consisting of spam or irrelevant comments. The share of defamatory comments had been less than 0.5% of the total number of comments.
…

3. Case-law of the Court of Justice of the European Union
[…]

The law
I. Alleged violation of Article 10 of the Convention
59. The applicant company complained that holding it liable for the comments posted by the readers of its Internet news portal infringed its freedom of expression as provided in Article 10 of the Convention, which reads as follows:
“1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority
and regardless of frontiers. This Article shall not prevent states from requiring the licensing of broadcasting, television or cinema enterprises.

2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.”

[...]

D. The Court’s assessment

1. Preliminary remarks and the scope of the Court’s assessment

110. The Court notes at the outset that user-generated expressive activity on the Internet provides an unprecedented platform for the exercise of freedom of expression. That is undisputed and has been recognised by the Court on previous occasions (see Ahmet Yıldırım v. Turkey, no.3111/10, §48, […]], and Times Newspapers Ltd (nos.1 and 2) v. the United Kingdom, nos.3002/03 and 23676/03, §27, […]). However, alongside these benefits, certain dangers may also arise. Defamatory and other types of clearly unlawful speech, including hate speech and speech inciting violence, can be disseminated like never before, worldwide, in a matter of seconds, and sometimes remain persistently available online. These two conflicting realities lie at the heart of this case. Bearing in mind the need to protect the values underlying the Convention, and considering that the rights under Article 10 and 8 of the Convention deserve equal respect, a balance must be struck that retains the essence of both rights. Thus, while the Court acknowledges that important benefits can be derived from the Internet in the exercise of freedom of expression, it is also mindful that liability for defamatory or other types of unlawful speech must, in principle, be retained and constitute an effective remedy for violations of personality rights.

[...]

112. Firstly, the Court observes that the Supreme Court recognised (see §14 of its judgment of 10 June 2009 as set out in §31 above) that “[p]ublishing of news and comments on an Internet portal is also a journalistic activity. At the same time, because of the nature of Internet media, it cannot reasonably be required of a portal operator to edit comments before publishing them in the same manner as applies for a printed media publication. While the publisher [of a printed media publication] is, through editing, the initiator of the publication of a comment, on the Internet portal the initiator of publication is the writer of the comment, who makes it accessible to the general public through the portal. Therefore, the portal operator is not the person to whom information is disclosed. Because of [their] economic interest in the publication of comments, both a publisher of printed media and an Internet portal operator are publishers/disclosers as entrepreneurs”.

113. The Court sees no reason to call into question the above distinction made by the Supreme Court. On the contrary, the starting-point of the Supreme Court’s reflections, that is, the recognition of differences between a portal operator and a traditional publisher, is in line with the international instruments in this field, which manifest a certain development in favour of distinguishing between the legal principles regulating the activities of the traditional print and audiovisual media on the one hand and Internet-based media operations on the other. In the recent Recommendation of the Committee of Ministers to the member States of the Council of Europe on a new notion of media, this is termed a “differentiated and graduated approach [that] requires that each actor whose services are identified as media or as an intermediary or auxiliary activity benefit from both the appropriate form (differentiated) and the appropriate level (graduated) of protection and that responsibility also be delimited in conformity with Article 10 of the European Convention on Human Rights and other relevant standards developed by the Council of Europe” (see §7 of the Appendix to Recommendation CM/Rec(2011)7, quoted in §46 above). Therefore, the Court considers that because of the particular nature of the Internet, the “duties and responsibilities” that are to be conferred on an Internet news portal for the purposes of Article 10 may differ to some degree from those of a traditional publisher, as regards third-party content.

114. Secondly, the Court observes that the Supreme Court of Estonia found that the “legal assessment by the courts of the twenty comments of a derogatory nature [was] substantiated. The courts [had] correctly found that those comments [were] defamatory since they [were] of a vulgar nature, degrade[d] human dignity and contain[ed] threats” (see §15 of the judgment as set out in §31 above). Further, in §16 of its judgment, the Supreme Court reiterated that the comments
degraded “human dignity” and were “clearly unlawful”. The Court notes that this characterisation and analysis of the unlawful nature of the comments in question (see §18 above) is obviously based on the fact that the majority of the comments are, viewed on their face, tantamount to an incitement to hatred or to violence against L.

115. Consequently, the Court considers that the case concerns the “duties and responsibilities” of Internet news portals, under Article 10 §2 of the Convention, when they provide for economic purposes a platform for user-generated comments on previously published content and some users – whether identified or anonymous – engage in clearly unlawful speech, which infringes the personality rights of others and amounts to hate speech and incitement to violence against them. The Court emphasises that the present case relates to a large professionally managed Internet news portal run on a commercial basis which published news articles of its own and invited its readers to comment on them.

116. Accordingly, the case does not concern other fora on the Internet where third-party comments can be disseminated, for example an Internet discussion forum or a bulletin board where users can freely set out their ideas on any topics without the discussion being channelled by any input from the forum’s manager; or a social media platform where the platform provider does not offer any content and where the content provider may be a private person running the website or a blog as a hobby.

117. Furthermore, the Court notes that the applicant company’s news portal was one of the biggest Internet media publications in the country; it had a wide readership and there was a known public concern about the controversial nature of the comments it attracted (see §15 above). Moreover, as outlined above, the impugned comments in the present case, as assessed by the Supreme Court, mainly constituted hate speech and speech that directly advocated acts of violence. Thus, the establishment of their unlawful nature did not require any linguistic or legal analysis since the remarks were on their face manifestly unlawful. It is against this background that the Court will proceed to examine the applicant company’s complaint.

2. Existence of an interference

118. The Court notes that it was not in dispute between the parties that the applicant company’s freedom of expression guaranteed under Article 10 of the Convention had been interfered with by the domestic courts’ decisions. The Court sees no reason to hold otherwise.

119. Such an interference with the applicant company’s right to freedom of expression must be “prescribed by law”, have one or more legitimate aims in the light of §2 of Article 10, and be “necessary in a democratic society”.

3. Lawfulness

120. The Court reiterates that the expression “prescribed by law” in the second §of Article 10 not only requires that the impugned measure should have a legal basis in domestic law, but also foresees the quality of the law in question, which should be accessible to the person concerned and foreseeable as to its effects (see, among other authorities, VgT Verein gegen Tierfabriken v. Switzerland, no.24699/94, §52, […]; Rotaru v. Romania [GC], no.28341/95, §52, […]; Gawęda v. Poland, no.26229/95, §39, […]; and Maestri v. Italy [GC], no.39748/98, §30, […]). However, it is primarily for the national authorities, notably the courts, to interpret and apply domestic law (see Centro Europa 7 S.r.l. and Di Stefano v. Italy [GC], no.38433/09, §140, […]; Kruslin v. France, 24 April 1990, §29, […]; and Kopp v. Switzerland, 25 March 1998, §59, […]).

121. One of the requirements flowing from the expression “prescribed by law” is foreseeability. Thus, a norm cannot be regarded as a “law” within the meaning of Article 10 §2 unless it is formulated with sufficient precision to enable the citizen to regulate his conduct; he must be able – if need be with appropriate advice – to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail. Those consequences need not be foreseeable with absolute certainty. Whilst certainty is desirable, it may bring in its train excessive rigidity, and the law must be able to keep pace with changing circumstances. Accordingly, many laws are inevitably couched in terms which, to a greater or lesser extent, are vague, and whose interpretation and application are questions of practice (see, for example, Lindon, Otchkovsky-Laurens and July v. France [GC], nos.21279/02 and 36448/02, §41, […], and Centro Europa 7 S.r.l. and Di Stefano, cited above, §141).

122. The level of precision required of domestic legislation – which cannot provide for every eventuality – depends to a considerable degree on the content of the law in question, the field it is designed to cover and the number and status of those to whom it is addressed (see Centro Europa
7 S.r.l. and Di Stefano, cited above, §142). The Court has found that persons carrying on a professional activity, who are used to having to proceed with a high degree of caution when pursuing their occupation, can on this account be expected to take special care in assessing the risks that such activity entails (see Lindon, Otchakovsky-Laurens and July, cited above, §41, with further references to Cantoni v. France, 15 November 1996, §35, [...] and Chauy and Others v. France, no.64915/01, §§43-45, [...]).

123. In the present case the parties’ opinions differed as to whether the interference with the applicant company’s freedom of expression was “prescribed by law”. The applicant company argued that there was no domestic law according to which an intermediary was to be taken as a professional publisher of comments posted on its website by third parties regardless of whether it was aware of their specific content. On the contrary, the applicant company relied on the domestic and European legislation on Internet service providers and argued that it expressly prohibited the imposition of liability on service providers for third-party content.

124. The Government referred to the relevant provisions of the civil law and domestic case-law to the effect that media publishers were liable for their publications along with the authors. They added that there was no case-law on the basis of which the applicant company could have presumed that the owner of an Internet news portal as a new media publication was not liable for the comments posted on its articles. In their view the Court should proceed from the facts as established and the law as applied and interpreted by the domestic courts and not take account of the applicant company’s references to EU law. In any event, the EU law referred to by the applicant company actually supported the domestic courts’ interpretations and conclusions.

125. The Court observes that the difference in the parties’ opinions as regards the law to be applied stems from their diverging views on the issue of how the applicant company is to be classified. According to the applicant company, it should be classified as an intermediary as regards the third-party comments, whereas the Government argued that the applicant company was to be seen as a media publisher, including with regard to such comments.

[...]

129. The Court accordingly finds that, as a professional publisher, the applicant company should have been familiar with the legislation and case-law, and could also have sought legal advice. The Court observes in this context that the Delfi news portal is one of the largest in Estonia. Public concern had already been expressed before the publication of the comments in the present case and the Minister of Justice had noted that victims of insults could bring a suit against Delfi and claim damages (see §15 above). Thus, the Court considers that the applicant company was in a position to assess the risks related to its activities and that it must have been able to foresee, to a reasonable degree, the consequences which these could entail. It therefore concludes that the interference in issue was “prescribed by law” within the meaning of the second §of Article 10 of the Convention.

4. Legitimate aim

130. The parties before the Grand Chamber did not dispute that the restriction of the applicant company’s freedom of expression had pursued the legitimate aim of protecting the reputation and rights of others. The Court sees no reason to hold otherwise.

5. Necessary in a democratic society

(a) General principles

131. The fundamental principles concerning the question whether an interference with freedom of expression is “necessary in a democratic society” are well established in the Court’s case-law and have been summarised as follows (see, among other authorities, Hertel v. Switzerland, 25 August 1998, §46, [...] Steel and Morris v. the United Kingdom, no.68416/01, §87, [...] Mouvement raëlien suisse v. Switzerland [GC], no.16354/06, §48, [...] and Animal Defenders International v. the United Kingdom [GC], no.48876/08, §100, [...]):

“(i) Freedom of expression constitutes one of the essential foundations of a democratic society and one of the basic conditions for its progress and for each individual’s self-fulfilment. Subject to §2 of Article 10, it is applicable not only to ‘information’ or ‘ideas’ that are favourably received or regarded as inoffensive or as a matter of indifference, but also to those that offend, shock or disturb. Such are the demands of pluralism, tolerance and broadmindedness without which there is no ‘democratic society’. As set forth in Article 10, this freedom is subject to exceptions, which ... must, however, be construed strictly, and the need for any restrictions must be established convincingly ...
(ii) The adjective ‘necessary’, within the meaning of Article 10 §2, implies the existence of a ‘pressing social need’. […]

(iii) […]

132. Furthermore, the Court has emphasised the essential function the press fulfils in a democratic society. Although the press must not overstep certain bounds, particularly as regards the reputation and rights of others and the need to prevent the disclosure of confidential information, its duty is nevertheless to impart – in a manner consistent with its obligations and responsibilities – information and ideas on all matters of public interest […]. Journalistic freedom also covers possible recourse to a degree of exaggeration, or even provocation […]. The limits of permissible criticism are narrower in relation to a private citizen than in relation to politicians or governments […].

133. Moreover, the Court has previously held that in the light of its accessibility and its capacity to store and communicate vast amounts of information, the Internet plays an important role in enhancing the public’s access to news and facilitating the dissemination of information in general (see Ahmet Yıldırım, cited above, §48, and Times Newspapers Ltd, cited above, §27). At the same time, the risk of harm posed by content and communications on the Internet to the exercise and enjoyment of human rights and freedoms, particularly the right to respect for private life, is certainly higher than that posed by the press (see Editorial Board of Pravoye Delo and Shtekel, cited above, §63).

134. In considering the “duties and responsibilities” of a journalist, the potential impact of the medium concerned is an important factor and it is commonly acknowledged that the audiovisual media often have a much more immediate and powerful effect than the print media (see Purcell and Others v. Ireland, no.15404/89, Commission decision of 16 April 1991, […], p. 262). The methods of objective and balanced reporting may vary considerably, depending among other things on the media in question (see Jersild, cited above, §31).

[…]

136. Moreover, the Court has held that speech that is incompatible with the values proclaimed and guaranteed by the Convention is not protected by Article 10 by virtue of Article 17 of the Convention. The examples of such speech examined by the Court have included statements denying the Holocaust, justifying a pro-Nazi policy, linking all Muslims with a grave act of terrorism, or portraying the Jews as the source of evil in Russia (see Lehideux and Isorni v. France, 23 September 1998, §§47 and 53, […]; Garaudy v. France (dec.), no.65831/01, […]; Norwood v. the United Kingdom (dec.), no.23131/03, […]; Witzsch v. Germany (dec.), no.7485/03, 13 December 2005; and Pavel Ivanov v. Russia (dec.), no.35222/04, 20 February 2007).

137. The Court further reiterates that the right to protection of reputation is a right which is protected by Article 8 of the Convention as part of the right to respect for private life (see Chauvy and Others, cited above, §70; Pfeifer v. Austria, no.12556/03, §35, 15 November 2007; and Polanco Torres and Movilla Polanco v. Spain, no.34147/06, §40, 21 September 2010). In order for Article 8 to come into play, however, an attack on a person’s reputation must attain a certain level of seriousness and be made in a manner causing prejudice to personal enjoyment of the right to respect for private life (see A. v. Norway, no.28070/06, §64, 9 April 2009, and Axel Springer AG v. Germany [GC], no.39954/08, §83, 7 February 2012).

[…]

(b) Application of the above principles to the present case

(i) Elements in the assessment of proportionality

140. The Court notes that it is not disputed that the comments posted by readers in reaction to the news article published on the applicant company’s Internet news portal, as presented in the portal’s commenting area, were of a clearly unlawful nature. Indeed, the applicant company removed the comments once it was notified by the injured party, and described them as “infringing” and “illicit” before the Chamber (see §84 of the Chamber judgment). Moreover, the Court is of the view that the majority of the impugned comments amounted to hate speech or incitements to violence and as such did not enjoy the protection of Article 10 (see §136 above). Thus, the freedom of expression of the authors of the comments is not at issue in the present case. Rather, the question before the Court is whether the domestic courts’ decisions, holding the applicant company liable for these comments posted by third parties, were in breach of its freedom to impart information as guaranteed by Article 10 of the Convention.

[…]
143. The Court agrees that these aspects are relevant for the concrete assessment of the proportionality of the interference in issue within the scope of the Court’s examination of the present case (see §§112 to 117 above).

(ii) Context of the comments

144. As regards the context of the comments, the Court accepts that the news article about the ferry company, published on the Delfi news portal, was a balanced one, contained no offensive language and gave rise to no arguments about unlawful statements in the domestic proceedings. The Court is aware that even such a balanced article on a seemingly neutral topic may provoke fierce discussions on the Internet. Furthermore, it attaches particular weight, in this context, to the nature of the Delfi news portal. It reiterates that Delfi was a professionally managed Internet news portal run on a commercial basis which sought to attract a large number of comments on news articles published by it. The Court observes that the Supreme Court explicitly referred to the fact that the applicant company had integrated the comment environment into its news portal, inviting visitors to the website to complement the news with their own judgments and opinions (comments). According to the findings of the Supreme Court, in the comment environment, the applicant company actively called for comments on the news items appearing on the portal. The number of visits to the applicant company’s portal depended on the number of comments; the revenue earned from advertisements published on the portal, in turn, depended on the number of visits. Thus, the Supreme Court concluded that the applicant company had an economic interest in the posting of comments. In the view of the Supreme Court, the fact that the applicant company was not the writer of the comments did not mean that it had no control over the comment environment (see §13 of the judgment as set out in §31 above).

145. The Court also notes in this regard that the “Rules of comment” on the Delfi website stated that the applicant company prohibited the posting of comments that were without substance and/or off-topic, were contrary to good practice, contained threats, insults, obscene expressions or vulgarities, or incited hostility, violence or illegal activities. Such comments could be removed and their authors’ ability to post comments could be restricted. Furthermore, the actual authors of the comments could not modify or delete their comments once they were posted on the applicant company’s news portal – only the applicant company had the technical means to do this. In the light of the above and the Supreme Court’s reasoning, the Court agrees with the Chamber’s finding that the applicant company must be considered to have exercised a substantial degree of control over the comments published on its portal.

146. In sum, the Court considers that it was sufficiently established by the Supreme Court that the applicant company’s involvement in making public the comments on its news articles on the Delfi news portal went beyond that of a passive, purely technical service provider. The Court therefore finds that the Supreme Court based its reasoning on this issue on grounds that were relevant for the purposes of Article 10 of the Convention.

(iii) Liability of the authors of the comments

147. In connection with the question whether the liability of the actual authors of the comments could serve as a sensible alternative to the liability of the Internet news portal in a case like the present one, the Court is mindful of the interest of Internet users in not disclosing their identity. Anonymity has long been a means of avoiding reprisals or unwanted attention. As such, it is capable of promoting the free flow of ideas and information in an important manner, including, notably, on the Internet. At the same time, the Court does not lose sight of the ease, scope and speed of the dissemination of information on the Internet, and the persistence of the information once disclosed, which may considerably aggravate the effects of unlawful speech on the Internet compared to traditional media. It also refers in this connection to a recent judgment of the Court of Justice of the European Union in the case of Google Spain and Google, in which that court, albeit in a different context, dealt with the problem of the availability on the Internet of information seriously interfering with a person’s private life over an extended period of time, and found that the individual’s fundamental rights, as a rule, overrode the economic interests of the search engine operator and the interests of other Internet users (see §56 above).

148. The Court observes that different degrees of anonymity are possible on the Internet. An Internet user may be anonymous to the wider public while being identifiable by a service provider through an account or contact data that may be either unverified or subject to some kind of verification – ranging from limited verification (for example, through activation of an account via an e-mail address or a social network account) to secure authentication, be it by the use of national
electronic identity cards or online banking authentication data allowing rather more secure identification of the user. A service provider may also allow an extensive degree of anonymity for its users, in which case the users are not required to identify themselves at all and they may only be traceable – to a limited extent – through the information retained by Internet access providers. The release of such information would usually require an injunction by the investigative or judicial authorities and would be subject to restrictive conditions. It may nevertheless be required in some cases in order to identify and prosecute perpetrators.

149. Thus, in the case of *K.U. v. Finland*, concerning an offence of “malicious misrepresentation” of a sexual nature against a minor, the Court found that “[a]lthough freedom of expression and confidentiality of communications are primary considerations and users of telecommunications and Internet services must have a guarantee that their own privacy and freedom of expression will be respected, such guarantee cannot be absolute and must yield on occasion to other legitimate imperatives, such as the prevention of disorder or crime or the protection of the rights and freedoms of others” (see *K.U. v. Finland*, no.2872/02, §49, [...]). The Court in that case rejected the Government’s argument that the applicant had had the possibility of obtaining damages from the service provider, finding that this was not sufficient in the circumstances of the case. It held that there had to be a remedy enabling the actual offender to be identified and brought to justice, whereas at the relevant time the regulatory framework of the respondent State had not provided for the possibility of ordering the Internet service provider to divulge the information required for that purpose (ibid., §§47 and 49). Although the case of *K.U. v. Finland* concerned a breach classified as a criminal offence under the domestic law and involved a more sweeping intrusion into the victim’s private life than the present case, it is evident from the Court’s reasoning that anonymity on the Internet, although an important value, must be balanced against other rights and interests.

150. As regards the establishment of the identity of the authors of the comments in civil proceedings, the Court notes that the parties’ positions differed as to its feasibility. On the basis of the information provided by the parties, the Court observes that the Estonian courts, in the “pre-trial taking of evidence” procedure under Article 244 of the Code of Civil Procedure (see §40 above), have granted requests by defamed persons for the disclosure by online newspapers or news portals of the IP addresses of authors who had posted allegedly defamatory comments and for the disclosure by Internet access providers of the names and addresses of the subscribers to whom the IP addresses in question had been assigned. The examples provided by the Government show mixed results: in some cases it has proved possible to establish the computer from which the comments had been made, while in other cases, for various technical reasons, this has proved impossible.

151. According to the Supreme Court’s judgment in the present case, the injured person had the choice of bringing a claim against the applicant company or the authors of the comments. The Court considers that the uncertain effectiveness of measures allowing the identity of the authors of the comments to be established, coupled with the lack of instruments put in place by the applicant company for the same purpose with a view to making it possible for a victim of hate speech to effectively bring a claim against the authors of the comments, are factors that support a finding that the Supreme Court based its judgment on relevant and sufficient grounds. The Court also refers, in this context, to the *Krone Verlag* (no.4) judgment, where it found that shifting the risk of the defamed person obtaining redress in defamation proceedings to the media company, which was usually in a better financial position than the defamer, was not as such a disproportionate interference with the media company’s right to freedom of expression (see *Krone Verlags GmbH & Co. KG v. Austria* (no.4), no.72331/01, §32, 9 November 2006).

(iv) Measures taken by the applicant company

152. The Court notes that the applicant company highlighted the number of comments on each article on its website, and therefore the places of the most lively exchanges must have been easily identifiable for the editors of the news portal. The article in issue in the present case attracted 185 comments, apparently well above average. The comments in question were removed by the applicant company some six weeks after they were uploaded on the website, upon notification by the injured person’s lawyers to the applicant company (see §§17 to 19 above).

153. The Court observes that the Supreme Court stated in its judgment that “[o]n account of the obligation arising from law to avoid causing harm, the [applicant company] should have prevented the publication of comments with clearly unlawful contents”. However, it also held that
“[a]fter the disclosure, the [applicant company had] failed to remove the comments – the unlawful content of which it should have been aware of – from the portal on its own initiative” (see §16 of the judgment as set out in §31 above). Therefore, the Supreme Court did not explicitly determine whether the applicant company was under an obligation to prevent the uploading of the comments on the website or whether it would have sufficed under domestic law for the applicant company to have removed the offending comments without delay after publication, to escape liability under the Obligations Act. The Court considers that when assessing the grounds upon which the Supreme Court relied in its judgment entailing an interference with the applicant’s Convention rights, there is nothing to suggest that the national court intended to restrict the applicant’s rights to a greater extent than that required to achieve the aim pursued. On this basis, and having regard to the freedom to impart information as enshrined in Article 10, the Court will thus proceed on the assumption that the Supreme Court’s judgment must be understood to mean that the subsequent removal of the comments by the applicant company, without delay after publication, would have sufficed for it to escape liability under domestic law. Consequently, and taking account of the above findings (see §145) to the effect that the applicant company must be considered to have exercised a substantial degree of control over the comments published on its portal, the Court does not consider that the imposition on the applicant company of an obligation to remove from its website, without delay after publication, comments that amounted to hate speech and incitement to violence, and were thus clearly unlawful on their face, amounted, in principle, to a disproportionate interference with its freedom of expression.

154. The pertinent issue in the present case is whether the national court’s findings that liability was justified, as the applicant company had not removed the comments without delay after publication, were based on relevant and sufficient grounds. With this in mind, account must, firstly, be taken of whether the applicant company had instituted mechanisms that were capable of filtering comments amounting to hate speech or speech entailing an incitement to violence.

155. The Court notes that the applicant company took certain measures in this regard. There was a disclaimer on the Delfi news portal stating that the writers of the comments – and not the applicant company – were accountable for them, and that the posting of comments that were contrary to good practice or contained threats, insults, obscene expressions or vulgarities, or incited hostility, violence or illegal activities, was prohibited. Furthermore, the portal had an automatic system of deletion of comments based on stems of certain vulgar words and it had a notice-and-take-down system in place, whereby anyone could notify it of an inappropriate comment by simply clicking on a button designated for that purpose, to bring it to the attention of the portal administrators. In addition, on some occasions the administrators removed inappropriate comments on their own initiative.

156. Thus, the Court notes that the applicant company cannot be said to have wholly neglected its duty to avoid causing harm to third parties. Nevertheless, and more importantly, the automatic word-based filter used by the applicant company failed to filter out odious hate speech and speech inciting violence posted by readers and thus limited its ability to expeditiously remove the offending comments. The Court reiterates that the majority of the words and expressions in question did not include sophisticated metaphors or contain hidden meanings or subtle threats. They were manifest expressions of hatred and blatant threats to the physical integrity of L. Thus, even if the automatic word-based filter may have been useful in some instances, the facts of the present case demonstrate that it was insufficient for detecting comments whose content did not constitute protected speech under Article 10 of the Convention (see §136 above). The Court notes that as a consequence of this failure of the filtering mechanism, such clearly unlawful comments remained online for six weeks (see §18 above).

157. The Court observes in this connection that on some occasions the portal administrators did remove inappropriate comments on their own initiative and that, apparently some time after the events of the present case, the applicant company set up a dedicated team of moderators. Having regard to the fact that there are ample possibilities for anyone to make his or her voice heard on the Internet, the Court considers that a large news portal’s obligation to take effective measures to limit the dissemination of hate speech and speech inciting violence – the issue in the present case – can by no means be equated to “private censorship”. While acknowledging the “important role” played by the Internet “in enhancing the public’s access to news and facilitating the dissemination of information in general” (see Ahmet Yildirim, cited above, §48, and Times Newspapers Ltd, cited above, §27), the Court reiterates that it is also mindful of the risk of harm posed by content and
communications on the Internet (see Editorial Board of Pravoye Delo and Shtekel, cited above, §63; see also Mosley, cited above, §130).

158. Moreover, depending on the circumstances, there may be no identifiable individual victim, for example in some cases of hate speech directed against a group of persons or speech directly inciting violence of the type manifested in several of the comments in the present case. In cases where an individual victim exists, he or she may be prevented from notifying an Internet service provider of the alleged violation of his or her rights. The Court attaches weight to the consideration that the ability of a potential victim of hate speech to continuously monitor the Internet is more limited than the ability of a large commercial Internet news portal to prevent or rapidly remove such comments.

159. Lastly, the Court observes that the applicant company has argued (see §78 above) that the Court should have due regard to the notice-and-take-down system that it had introduced. If accompanied by effective procedures allowing for rapid response, this system can in the Court’s view function in many cases as an appropriate tool for balancing the rights and interests of all those involved. However, in cases such as the present one, where third-party user comments are in the form of hate speech and direct threats to the physical integrity of individuals, as understood in the Court’s case-law (see §136 above), the Court considers, as stated above (see §153), that the rights and interests of others and of society as a whole may entitle Contracting States to impose liability on Internet news portals, without contravening Article 10 of the Convention, if they fail to take measures to remove clearly unlawful comments without delay, even without notice from the alleged victim or from third parties.

(v) Consequences for the applicant company

160. Finally, turning to the question of what consequences resulted from the domestic proceedings for the applicant company, the Court notes that the company was obliged to pay the injured person the equivalent of EUR 320 in compensation for non-pecuniary damage. It agrees with the finding of the Chamber that this sum, also taking into account the fact that the applicant company was a professional operator of one of the largest Internet news portals in Estonia, can by no means be considered disproportionate to the breach established by the domestic courts (see §93 of the Chamber judgment). The Court notes in this connection that it has also had regard to the domestic post-Delfi case-law on the liability of the operators of Internet news portals (see §43 above). It observes that in these cases the lower courts have followed the Supreme Court’s judgment in Delfi but no awards have been made for non-pecuniary damage. In other words, the tangible result for the operators in post-Delfi cases has been that they have taken down the offending comments but have not been ordered to pay compensation for non-pecuniary damage.

161. The Court also observes that it does not appear that the applicant company had to change its business model as a result of the domestic proceedings. According to the information available, the Delfi news portal has continued to be one of Estonia’s largest Internet publications and by far the most popular for posting comments, the number of which has continued to increase. Anonymous comments – now existing alongside the possibility of posting registered comments, which are displayed to readers first – are still predominant and the applicant company has set up a team of moderators carrying out follow-up moderation of comments posted on the portal (see §§32 and 83 above). In these circumstances, the Court cannot conclude that the interference with the applicant company’s freedom of expression was disproportionate on that account either.

(vi) Conclusion

162. Based on the concrete assessment of the above aspects, taking into account the reasoning of the Supreme Court in the present case, in particular the extreme nature of the comments in question, the fact that the comments were posted in reaction to an article published by the applicant company on its professionally managed news portal run on a commercial basis, the insufficiency of the measures taken by the applicant company to remove without delay after publication comments amounting to hate speech and speech inciting violence and to ensure a realistic prospect of the authors of such comments being held liable, and the moderate sanction imposed on the applicant company, the Court finds that the domestic courts’ imposition of liability on the applicant company was based on relevant and sufficient grounds, having regard to the margin of appreciation afforded to the respondent State. Therefore, the measure did not constitute a disproportionate restriction on the applicant company’s right to freedom of expression.

Accordingly, there has been no violation of Article 10 of the Convention.

For these reasons, the Court
Holds, by fifteen votes to two, that there has been no violation of Article 10 of the Convention.

[...]

In accordance with Article 45 §2 of the Convention and Rule 74 §2 of the Rules of Court, the following separate opinions are annexed to this judgment:

(a) joint concurring opinion of Judges Raimondi, Karakas, De Gaetano and Kjølbro;
(b) concurring opinion of Judge Zupančič;
(c) joint dissenting opinion of Judges Sajó and Tsotsoria.

Joint concurring opinion of Judges Raimondi, Karakas, De Gaetano and Kjølbro

[...]

4. There are two possible readings of the Supreme Court’s judgment: (1) Delfi was liable as it did not “prevent” the unlawful comments from being published, and its liability was aggravated by the fact that it did not subsequently “remove” the comments; or (2) Delfi did not “prevent” the unlawful comments from being published, and as it did not subsequently “remove” the comments without delay, it was liable for them.

5. The Court has decided to read the Supreme Court’s judgment in the second sense, thereby avoiding the difficult question of the possible liability of a news portal for not having “prevented” unlawful user-generated comments from being published. However, had the Court read the Supreme Court’s judgment in the first sense, the outcome of the case might have been different.

6. If the Supreme Court’s judgment were to be understood in the first sense, it would enshrine an interpretation of domestic legislation that would entail a risk of imposing excessive burdens on a news portal such as Delfi. In fact, in order to avoid liability for comments written by readers of its articles, a news portal would have to prevent such comments from being published (and would also have to remove any such comments that were published). This might, in practice, require an effective monitoring system, be it automatic or manual. In other words, a news portal might have to pre-monitor comments in order to avoid publishing clearly unlawful comments made by readers. Furthermore, if the liability of a news portal was closely linked to the clearly unlawful nature of the comments, without it being necessary for the plaintiff to prove that the news portal knew or ought to have known that the comments would be or had been published on the portal, the portal would in practice be obliged to act on the assumption that such comments could be made by readers and therefore to take the necessary measures to avoid them being published, which in practice would require pre-monitoring measures to be adopted.

[...]

7. Therefore, in our view, finding a news portal liable for not having “prevented” the publication of user-generated comments would in practice imply that the portal would have to pre-monitor each and every user-generated comment in order to avoid liability for any unlawful comments. This could in practice lead to a disproportionate interference with the news portal’s freedom of expression as guaranteed by Article 10.

[...]

10. A news portal such as Delfi, which invites readers of articles to write comments that are made public on the portal, will assume “duties and responsibilities” as provided for in domestic legislation. Furthermore, it follows from Article 8 of the Convention that member States have an obligation to effectively protect the reputation and honour of individuals. Therefore, Article 10 of the Convention cannot be interpreted as prohibiting member States from imposing obligations on news portals such as Delfi when they allow readers to write comments that are made public. In fact, member States may in certain circumstances have an obligation to do so in order to protect the honour and reputation of others. Thus, member States may decide that a news portal is to be regarded as the publisher of the comments in question. Furthermore, they may prescribe that news portals may be held liable for clearly unlawful comments, such as insults, threats and hate speech, which are written by users and made public on the portal. However, in exercising their power to do so, member States must comply with their obligations under Article 10 of the Convention. Therefore, domestic legislation should not restrict the freedom of expression by imposing excessive burdens on news portals.

11. In our view, member States may hold a news portal, such as Delfi, liable for clearly unlawful comments such as insults, threats and hate speech by readers of its articles if the portal...
knew, or ought to have known, that such comments would be or had been published on the portal. Furthermore, member States may hold a news portal liable in such situations if it fails to act promptly when made aware of such comments published on the portal.

15. Having regard to the clearly unlawful nature of the comments in question, as well as the fact that they remained on the news portal for six weeks before they were removed, we do not find it disproportionate for the Supreme Court to find Delfi liable as it had “failed to remove the comments – the unlawful content of which it should have been aware of – from the portal at its own initiative”. In fact, not being aware of such clearly unlawful comments for such an extended period of time almost amounts to wilful ignorance, which cannot serve as a basis for avoiding civil liability.

Concurring opinion of Judge Zupančič

Also, in my opinion, it is completely unacceptable that an Internet portal or any other kind of mass media should be permitted to publish any kind of anonymous comments. We seem to have forgotten that “letters to the editor”, not so long ago, were double-checked as to the identity of the author before they were ever deemed publishable. The Government argued (see §90 of the judgment) that the biggest international news portals did not allow anonymous (that is, unregistered) comments and referred to an opinion that there was a trend away from anonymity. At the same time, anonymous comments tended to be more insulting than the comments by persons who had registered, and harsh comments attracted more readers. The Government argued that Delfi had been notorious for exactly this reason.

On the other hand, in the case of Print Zeitungverlag GmbH v. Austria (no. 26547/07, judgment delivered on 10 October 2013, the same day as the Chamber judgment in Delfi) the Court held that an award of damages amounting to 2,000 euros (EUR) for the publication of an anonymous letter in print was – and rightly so! – compatible with its previous case-law. [...] The mass media used to be run according to the obvious principle that the great freedom enjoyed by the press implied a commensurate level of responsibility. To enable technically the publication of extremely aggressive forms of defamation, all this due to crass commercial interest, and then to shrug one’s shoulders, maintaining that an Internet provider is not responsible for these attacks on the personality rights of others, is totally unacceptable.

According to the old tradition of the protection of personality rights, which again go back to Roman law, the amount of approximately EUR 300 awarded in compensation in the present case is clearly inadequate as far as damages for the injury to the aggrieved persons are concerned. The mere comparison with the above-mentioned case of Print Zeitungverlag GmbH v. Austria, which involved only two aggrieved persons and a printed medium with very limited distribution, demonstrates that a much higher award of damages was called for in the present case.

Joint dissenting opinion of Judges Sajó and Tsotsoria

I. - Collateral censorship

1. In this judgment the Court has approved a liability system that imposes a requirement of constructive knowledge on active Internet intermediaries[...] (that is, hosts who provide their own content and open their intermediary services for third parties to comment on that content). We find the potential consequences of this standard troubling. The consequences are easy to foresee. For the sake of preventing defamation of all kinds, and perhaps all "illegal" activities, all comments will have to be monitored from the moment they are posted. As a consequence, active intermediaries and blog operators will have considerable incentives to discontinue offering a comments feature, and the fear of liability may lead to additional self-censorship by operators. This is an invitation to self-censorship at its worst.

2. We regret that the Court did not rely on the prophetic warnings of Professor Jack Balkin [...]. As Professor Balkin has demonstrated, the technological infrastructure behind digital communication is subject to less visible forms of control by private and public regulators, and the Court has just added another such form to this panoply. Governments may not always be directly censoring expression, but by putting pressure and imposing liability on those who control the
technological infrastructure (ISPs, etc.), they create an environment in which collateral or private-party censorship is the inevitable result. Collateral censorship “occurs when the state holds one private party A liable for the speech of another private party B, and A has the power to block, censor, or otherwise control access to B’s speech” […]. Because A is liable for someone else’s speech, A has strong incentives to over-censor, to limit access, and to deny B’s ability to communicate using the platform that A controls. In effect, the fear of liability causes A to impose prior restraints on B’s speech and to stifle even protected speech. “What looks like a problem from the standpoint of free expression ... may look like an opportunity from the standpoint of governments that cannot easily locate anonymous speakers and want to ensure that harmful or illegal speech does not propagate.” […]. These technological tools for reviewing content before it is communicated online lead (among other things) to: deliberate overbreadth; limited procedural protections (the action is taken outside the context of a trial); and shifting of the burden of error costs (the entity in charge of filtering will err on the side of protecting its own liability, rather than protecting freedom of expression).

6. The general context

The present judgment expressly deals with the general context (see the “Preliminary remarks” section starting at §110) but without determining “issues on public-policy grounds”. The Internet is described as an “unprecedented platform” and while there is reference to benefits, it is described as posing “certain dangers”, the advantages being scarcely mentioned. We disagree. The Internet is more than a uniquely dangerous novelty. It is a sphere of robust public discourse with novel opportunities for enhanced democracy. Comments are a crucial part of this new enhanced exchange of ideas among citizens. This has been the Court’s understanding so far in its case-law (see Ashby Donald and Others v. France, no.36769/08, §34, 10 January 2013, and also Węgrzynowski and Smolczewski v. Poland, no.33846/07, §58, 16 July 2013) […].

Consequences

8. The Court has endorsed the standard of the Estonian Supreme Court, namely that active intermediaries must remove comments “without delay” after publication (see §153 of the judgment), and not upon notice or on other grounds linked to actual knowledge. Active intermediaries are therefore invited to exercise prior restraint. Moreover, member States will be forced to introduce a similar approach because otherwise, according to the logic of the present judgment, there is no proper protection for the rights of those who feel defamed by comments. To avoid trouble, for active intermediaries the safe harbour will simply be to disable comments […].

8. Social media operators have already institutionalised over-censorship by allowing a policy of banning sites and posts which have been “reported”, without conducting a serious investigation into the matter. The policy adopted by Facebook is another victory for the troll mentality. Note that Facebook requires (all) user-imposed censorship to take place in a legal environment that grants service providers immunity under the Communications Decency Act 230 (a). Imagine what will happen where there is no immunity.

9. The Court is aware of the unhappy consequences of adopting a standard that can be satisfied only by constant monitoring of all comments (and implicitly, all user-generated content). For the Court, “the case does not concern other fora on the Internet ... or a social media platform ... [where] the content provider may be a private person running the website or a blog as a hobby” (see §116 of the judgment). It is hard to imagine how this “damage control” will help. Freedom of expression cannot be a matter of a hobby.

II. Delfi’s role as active intermediary

11. This case is about interference with the freedom of expression of Delfi as an active intermediary. Delfi published an article on the destruction of ice roads by a public service ferry company on its news portal and it enabled comments on the article. It is undisputed that there was nothing illegal in the article. It was accepted by the national courts, and we could not agree more, that Delfi was engaged in journalistic activities and that the opening up of a comment space formed part of the news portal. However, the news portal was not the author of the unedited comments. Furthermore, at least in the Chamber’s view (see §86 of its judgment), the debate concerned a matter of “a certain degree” of public interest. We believe that the article dealt with a matter of
public interest and that the comments, even the impugned ones, were part of the debate even though they may have been excessive or impermissible. Delfi was held liable under the Civil Code of Estonia for defamation originating from comments posted in the comment space attached to the article. This concerned twenty comments.

[...]

Publishers’ liability extended: base economic interest
[...]

29. Over the last three hundred years, ideas have been generated for money and this has never been held to reduce the level of protection otherwise granted to speech. We do not live in the aristocratic world of the Roman auctor who could afford not to care about the financial return on ideas (though very often being dependent on imperial pleasure). It cannot be held against a newspaper or publisher that they operate an outlet as a commercial enterprise. One cannot expect the production of ideas for free. There will be no generation of ideas without adequate financial means; the material reward and the commercial nature of the press enterprise are not (and cannot be) grounds for diminishing the level of protection afforded to the press. Information is costly; its efficient communication is not a mere hobby. The same platform that has been understood as commercial, and thus subject to increased liability, is also a platform for enhanced, interactive discourse on a matter of public interest. This aspect has not been taken into consideration in the balancing exercise.

30. However, the Court does provide at least one relevant consideration for extending the liability of an active intermediary. It is certainly true that the active intermediary can exercise control over the comments that appear on its site and it is also true that by creating a space for comments, and inviting users to participate, it engages in an expressive activity that entails responsibility. But the nature of the control does not imply identification with a traditional publisher.

31. There are additional differences between a publisher (understood here as a newspaper editor, someone who controls content) and an active intermediary:
   (a) in a newspaper the journalist is typically an employee (although there are good reasons to protect a journalist against his or her editor/employer); and
   (b) in principle, the editor is in a position to know in advance the content of an article to be published and has the decision-making power and the means to control the publication in advance.

Contrary to the case of a publisher, these elements are only partially present in the case of active intermediaries who host their own content and actively monitor all data (that is to say, are in the position to read it and remove it after the data are made accessible), as in the case of Delfi. The active intermediary has prior control only to the extent that this is made possible by a filtering mechanism. It also has the power to remove a message or block access to it. However, in normal situations the active intermediary has no personal control over the person who posts the message. The commenter is not the employee of the publisher and in most cases is not known to the publisher. The publication occurs without the decision of the editor. Hence the level of knowledge and control differs significantly.

32. Control presupposes knowledge. In this regard the difference between the editor/publisher and the active intermediary is obvious.

The level of responsibility

33. While Delfi cannot be defined as a publisher, the company does voluntarily provide an opportunity for comments and, even if this activity is a matter of freedom of expression of a journalistic nature, this does not exempt the activity from liability. The Information Society Services Act does envisage such liability, among other things for storage, as is the case here. The Act bases liability on “actual knowledge” and entails a duty of expeditious removal. The Court found this to be insufficient.

34. The Court finds it to be a relevant and sufficient consideration that the Supreme Court limited the responsibility of the applicant company to post-publication liability. However, as quoted in §153 of the judgment, the Supreme Court stated that the applicant company “should have prevented the publication of comments”. The fact that it “also held” that there was a duty of removal after the disclosure does not change the first statement. Both pre- and post-disclosure liability are being advocated here and this cannot be disregarded when it comes to the evaluation of “sufficient reasons”. [...]

It was under this standard that Delfi was found to be at fault for the disclosure of the information, which could not have been undone by removal upon request.
35. The duty to remove offensive comments without actual knowledge of their existence and immediately after they are published means that the active intermediary has to provide supervision 24/7. For all practical purposes, this is absolute and strict liability, which is in no sense different from blanket prior restraint. No reasons are given as to why only this level of liability satisfies the protection of the relevant interests.

[...]

****

DISCUSSIONE

1. Delfi dovrebbe essere responsabile per i commenti dei lettori agli articoli pubblicati sul portale? Se sì, sempre, o solo a certe condizioni? Nel caso, quali?
2. Delfi deve essere considerato come un service provider o invece (o anche) come l’editore o il coordinatore della pubblicazione on-line?
3. Quali sono le misure individuate da Delfi per ridurre le probabilità di commenti diffamatori o minacciosi? Le ritenete sufficienti?
4. Delfi ricopre un “ruolo attivo” sulla pubblicazione dei commenti dei lettori?
5. A Delfi può essere ascritta la violazione di un obbligo generalizzato di sorveglianza sui contenuti pubblicati?
6. Quale è, secondo voi, il giusto bilanciamento tra diritto alla privacy e libertà di espressione, in riferimento alla responsabilità di soggetti come Delfi?
7. Quali possono essere le conseguenze di questo caso sullo sviluppo della Rete?

****

NORME

- artt.8, 10, CEDU
4.2. Mancata informativa e responsabilità del provider

Corte di Cassazione, sez.III penale, 3 febbraio 2014, n.5107

Ritenuto in fatto

La condotta contestata consiste, in particolare, nell'avere omesso un'informativa sulla privacy, visualizzabile in italiano dalla pagina iniziale del servizio Google video, in sede di attivazione del relativo account, al fine di porre in essere l'upload di files, in ordine a quanto prescritto dal comma 1 del richiamato art.13 e, per esso, del valido consenso di cui all'art.23, comma 3. La violazione ipotizzata investe anche l'art.26 richiamato, riguardando dati idonei a rivelare lo stato di salute della persona inquadrata nel video, e l'art.17 anch'esso richiamato, per i rischi specifici insiti nel tipo di trattamento omesso, anche in relazione alle concrete misure organizzative da prestare.

2. Con sentenza del 21 dicembre 2012, la Corte d'appello di Milano ha riformato, per la parte che qui rileva, la sentenza impugnata, evidenziando che l'art.167 del d.lgs. n.196 del 2003 non richiama il precedente art.13 e, dunque, non impone all'Internet provider di rendere edotto l'utente circa l'esistenza e i contenuti della legislazione sulla privacy. Infatti, l'eventuale violazione del citato art.13, consistente nell'omessa o inidonea informativa all'interessato, viene punita non dall'art.167, bensì dal precedente art.161, che prevede una sanzione amministrativa. Nella stessa sentenza si esclude, inoltre, la configurabilità di un concorso omissivo nel reato contestato. Si esclude, altresì, la sussistenza del dolo specifico richiesto dalla disposizione incriminatrice, sul rilievo che gli imputati non erano preventivamente a conoscenza del filmato e dell'immissione del dato personale illecitamente trattato e sull'ulteriore rilievo della incompatibilità giuridica del detto dolo specifico col dolo eventuale individuato dal Tribunale in capo agli imputati.

3. Quest'ultima sentenza è stata impugnata, con ricorso per cassazione, dal Procuratore generale della Repubblica presso la Corte d'appello di Milano.

[...]

Considerato in diritto
5. Il ricorso del Procuratore generale non è fondato.
6. La complessità e la novità delle questioni trattate impongono una sintetica ricostruzione del quadro normativo interno di riferimento.

6.1. Il comma 1 dell'art.4 del Codice Privacy reca le seguenti definizioni: «a) "trattamento", qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modifica, la selezione, l'elaborazione, il riferimento, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in un'archivio di dati; b) "dato personale", qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale; [...] d) "dati sensibili", i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale; [...] f) "titolare", la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di
dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza; g) "responsabile", la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali; [...] i) "interessato", la persona fisica, cui si riferiscono i dati personali; l) "comunicazione", il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione; m) "diffusione", il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione».

6.2. L'art.13 del Codice Privacy prevede, al comma 1, che: «L'interessato o la persona presso la quale sono raccolti i dati personali sono previamente informati oralmente o per iscritto circa: a) le finalità e le modalità del trattamento cui sono destinati i dati; b) la natura obbligatoria o facoltativa del conferimento dei dati; c) le conseguenze di un eventuale rifiuto di rispondere; d) i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, e l'ambito di diffusione dei dati medesimi; e) i diritti di cui all'art.7; f) gli estremi identificativi del titolare e, se designati, del rappresentante nel territorio dello Stato ai sensi dell'art.5 e del responsabile. Quando il titolare ha designato più responsabili è indicato almeno uno di essi, indicando il sito della rete di comunicazione o le modalità attraverso le quali è conoscibile in modo agevole l'elenco aggiornato dei responsabili. Quando è stato designato un responsabile per il riscontro all'interessato in caso di esercizio dei diritti di cui all'art.7, è indicato tale responsabile». Prevede inoltre, al comma 4, che, «Se i dati personali non sono raccolti presso l'interessato, l'informativa di cui al comma 1, comprensiva delle categorie di dati trattati, è data al medesimo interessato all'atto della registrazione dei dati o, quando è prevista la loro comunicazione, non oltre la prima comunicazione».

La violazione delle disposizioni dell'art.13 è punita dal successivo art.161 del Codice Privacy con la sanzione amministrativa del pagamento di una somma di denaro.

6.3. L'art.17 dello stesso Codice prevede, poi, che il trattamento di dati che presentano rischi specifici «per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che può determinare, è ammesso nel rispetto di misure ed accorgimenti a garanzia dell'interessato, ove prescritti». Tali misure e accorgimenti «sono prescritti dal Garante in applicazione dei principi sanciti dal presente codice, nell'ambito di una verifica preliminare all'inizio del trattamento, effettuata anche in relazione a determinate categorie di titolari o di trattamenti, anche a seguito di un interpello del titolare».

6.4. L'art.23 dispone - per quanto qui rileva - che il trattamento di dati personali da parte di privati o di enti pubblici economici è ammesso solo con il consenso espresso dell'interessato e che tale consenso è manifestato in forma scritta quando il trattamento riguarda dati sensibili.

6.5. Il successivo art.26, dopo avere affermato, al comma 1, che «i dati sensibili possono essere oggetto di trattamento solo con il consenso scritto dell'interessato e previa autorizzazione del Garante, nell'osservanza dei presupposti e dei limiti stabiliti dal presente codice, nonché dalla legge e dai regolamenti», prevede, al comma 5, che «i dati idonei a rivelare lo stato di salute non possono essere diffusi».

6.6. La violazione di tali ultime disposizioni è sanzionata dall'art.167, a norma del quale, «1. Salvo che il fatto costituisca più grave reato, chiedendo, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli artt.18, 19, 23, 123, 126 e 130, ovvero in applicazione dell'art.129, è punito, se dal fatto deriva nocumo, con la reclusione da sei a diciotto mesi o, se il fatto consiste nella comunicazione o diffusione, con la reclusione da sei a ventiquattro mesi. 2. Salvo che il fatto costituisca più grave reato, chiedendo, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli artt.17, 20, 21, 22, commi 8 e 11, 25, 26, 27 e 45, è punito, se dal fatto deriva nocumo, con la reclusione da uno a tre anni». 6.7. A tale disciplina si affianca quella contenuta nel d.lgs. 9 aprile 2003, n.70 (Attuazione della direttiva 2000/31/CE relativa a taluni aspetti giuridici dei servizi della società dell'informazione nel mercato interno, con particolare riferimento al commercio elettronico), che all'art.1, comma 2, alinea e lett.b), dispone che «Non rientrano nel campo di applicazione del presente decreto: [...] b) le questioni relative al diritto alla riservatezza, con riguardo al trattamento dei dati personali nel

6.8. Quanto alla responsabilità nell'attività di memorizzazione di informazioni (hosting), il successivo art.16 del medesimo d.lgs. n.70 del 2003 prevede che, «1. Nella prestazione di un servizio della società dell'informazione, consistente nella memorizzazione di informazioni fornite da un destinatario del servizio, il prestatore non è responsabile delle informazioni memorizzate a richiesta di un destinatario del servizio, a condizione che detto prestatore: a) non sia effettivamente a conoscenza del fatto che l'attività o l'informazione è illecita e, per quanto attiene ad azioni risarctorie, non sia al corrente di fatti o di circostanze che rendono manifesta l'illicità dell'attività o dell'informazione; b) non appena a conoscenza di tali fatti, su comunicazione delle autorità competenti, agisca immediatamente per rimuovere le informazioni o per disabilitarne l'accesso. 2. Le disposizioni di cui al comma 1 non si applicano se il destinatario del servizio agisce sotto l'autorità o il controllo del prestatore. 3. L'autorità giudiziaria o quella amministrativa competente può esigere, anche in via d'urgenza, che il prestatore, nell'esercizio delle attività di cui al comma 1, impedisca o ponga fine alle violazioni commesse».

6.9. Infine, a norma del successivo art.17 (Assenza dell'obbligo generale di sorveglianza), «1. Nella prestazione dei servizi di cui agli artt.14, 15 e 16, il prestatore non è assoggettato ad un obbligo generale di sorveglianza sulle informazioni che trasmette o memorizza, né ad un obbligo generale di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite. 2. Fatte salve le disposizioni di cui agli artt.14, 15 e 16, il prestatore è comunque tenuto: a) ad informare senza indugio l'autorità giudiziaria o quella amministrativa avente funzioni di vigilanza, qualora sia a conoscenza di presunte attività o informazioni illecite riguardanti un suo destinatario del servizio della società dell'informazione; b) a fornire senza indugio, a richiesta delle autorità competenti, le informazioni in suo possesso che consentano l'identificazione del destinatario dei suoi servizi con cui ha accordi di memorizzazione dei dati, al fine di individuare e prevenire attività illecite. 3. Il prestatore è civilmente responsabile del contenuto di tali servizi nel caso in cui, richiesto dall'autorità giudiziaria o amministrativa avente funzioni di vigilanza, non ha agito prontamente per impedire l'accesso a detto contenuto, ovvero se, avendo avuto conoscenza del carattere illecito o pregiudizievole per un terzo del contenuto di un servizio al quale assicura l'accesso, non ha provveduto ad informarne l'autorità competente».

7.1. A tali conclusioni si giunge muovendo dall'analisi delle definizioni di "trattamento" e "titolare del trattamento" fornite dal richiamato art.4 del Codice Privacy. Infatti, se non vi è dubbio che il concetto di "trattamento" sia assai ampio, perché comprensivo di ogni operazione che abbia ad oggetto dati personali, indipendentemente dai mezzi e dalle tecniche utilizzati, il concetto di "titolare" è, invece, assai più specifico, perché si incendra sull'esistenza di un potere decisionale in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati. Dalla definizione legislativa si desume, in altri termini, che titolare del trattamento non è chiunque materialmente svolga il trattamento stesso, ma solo il soggetto che possa determinarne gli scopi, i modi, i mezzi.

Dal complesso dei precetti fissati dagli artt.13, 17, 23, 26 del Codice Privacy, interpretati in combinato disposto con le norme sanzionatorie degli artt.161 167 dello stesso Codice emerge, poi, che essi sono tutti diretti al titolare del trattamento, eventualmente nella persona del "responsabile", ovvero del soggetto preposto al trattamento stesso dal titolare, ai sensi dell'art.4, comma 1, lett.g). Tali disposizioni presuppongono, infatti, l'esistenza di un effettivo potere decisionale circa: a) le finalità e le modalità del trattamento cui sono destinati i dati e la comunicazione eventuale dei dati stessi ad altri soggetti, anche attraverso la designazione dei responsabili (art.13); b) la gestione dei rischi specifici «per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, in relazione alla natura dei dati o alle modalità del trattamento» (art.17); c) la ricezione del consenso degli interessati, nel rispetto dei divieti di legge (artt.23 e 26).

Ne deriva, più in particolare, che i reati di cui all'art.167 del Codice Privacy - per i quali qui si procede - devono essere intesi come reati propri, trattandosi di condotte che si concretizzano in violazioni di obblighi dei quali è destinatario in modo specifico il solo titolare del trattamento e non
7.2. Tali conclusioni trovano applicazione anche con riguardo alla figura dell'Internet hosting provider, perché esso è definito dall'art.16 del d.lgs. n.70 del 2003 come colui che si limita a prestare un «servizio consistente nella memorizzazione di informazioni fornite da un destinatario del servizio». Da tale definizione, interpretata nel contesto complessivo dello stesso art.16, emerge, infatti, che il gestore del servizio di hosting non ha alcun controllo sui dati memorizzati, né contribuisce in alcun modo alla loro scelta, alla loro ricerca o alla formazione del file che li contiene, essendo tali dati interamente ascrivibili all'utente destinatario del servizio che li carica sulla piattaforma messa a sua disposizione. A tale proposito, risulta significativo che, secondo l'espressa previsione dello stesso art.16, lo hosting provider non sia responsabile delle informazioni memorizzate a richiesta di un destinatario del servizio. E ciò, alla duplice condizione: che il provider non sia effettivamente a conoscenza del fatto che l'attività o l'informazione è illecita e, per quanto attiene ad azioni risarcitorie, non sia al corrente di fatti o di circostanze che rendono manifesta l'illicetità dell'attività o dell'informazione; che, non appena a conoscenza di tali fatti, su comunicazione delle autorità competenti, agisca immediatamente per rimuovere le informazioni o per disabilitarne l'accesso. Così disponendo, in conformità della direttiva 2000/31/CE, il legislatore ha inteso porre qualsi dei presupposti della responsabilità del provider proprio la sua effettiva conoscenza dei dati immessi dall'utente e l'eventuale inerzia nella rimozione delle informazioni da lui conosciute come illecite. Se ne desume, ai fini della ricostruzione interpretativa della figura del titolare del trattamento dei dati, che il legislatore ha inteso far coincidere il potere decisionale sul trattamento con la capacità di concretamente incidere su tali dati, che non può prescindere dalla conoscenza dei dati stessi. In altri termini, finché il dato illecito è sconosciuto al service provider, questo non può essere considerato quale titolare del trattamento, perché privo di qualisoglia potere decisionale sul dato stesso; quando, invece, il provider sia a conoscenza del dato illecito e non si attivi per la sua immediata rimozione o per renderlo comunque inaccessibile esso assume a pieno titolo la qualifica di titolare del trattamento ed è, dunque, destinatario dei precetti e delle sanzioni penali del Codice Privacy. In via generale, sono, dunque gli utenti ad essere titolari del trattamento dei dati personali di terzi ospitati nei servizi di hosting e non i gestori che si limitano a fornire tali servizi.

7.3. L'interpretazione appena delineata risulta ulteriormente confermata dal tenore letterale del successivo art.17 - applicabile a tutte le categorie di provider disciplinate dagli articoli precedenti, ivi compreso lo hosting service provider - che esclude la configurabilità di un obbligo generale di sorveglianza sulle informazioni trasmesse o memorizzate e di un obbligo generale di ricercare attivamente eventuali illeciti. La stessa disposizione individua il punto di equilibrio fra la libertà del provider e la tutela dei soggetti eventualmente danneggiati nella fissazione di obblighi di informazione alle autorità, a carico dello stesso provider, relativamente a presunte attività o informazioni illecite dei quali sia venuto a conoscenza, anche al fine di consentire l'individuazione dei responsabili.

Né a tale conclusione può obiettarsi - come fa il Procuratore generale con il secondo motivo di ricorso - che l'art.1, comma 2, lett.b), del d.lgs. n.70 del 2003 prevede espressamente che non rientrano nel campo di applicazione della normativa sul commercio elettronico le questioni relative al diritto alla riservatezza, con riguardo al trattamento dei dati personali nel settore delle telecomunicazioni.

La richiamata disciplina sul commercio elettronico viene infatti in rilievo - come visto - non in via diretta ma solo in via interpretativa, al fine di chiarire ulteriormente e confermare la portata che la disciplina in materia di privacy ha già di per sé. In questo quadro, la definizione di Internet hosting provider contenuta nell'art.16 del richiamato d.lgs. n.70 del 2003 deve essere intesa come meramente ripetitiva della nozione comune di Internet hosting provider già desumibile dal linguaggio utilizzato dagli operatori informatici. Si tratta, peraltro, di una nozione che si pone in linea con l'orientamento del Gruppo di lavoro istituito dall'art.29 della direttiva 95/46/CE e composto dai rappresentanti delle autorità garanti in materia di privacy dei singoli Stati membri; organo consultivo indipendente avente il compito di esaminare le questioni attinenti all'applicazione delle norme nazionali di attuazione di detta direttiva. Nei suoi pareri (v., in particolare, il n.5 del 2009 e il n.1 del 2010 […]) si evidenzia, in particolare, che i titolari del trattamento dei dati caricati in siti di hosting sono i singoli utenti che li hanno caricati e che l'essere titolare del trattamento deriva dal fatto concreto che un soggetto abbia scelto di trattare dati personali per propri fini; con la
conseguenza che la persona che può essere chiamata a rispondere delle violazioni delle norme sulla protezione dei dati è sempre il titolare del trattamento e non il mero hosting provider. Analoghe considerazioni vengono svolte, a proposito del fornitore di servizi di motore di ricerca su Internet, ai p.ti 84 e seguenti delle conclusioni dell'Avvocato generale presentate il 25 giugno 2013 di fronte alla Corte di Giustizia nella causa C-131/12 (Google Spain SL e Google Inc. contro Agencia Española de Protección de Datos e Mario Costeja González), laddove si precisa, in particolare, che tale fornitore è riconducibile alla categoria dei titolari del trattamento di dati solo laddove incida direttamente sulla struttura degli indici di ricerca, ad esempio favorendo o rendendo più difficile il reperimento di un determinato sito.

7.4. A tali considerazioni deve aggiungersi, infine, che la clausola di cui all'art.1, comma 5, lett.b), della direttiva sul commercio elettronico, ripresa da quella contenuta nell'art.1, comma 2, lett.b), del d.lgs. n.70 del 2003 non ha di per sé la funzione di rendere inoperanti comunque in ogni fattispecie che riguardi la materia della protezione dei dati personali le norme in materia di commercio elettronico. Più semplicemente, detta clausola ha la funzione di chiarire che la tutela dei dati personali è disciplinata da un corpus normativo diverso da quello sul commercio elettronico; corpus normativo che rimane applicabile in ambito telematico anche in seguito all'emanazione della normativa sul commercio elettronico. Da ciò discende l'ovvia conseguenza che l'applicazione delle norme in materia di commercio elettronico deve avvenire in armonia con le norme in materia di tutela dei dati personali; armonia perfettamente riscontrabile - come appena visto - nel caso della determinazione dell'ambito di responsabilità penale dell'Internet hosting provider relativamente ai dati sensibili caricati dagli utenti sulla sua piattaforma. Tale interpretazione trova piena conferma, inoltre, nella Prima relazione della Commissione in merito all'applicazione della direttiva 2000/31/CE, del 21 novembre 2003, in cui si legge, al §4.6, che le limitazioni della responsabilità giuridica stabilite dalla direttiva sul commercio elettronico hanno carattere generale e coprono tanto la responsabilità civile quanto quella penale, per tutti i tipi di attività illegali intraprese da terzi. Un'ulteriore conferma è data, poi, dalla sentenza della Corte di Giustizia dell'Unione Europea 23 marzo 2010, nei procedimenti da C-236/08 a C-238/08 (p.to 120), nella quale si afferma che l'art.14 della Direttiva sul commercio elettronico (corrispondente all'art.16 del d.lgs. n.70 del 2003) deve essere interpretato nel senso che si applica al prestatore di un servizio di posizionamento su Internet qualora detto prestatore non abbia svolto un ruolo attivo nel ripristino o nella rimozione; c) la rimozione era stata chiesta dalla Polizia postale il 7 novembre 2006; d) in quello stesso giorno il video era stato rimosso dal provider.

8. I principi appena enunciati trovano applicazione anche nel caso in esame, nel quale, in estrema sintesi: a) il video raffigurante un soggetto affetto da sindrome di Down ingiuriato e preso in giro dai suoi compagni proprio in relazione alla sua particolare sindrome era stato caricato su Google video, servizio di Internet hosting, all'insaputa di tale soggetto; b) nei giorni 5 e 6 novembre 2006 alcuni utenti avevano segnalato la presenza del video sul sito e ne avevano chiesto la rimozione; c) la rimozione era stata chiesta dalla Polizia postale il 7 novembre 2006; d) in quello stesso giorno il video era stato rimosso dal provider.

La posizione di Google Italia S.r.l. e dei suoi responsabili, imputati nel presente procedimento, è infatti quella di mero Internet hosting provider, soggetto che si limita a fornire una piattaforma sulla quale gli utenti possono liberamente caricare i loro video; video del cui contenuto restano gli esclusivi responsabili. Ne consegue che gli imputati non sono titolari di alcun trattamento e che gli unici titolari del trattamento dei dati sensibili eventualmente contenuti nei video caricati sul sito sono gli stessi utenti che li hanno caricati, ai quali soli possono essere applicate le sanzioni, amministrative e penali, previste per il titolare del trattamento dal Codice Privacy.

8.1. Tale essendo l'ambito nel quale va inquadrata la fattispecie concreta, deve rilevarsi che il primo motivo di ricorso è infondata.

Il ricorrente lamenta, in particolare, che la Corte d'appello non avrebbe considerato che, per i dati idonei a rivelare lo stato di salute, vige un divieto assoluto di loro diffusione anche in presenza del consenso dell'interessato, ai sensi dell'art.26, comma 5, del d.lgs. n.196 del 2003. Non si sarebbe considerato, inoltre, che lo status di soggetto affetto da sindrome di Down del ragazzo ripreso era ben percepibile dalla visione del video e risultava dal titolo dei video stesso.
Quanto al primo di tali rilievi - ulteriormente sviluppato nell’ambito del terzo motivo di ricorso - deve premettersi che, secondo quanto affermato dalla giurisprudenza di questa Corte, pur nel diverso ambito del bilanciamento fra diritto di cronaca e protezione dei dati personali (sez.III, 4 maggio 2011, n.17215), la pubblicazione di un’immagine che rappresenti le condizioni di salute di un soggetto - si trattava in quel caso della foto di una persona ricoverata in fin di vita con il volto devastato da un colpo di arma da fuoco - configura un trattamento di dati personali. E ciò, perché - come già osservato - il concetto di “trattamento” è assai ampio e prescinde dall’insinuamento dei dati in una vera e propria banca dati, potendosi concretizzare in qualunque operazione di utilizzazione e diffusione di tali dati, anche per mezzo della rappresentazione fotografica o della ripresa video.

Ne consegue - con riferimento al caso di specie - che la realizzazione e il caricamento sul sito del video da parte degli utenti del servizio Google video configura un “trattamento” ai sensi dell’art.4, comma 1, lett.a), del Codice Privacy, effettuato in violazione del divieto di diffusione dei dati idonei a rilevare lo stato di salute fissato dal successivo art.26, comma 5.

Circa i responsabili della violazione, deve però ribadirsi che - contrariamente a quanto sostenuto dal ricorrente - questi sono da identificarsi con gli utenti che hanno caricato il video sulla piattaforma Google video e non con i soggetti responsabili per la gestione di tale piattaforma, trattandosi, come già ampiamente visto, di un mero servizio di hosting.

Ed è proprio la natura del servizio reso ad escludere anche la fondatezza del secondo dei rilievi svolti dal Procuratore generale nell’ambito del primo motivo di ricorso, non essendo configurabile alcun obbligo generale di controllo in capo ai rappresentanti di Google Italy s.r.l., gestore del servizio stesso.

8.2. Sull’infondatezza del secondo motivo di ricorso, relativamente alla pretesa inapplicabilità della normativa sul commercio elettronico alle questioni relative al diritto alla riservatezza, è sufficiente qui richiamare le considerazioni già ampiamente svolte sub 7.3.

Quanto alla pretesa non riconducibilità dell’attività svolta da Google Italy s.r.l. alla categoria dell’hosting, devono essere invece richiamati i rilievi sub 8., dovendosi ribadire che nel caso di specie il provider si è limitato a fornire ospitalità ai video inseriti dagli utenti, senza fornire alcun contributo nel determinare il contenuto dei video stessi.

8.3. Analoghe considerazioni valgono con riferimento al terzo motivo di doglianza, con cui si deduce l’inosservanza degli artt.167, 13, 23, 4, del d.lgs. n.196 del 2003 e si afferma che, seconda l’art.13, comma 4, richiamato, se i dati personali non sono raccolti presso l’interessato, l’informativa di cui al comma 1, comprensiva delle categorie dei dati trattati, deve essere data dal provider all’interessato all’atto della registrazione dei dati o, quando è prevista la loro comunicazione, non oltre la prima comunicazione.

Va infatti rilevato che nessuno obbligo sussiste in capo al provider, non essendo questo, ma il singolo utente il responsabile del trattamento dei dati personali contenuti nel video caricato dall’utente stesso. E ciò, a prescindere dall’ulteriore analisi del quadro normativo, dalla quale emerge con chiarezza che l’eventuale violazione dell’art.13 del Codice Privacy è sanzionata in via meramente amministrativa dal successivo art.161 e non rientra, invece, fra quelle sanzionate penalmente dall’art.167.

Il ricorrente afferma, poi, che vi sarebbe una qualche analogia tra la fattispecie per la quale qui si procede e quella esaminata dalla sentenza Cass., sez.III, 24 maggio 2012, n.23798, con la quale era stata affermata la responsabilità penale del legale rappresentante e del responsabile della privacy di una società, per illecito trattamento di dati personali, in relazione al caso di passaggio di mano di un database formato da centinaia di migliaia di indirizzi e-mail, per la mancanza dell’informativa volta ad acquisire il consenso degli interessati.

Tale affermazione non merita, all’evidenza, di essere condivisa perché non tiene conto delle peculiarità della posizione dell’Internet host provider più volte evidenziate rispetto alla posizione di un soggetto che, detenendo una vera e propria banca dati contenente gli indirizzi di una serie di soggetti, che lui stesso ha formato e gestito e della quale conosce fin dall’inizio il contenuto e le finalità, la cede ad un altro soggetto senza preocuparsi di acquisire il consenso degli interessati.

8.4. I rilievi finora svolti conducono ad escludere in radice la configurabilità, sotto il profilo oggettivo, di una responsabilità penale dell’Internet host provider e rendono, dunque, superfluo l’esame del quarto motivo di ricorso e dei correlati rilievi contenuti nella memoria difensiva relativamente alla configurabilità dell’elemento soggettivo del reato. E ciò, a prescindere dall’ulteriore considerazione che la mancanza di una conoscenza, in capo al provider, del dato sensibile contenuto nel video caricato dagli utenti sul suo sito e la mancanza di un obbligo...
generale di sorveglianza inducono ad escludere comunque - come ben evidenziato dalla Corte d'appello - la rappresentazione e la conseguente volizione da parte degli imputati del fatto tipico, costituito dall'abusivo trattamento di tale dato.

[...]

P.Q.M.
Rigetta il ricorso del Procuratore generale.

*****

DISCUSSIONE

1. La definizione di “dato personale” fa riferimento anche a foto, filmati, tag? Siete d’accordo?
2. Cosa si intende per “informativa” nella disciplina del Codice per la protezione dei dati personali? Come si applica in relazione ai contenuti pubblicati in Rete?
3. Google era da ritenere responsabile, in concorso, per il reato di diffamazione? Perché?
4. Google ricopriva un “ruolo attivo” nella pubblicazione di contenuti?
5. A Google poteva essere ascrutta la violazione di un obbligo generalizzato di sorveglianza sui contenuti pubblicati?
6. Quali sarebbero state le conseguenze di questo caso sullo sviluppo della Rete se la sentenza di primo grado fosse stata confermata?

*****

NORME

- art.40, c.p.
- artt.13, 17, 23, 26, 110, 161, 167, d.lgs. n.196/2003
- artt.16, 17, d.lgs. n.70/2003
European Court of Human Rights, Fourth Section, 2 February 2016, appl. n.22947/13
(MTE and Index.hu v. Hungary)

Procedure
1. The case originated in an application (no.22947/13) against Hungary lodged with the Court under Article 34 of the Convention for the Protection of Human Rights and Fundamental Freedoms (“the Convention”) by two legal entities registered under Hungarian law, Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt (“the applicants”), on 28 March 2013 respectively.

The facts
I. The circumstances of the case
5. The first applicant, Magyar Tartalomszolgáltatók Egyesülete (“MTE”) is an association seated in Budapest. It is the self-regulatory body of Hungarian Internet content providers, monitoring the implementation of a professional code of Internet content providing and a code of ethics, as well as operating an arbitration commission whose decision are binding on its eleven members.

The second applicant, Index.hu Zrt (“Index”) is a company limited by shares, seated in Budapest. It is the owner of one of the major Internet news portals in Hungary.

6. At the material time both applicants allowed users to comment on the publications appearing on their portals. Comments could be uploaded following registration and were not previously edited or moderated by the applicants.

7. The applicants advised their readers, in the form of disclaimers, that the comments did not reflect the portals’ own opinion and that the authors of comments were responsible for their contents.

8. Both applicants put in place a system of notice-and-take-down, namely, any reader could notify the service provider of any comment of concern and request its deletion. In addition, in the case of Index, comments were partially moderated, and removed, if necessary.

9. Both portals stated that comments infringing the personality rights of others could not be uploaded on the websites.

10. Index’s “Principles of moderation” contained the following:

“1. Deletion of comments
1.1. Especially forbidden are:
1. comments that, at the time of their posting, infringe the laws of Hungary, indicate or incite to crime or any other unlawful act...
3. vulgar, aggressive, threatening comments. What is vulgar, aggressive or threatening has to be decided by the moderators, in the light of the given topic...”

11. On 5 February 2010 MTE published an opinion under the title “Another unethical commercial conduct on the net” about two real estate management websites, owned by the same company. According to the opinion, the two websites provided thirty-day long advertising service for their users free of charge. Following the expiry of the thirty-day free period, the service became subject to a fee; and this without prior notification of the users. This was possible because, by registering on the website, the users accepted the terms and conditions stipulating that they could be changed unilaterally by the service provider. The opinion also noted that the service provider removed any obsolete advertisements and personal data from the websites only if any overdue charges were paid. The opinion concluded that the conduct of the service provider was unethical and misleading.

12. The opinion attracted some comments of users, acting under pseudonyms, amongst which there were the following:

“They have talked about these two rubbish real estate websites (“két szemét ingatlanos oldalról”) a thousand times already.”

“Is this not that Benkő-Sándor-sort-of sly, rubbish, mug company (“benkősándoros sunyi szemét lehúző cég”) again? I ran into it two years ago, since then they have kept sending me
emails about my overdue debts and this and that. I am above 100,000 [Hungarian forints] now. I have not paid and I am not going to. That’s it.”

13. On 8 February 2010 the Internet portal www.vg.hu, operated by Zöld Újság Zrt, reproduced the opinion word by word under the title “Another mug scandal”.

14. The consumer protection column of Index also wrote about the opinion under the title “Content providers condemn [one of the incriminated property websites]”, publishing the full text of the opinion. One of the user comments posted on Index by a reader acting under a pseudonym read as follows:

“They like this should go and shit a hedgehog and spend all their money on their mothers’ tombs until they drop dead.” (“Azért az ilyenek szarjanak sűnt és költsek az összes bevételüket anyjuk sírjára, amíg meg nem dögölnek.”)

15. On 17 February 2010 the company operating the websites concerned brought a civil action before the Budapest Regional Court against the applicants and Zöld Újság Zrt. The plaintiff claimed that the opinion, whose content was false and offensive, and the subsequent comments had infringed its right to good reputation.

Once learning of the impending court action, the applicants removed the impugned comments at once.

16. In their counterclaims before the Regional Court, the applicants argued that they, as intermediary publishers under Act no.CVIII of 2001, were not liable for the user comments. They noted that the business practice of the plaintiff, affecting wide ranges of consumers, attracted numerous complaints to the consumer protection organs and prompted several procedures against the company.

17. On 31 March 2011 the Regional Court partially sustained the claim, holding that the plaintiff’s right to good reputation had been infringed. As a preliminary remark, the court observed that consumer protection bodies had instituted various proceedings against the plaintiff company, since it had not informed its clients adequately about its business policies.

The Court found that the comments (see §§12 and 14 above) were offensive, insulting and humiliating and went beyond the acceptable limits of freedom of expression. The court rejected the applicants’ argument that they were only intermediaries and their sole obligation was to remove certain contents, in case of a complaint. It found that the comments constituted edited content, fell in the same category as readers’ letters and the respondents were liable for enabling their publication, notwithstanding the fact that later on they had removed them.

As regards the content of the opinion as such, the court found that it had contributed to an on-going social and professional debate on the questionable conduct of the real estate websites and did not exceed the acceptable level of criticism.

18. Both parties appealed. In their appeal the applicants argued that the plaintiff had not requested them to remove the offensive comments. Nonetheless, they had done so as soon as soon as they had been informed of the plaintiff’s action. They also argued that users’ comments were to be distinguished from readers’ letters, since these latter were only published on the basis of editorial decisions, whereas comments did not constitute edited content. They argued that, in respect of comments, they had only acted as service providers of information storage.

19. On 27 October 2011 the Budapest Court of Appeal upheld in essence the first-instance decision but amended its reasoning. It ordered each applicant to pay 5,000 Hungarian forints (HUF) as first-instance and HUF 36,000 as second-instance procedural fee.

20. The Court of Appeal held that – as opposed to readers’ letters whose publication was dependent on editorial decisions – the comments, unedited, reflected the opinions of the sole commenters. Notwithstanding that, the owner of the website concerned was liable for them. According to the court’s reasoning, Act no.CVIII of 2001, transposing Directive 2000/31/EC on Electronic Commerce into Hungarian law, did not apply to the applicants’ case since it only related to electronic services of commercial nature, in particular to purchases through the Internet. Under section 2(3) of the Act, electronic commercial services were information society-related services whose purpose was the sale, purchase or exchange of a tangible and moveable property, which was not the situation in the applicants’ case. In any event, pursuant to its section 1(4), the scope of the Act did not extend to expressions made by persons acting outside the sphere of economic or professional activities or public duties, even if uttered in connection with a purchase through the Internet. For the Court of Appeal, the comments were private utterances which did not fall under Act no.CVIII of 2001 on Electronic Commercial Services. Thus, there was no reason to assess the
meaning of the terms of ‘hosting service providers’ and ‘intermediaries’ under that Act. Nonetheless, the comments attracted the applicability of the Civil Code rules on personality rights, notably Article 78. Since the comments were injurious for the plaintiff, the applicants bore objective liability for their publication, irrespectively of the subsequent removal, which was only relevant for the assessment of any compensation.

21. The applicants lodged a petition for review with the Kúria. They argued that, in their interpretation of the relevant law, they were under no obligation to monitor or edit the comments uploaded by readers on their websites.

22. On 13 June 2012 the Kúria upheld the previous judgments. It stressed that the applicants, by enabling readers to make comments on their websites, had assumed objective liability for any injurious or unlawful comments made by those readers. It rejected the applicants’ argument that they were only intermediary providers which allowed them to escape any liability for the contents of comments, other than removing them if injurious to a third party. The Kúria held that the applicants were not intermediaries in terms of section 2(lc) of Act no.CVIII and they could not invoke the limited liability of hosting service providers. It shared the Court of Appeal’s view in finding that the comments were capable of harming the plaintiff’s good reputation and that the applicants’ liability consisted of their having allowed their publication.

The Kúria imposed HUF 75,000 on each applicant as review costs, including the costs of the plaintiff’s legal representation.

This decision was served on 2 October 2012.

23. The applicants introduced a constitutional complaint on 3 January 2013, arguing in essence that the courts’ rulings holding them responsible for the contents of the comments amounted to an unjustified restriction on their freedom of expression.

24. On 11 March 2013 the Constitutional Court declared the complaint admissible.

25. On 27 May 2014 the Constitutional Court dismissed the constitutional complaint, (decision no.19/2014. (V.30.) AB). In the analysis of the proportionality of the interference, the Constitutional Court explained the absence of unconstitutionality in the case as follows.

“[43] In the case concerned by the Kúria’s judgment, the operator of the webpage did not moderate the comments. The identities of those primarily responsible, unless figuring nominatively, are unknown; and for that reason, the liability lies with the operator of the webpage.

[44] In the present case, the aggrieved fundamental right is not the right to freedom of expression as such, but one of its particular elements, the right to freedom of the press.

[50] It is without doubt that blogs and comments constitute expressions and as such attract the protection of Chapter IX of the Fundamental Law.

[59] The liability incumbent on the operator of the webpage obviously restricts freedom of the press – which includes, without doubt, communication on the Internet.

[63] The legislation pursues a constitutionally justified aim. It is also suitable for that purpose in that, without the liability of the operator of the webpage, the person concerned could hardly receive compensation for the grievance. However, the proportionality of the restriction is open to doubt from two perspectives: is it proportionate to hold the operator of the webpage liable for the expression which proved to be unlawful; and moreover, is the extent of the liability (that is, the amount of compensation) proportionate?

[65] If the liability for the publication of comments is based on the very fact of the publication itself, it is not justified to distinguish between moderated and non-moderated comments in regard to the proportionality of the restriction on the fundamental right in question. … The Constitutional Court has already held that the liability of press organs – not of the author – as applied in order to protect personality rights is constitutional.”

[...]

The law

I. Alleged violation of article 10 of the Convention

29. The applicants complained that the rulings of the Hungarian courts establishing objective liability on the side of Internet websites for the contents of users’ comments amounts to an infringement of freedom of expression as provided in Article 10 of the Convention, which reads as follows:

“One. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority
and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.

2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary."

[...]

B. Merits
[...]

2. The Court's assessment

45. The Court notes that it was not in dispute between the parties that the applicants’ freedom of expression guaranteed under Article 10 of the Convention had been interfered with by the domestic courts' decisions. The Court sees no reason to hold otherwise.

46. Such an interference with the applicant company's right to freedom of expression must be "prescribed by law", have one or more legitimate aims in the light of §2 of Article 10, and be "necessary in a democratic society".

47. In the present case the parties' opinion differed as to whether the interference with the applicants’ freedom of expression was "prescribed by law". The applicants argued that under the European legislation hosting service providers had restricted liability for third-party comments. The Government referred to section 1(4) of Act no.CVIII of 2001 to the effect that private expressions, such as the impugned comments, fell outside the scope of that Act. They relied on section 75(1) and 78(1)-(2) of the Civil Code and argued that the applicants were liable for imparting and disseminating private opinions expressed by third-parties.

48. The Court observes that the Court of Appeal concluded that the applicants’ case did not concern electronic commercial activities, and, in any case, pursuant to its section 1(4), Act no.CVIII of 2001 was not applicable to the impugned comments (see §20 above). The Kúria, while upholding the second-instance judgment found, without further explanation, that the applicants were not intermediaries in terms of section 2(lc) of that Act (see §22 above).

The domestic courts, thus, chose to apply Article 78 of the Civil Code, although, apparently, for different reasons.

49. The Court reiterates in this context that it is not its task to take the place of the domestic courts. It is primarily for the national authorities, notably the courts, to interpret and apply domestic law (see, among others, Rekvényi v. Hungary [GC], no.25390/94, ¶35, [...]). The Court also reiterates that it is not for it to express a view on the appropriateness of methods chosen by the legislature of a respondent State to regulate a given field. Its task is confined to determining whether the methods adopted and the effects they entail are in conformity with the Convention (see Gorzelik and Others v. Poland [GC], no.44158/98, ¶67, [...]). Thus, the Court confines itself to examining whether the Kúria’s application of the relevant provisions of the Civil Code to the applicants’ situation was foreseeable for the purposes of Article 10 §2 of the Convention. As the Court has previously held, the level of precision required of domestic legislation – which cannot provide for every eventuality – depends to a considerable degree on the content of the law in question, the field it is designed to cover and the number and status of those to whom it is addressed (see Centro Europa 7 S.r.l. and Di Stefano v. Italy [GC], no.38433/09, ¶142, [...]). The Court has found that persons carrying on a professional activity, who are used to having to proceed with a high degree of caution when pursuing their occupation, can on this account be expected to take special care in assessing the risks that such activity entails (see Lindon, Otchakovskv-Laurens and July v. France [GC], nos.21279/02 and 36448/02, ¶41, [...]).

50. The Court notes that the Kúria did not embark on an explanation whether and how Directive 2000/31/EC was taken into account when interpreting section 2(lc) of Act no.CVIII of 2001 and arriving to the conclusion that the applicants were not intermediaries in terms of that provision, despite the applicants’ suggestion that the correct application of the EU law should have exculpated them in the circumstances.

51. Nonetheless, the Court is satisfied on the facts of this case that the provisions of the Civil Code made it foreseeable for a media publisher running a large Internet news portal for an economic purpose and for a self-regulatory body of Internet content providers, that they could, in
principle, be held liable under domestic law for unlawful comments of third-parties. Thus, the Court considers that the applicants was in a position to assess the risks related to their activities and that they must have been able to foresee, to a reasonable degree, the consequences which these could entail. It therefore concludes that the interference in issue was “prescribed by law” within the meaning of the second paragraph of Article 10 of the Convention (see mutatis mutandis, Delfi AS, cited above, §§125 to 129).

52. The Government submitted that the interference pursued the legitimate aim of protecting the rights of others. The Court accepts this.

53. It thus remains to be ascertained whether it was “necessary in a democratic society” in order to achieve the aim pursued.

(a) General principles

54. The fundamental principles concerning the question whether an interference with freedom of expression is “necessary in a democratic society” are well established in the Court’s case-law and have been summarised as follows (see, among other authorities, Hertel v. Switzerland, 25 August 1998, §46, [...] ; Steel and Morris v. the United Kingdom, no.68416/01, §87, [...] ; Mouvement raelien suisse v. Switzerland [GC], no.16354/06, §48, [...] ; Animal Defenders International v. the United Kingdom [GC], no.48876/08, §100, [...] ; and most recently in Delfi AS, cited above, §131):

“(...) Freedom of expression constitutes one of the essential foundations of a democratic society and one of the basic conditions for its progress and for each individual’s self-fulfilment. Subject to §2 of Article 10, it is applicable not only to ‘information’ or ‘ideas’ that are favourably received or regarded as inoffensive or as a matter of indifference, but also to those that offend, shock or disturb. Such are the demands of pluralism, tolerance and broadmindedness without which there is no ‘democratic society’. As set forth in Article 10, this freedom is subject to exceptions, which ... must, however, be construed strictly, and the need for any restrictions must be established convincingly ...

(ii) The adjective ‘necessary’, within the meaning of Article 10 §2, implies the existence of a ‘pressing social need’. The Contracting States have a certain margin of appreciation in assessing whether such a need exists, but it goes hand in hand with European supervision, embracing both the legislation and the decisions applying it, even those given by an independent court. The Court is therefore empowered to give the final ruling on whether a ‘restriction’ is reconcilable with freedom of expression as protected by Article 10.

(iii) The Court’s task, in exercising its supervisory jurisdiction, is not to take the place of the competent national authorities but rather to review under Article 10 the decisions they delivered pursuant to their power of appreciation. This does not mean that the supervision is limited to ascertaining whether the respondent State exercised its discretion reasonably, carefully and in good faith; what the Court has to do is to look at the interference complained of in the light of the case as a whole and determine whether it was ‘proportionate to the legitimate aim pursued’ and whether the reasons adduced by the national authorities to justify it are ‘relevant and sufficient’... In doing so, the Court has to satisfy itself that the national authorities applied standards which were in conformity with the principles embodied in Article 10 and, moreover, that they relied on an acceptable assessment of the relevant facts ...”

55. Furthermore, the Court has emphasised the essential function the press fulfils in a democratic society. Although the press must not overstep certain bounds, particularly as regards the reputation and rights of others and the need to prevent the disclosure of confidential information, its duty is nevertheless to impart – in a manner consistent with its obligations and responsibilities – information and ideas on all matters of public interest (see Bladet Tromsø and Stensaas v. Norway [GC], no.21980/93, §58, [...] ; Jersild v. Denmark, 23 September 1994, §31, [...] ; and De Haes and Gijseels v. Belgium, 24 February 1997, §37, [...] ). Journalistic freedom also covers possible recourse to a degree of exaggeration, or even provocation (see Couderc and Hachette Filipacchi Associés v. France [GC] (no.40454/07, §89, 10 November 2015; Bladet Tromsø and Stensaas, cited above, §59; and Prager and Oberschlick v. Austria, 26 April 1995, §38, [...] ). The limits of permissible criticism are narrower in relation to a private citizen than in relation to politicians or governments (see, for example, Delfi AS, cited above, §132; Castells v. Spain, 23 April 1992, §46, [...] ; Incal v. Turkey, 9 June 1998, §54, [...] ; and Tammer v. Estonia, no.41205/98, §62, [...] ).
56. Moreover, the Court has previously held that in the light of its accessibility and its capacity to store and communicate vast amounts of information, the Internet plays an important role in enhancing the public’s access to news and facilitating the dissemination of information in general (see Ahmet Yıldırım v. Turkey, no.3111/10, §48, […] Times Newspapers Ltd v. the United Kingdom (nos.1 and 2), nos.3002/03 and 23676/03, §27, […] and Delfi, cited above, §133). At the same time, in considering the “duties and responsibilities” of a journalist, the potential impact of the medium concerned is an important factor (see Delfi, cited above, §134; see also Jersild v. Denmark, cited above, §31).

57. The Court further reiterates that the right to protection of reputation is a right which is protected by Article 8 of the Convention as part of the right to respect for private life (see Chauvy and Others v. France, no.64915/01, §70, […] and Polanco Torres and Movilla Polanco v. Spain, no.34147/06, §40, 21 September 2010). In order for Article 8 to come into play, however, an attack on a person’s reputation must attain a certain level of seriousness and be made in a manner causing prejudice to personal enjoyment of the right to respect for private life (see Delfi AS, cited above, §137; Axel Springer AG v. Germany [GC], no.39954/08, §83, 7 February 2012; and A. v. Norway, no.28070/06, §64, 9 April 2009).

58. When examining whether there is a need for an interference with freedom of expression in a democratic society in the interests of the “protection of the reputation or rights of others”, the Court may be required to ascertain whether the domestic authorities have struck a fair balance when protecting two values guaranteed by the Convention which may come into conflict with each other in certain cases, namely on the one hand freedom of expression protected by Article 10, and on the other the right to respect for private life enshrined in Article 8 (see Delfi AS, cited above, §138; Axel Springer AG, cited above, §84; Hachette Filipacchi Associés v. France, no.71111/01, §43, 14 June 2007; MGN Limited v. the United Kingdom, no.39401/04, §142, 18 January 2011).

59. The Court has found that, as a matter of principle, the rights guaranteed under Articles 8 and 10 deserve equal respect, and the outcome of an application should not vary according to whether it has been lodged with the Court under Article 10 of the Convention by the publisher of an offending article or under Article 8 of the Convention by the person who has been the subject of that article. Accordingly, the margin of appreciation should be the same in both cases (see Axel Springer AG, cited above, §87, and Von Hannover v. Germany (no.2) [GC], nos.40660/08 and 60641/08, §106, […] with further references to the cases of Hachette Filipacchi Associés, cited above, §41; Timciuc v. Romania (dec.), no.28999/03, §144, 12 October 2010; and Mosley v. the United Kingdom, no.48009/08, §111, 10 May 2011). Where the balancing exercise between those two rights has been undertaken by the national authorities in conformity with the criteria laid down in the Court’s case-law, the Court would require strong reasons to substitute its view for that of the domestic courts (see Axel Springer AG, cited above, §88, and Von Hannover (no.2), cited above, §107, with further references to MGN Limited, cited above, §§150 and 155; and Palomo Sánchez and Others v. Spain [GC], nos.28955/06, 28957/06, 28959/06 and 28964/06, §57, 12 September 2011). In other words, there will usually be a wide margin afforded by the Court if the State is required to strike a balance between competing private interests or competing Convention rights (see Delfi AS, cited above, §139; Evans v. the United Kingdom [GC], no.6339/05, §77, […]; Chassagnou and Others v. France [GC], nos.25088/94, 28331/95 and 28443/95, §113, […] and Ashby Donald and Others v. France, no.36769/08, §40, 10 January 2013).

(b) Application of those principles to the present case
(i) Preliminary remarks and applicable criteria

60. In order to determine the standards applicable in the instant case, the Court will consider the nature of the applicants’ rights of expression in view of their role in the process of communication and the specific interest protected by the interference, namely — as was implied by the domestic courts — the rights of others.

61. The Court notes that both the first applicant, as a self-regulatory body of internet service providers, and the second applicant, as a large news portal, provided forum for the exercise of expression rights, enabling the public to impart information and ideas. Thus, the Court shares the Constitutional Court’s view according to which the applicants’ conduct must be assessed in the light of the principles applicable to the press (see §25 above).

62. The Court reiterates in this regard that although not publishers of the comments in the traditional sense, Internet news portals must, in principle, assume duties and responsibilities.
Because of the particular nature of the Internet, those duties and responsibilities may differ to some degree from those of a traditional publisher, notably as regards third-party contents (see *Delfi AS*, cited above, §113).

63. In particular, the Court has examined in the case of *Delfi AS* the duties and responsibilities under Article 10 §2 of large Internet news portals where they provide, for economic purposes, a platform for user-generated comments and where the users of such platforms engage in clearly unlawful expressions, amounting to hate speech and incitement to violence.

64. However, the present case is different. Although offensive and vulgar (see §§12 and 14 above), the incriminated comments did not constitute clearly unlawful speech; and they certainly did not amount to hate speech or incitement to violence. Furthermore, while the second applicant is the owner of a large media outlet which must be regarded as having economic interests, the first applicant is a non-profit self-regulatory association of Internet service providers, with no known such interests.

65. The domestic courts found that the impugned statements violated the personality rights and reputation of the plaintiff company, a moral person. At this juncture the Court notes that the domestic authorities accepted without any further analysis or justification that the impugned statements were injurious to the reputation of the plaintiff company.

66. As the Court has previously held, legal persons could not claim to be a victim of a violation of personality rights, whose holders could only be natural persons (see *Sdružení Jihočeské Matky v. Czech Republic* (dec.), no.19101/03, 10 July 2006). There is a difference between the commercial reputational interests of a company and the reputation of an individual concerning his or her social status. Whereas the latter might have repercussions on one’s dignity, for the Court, interests of commercial reputation are devoid of that moral dimension (see *Uj v. Hungary*, no.23954/10, §22, 19 July 2011). Moreover, the Court reiterates that there is an interest in protecting the commercial success and viability of companies, for the benefit of shareholders and employees, but also for the wider economic good. The State therefore enjoys a margin of appreciation as to the means it provides under domestic law to enable a company to challenge the truth, and limit the damage, of allegations which risk harming its reputation (see *Steel and Morris v. the United Kingdom*, no.68416/01, §94, […]; *Kuliś and Różyczki v. Poland*, no.27209/03, §35, […]).

67. However, in the present case it is not necessary to decide whether the plaintiff company could justifiably rely on its right to reputation, seen from the perspective of Article 8 of the Convention. It suffices to observe that the domestic courts found that the comments in question constituted an infringement of its personality rights. Indeed, it cannot be excluded that the impugned comments were injurious towards the natural person behind the company and that, in this sense, the decisions of the domestic courts intended to protect, in an indirect manner, that person from defamatory statements. The Court will therefore proceed under the assumption that – giving the benefit of the doubt to the domestic courts’ stance identifying a valid reputational interest – there was to be a balancing between the applicants’ Article 10 rights and the plaintiff’s Article 8 rights.

68. The Court has already had occasion to lay down the relevant principles which must guide its assessment in the area of balancing the protection of freedom of expression as enshrined in Article 10 and the protection of the reputation of those against whom allegations were made, a right which, as an aspect of private life, is protected by Article 8 of the Convention. It identified a number of relevant criteria, out of which the particularly pertinent in the present case, to which the Court will revert below, are: contribution to a debate of public interest, the subject of the report, the prior conduct of the person concerned, the content, form and consequences of the publication, and the gravity of the penalty imposed on the journalists or publishers (see *Couderc and Hachette Filipacchi Associés v. France* [GC], cited above, §93; *Von Hannover* (no.2), cited above, §§108 to 113, […]; and *Axel Springer AG*, cited above, §§90-95, 7 February 2012). At this juncture the Court would add that the outcome of such a balancing performed by the domestic courts will be acceptable in so far as those courts applied the appropriate criteria and, moreover, weighed the relative importance of each criterion with due respect paid to the particular circumstances of the case.

69. In the case of *Delfi AS*, the Grand Chamber identified the following specific aspects of freedom of expression in terms of protagonists playing an intermediary role on the Internet, as being relevant for the concrete assessment of the interference in question: the context of the comments, the measures applied by the applicant company in order to prevent or remove
defamatory comments, the liability of the actual authors of the comments as an alternative to the intermediary’s liability, and the consequences of the domestic proceedings for the applicant company (see Delfi AS, cited above, §§142-43).

70. These latter criteria were established so as to assess the liability of large Internet news portals for not having removed from their websites, without delay after publication, comments that amounted to hate speech and incitement to violence. However, for the Court, they are also relevant for the assessment of the proportionality of the interference in the present case, free of the pivotal element of hate speech. It is therefore convenient to examine the balancing, if any, performed by the domestic courts and the extent to which the relevant criteria (see Von Hannover (no.2), cited above, §§108 to 113) were applied in that process, with regard to the specific aspects dictated by the applicants’ respective positions (see Delfi AS, cited above, §§142-43).

71. Consequently, it has to be ascertained if the domestic authorities struck an appropriate balance between the applicants’ right under Article 10, as protagonists in providing Internet platform for, or inviting expressions from, third-parties on the one hand, and the rights of the plaintiff company not to sustain allegations infringing its rights under Article 8, on the other. In particular, in the light of the Kúria’s reasoning, the Court must examine whether the domestic courts’ imposition of liability on the applicants for third-party comments was based on relevant and sufficient reasons in the particular circumstances of the case.

The Court itself will proceed to assess the relevant criteria as laid down in its case-law to the extent that the domestic authorities failed to do so.

(ii) Context and content of the impugned comments

72. As regards the context of the comments, the Court notes that the underlying article concerned the business practice of two large real estate websites, which was deemed misleading and injurious to their clients, thus there was a public interest in ensuring an informed public debate over a matter concerning many consumers and Internet users. The conduct in question had already generated numerous complaints to the consumer protection organs and prompted various procedures against the company concerned (see §16 above). The Court is therefore satisfied that the comments triggered by the article can be regarded as going to a matter of public interest.

Moreover, against this background, the article cannot be considered to be devoid of a factual basis or provoking gratuitously offensive comments.

73. The Court attaches importance to the fact that the second applicant is the owner of a large news portal, run on a commercial basis and obviously attracting a large number of comments. On the contrary, there is no appearance that the situation of the first applicant, the self-regulatory association of Internet content providers, was in any manner similar; indeed, the latter’s publication of contents of predominantly professional nature was unlikely to provoke heated discussions on the Internet. At any rate, the domestic courts appear to have paid no attention to the role, if any, which the applicants respectively played in generating the comments.

74. As regards the contents of the comments, the domestic courts found that they had overstepped the acceptable limits of freedom of opinion and infringed the right to reputation of the plaintiff company, in that they were unreasonably offensive, injurious and degrading.

75. For the Court, the issue in the instant case is not defamatory statements of fact but value judgments or opinions, as was admitted by the domestic courts. They were denouncements of a commercial conduct and were partly influenced by the commentators’ personal frustration of having been tricked by the company. Indeed, the remarks can be considered as an ill-considered reaction (compare and contrast Palomo Sánchez and Others cited above, §73). They were posted in the context of a dispute over the business policy of the plaintiff company perceived as being harmful to a number of clients.

76. Furthermore, the expressions used in the comments were offensive, one of them being outright vulgar. As the Court has previously held, offence may fall outside the protection of freedom of expression if it amounts to wanton denigration, for example where the sole intent of the offensive statement is to insult (see Skafka v. Poland, no.43425/98, §34, 27 May 2003); but the use of vulgar phrases in itself is not decisive in the assessment of an offensive expression. For the Court, style constitutes part of the communication as the form of expression and is as such protected together with the content of the expression (see Uj, cited above, §23).

77. Without losing sight of the effects of defamation on the Internet, especially given the ease, scope and speed of the dissemination of information (see Delfi AS, cited above, §147), the Court also considers that regard must be had to the specificities of the style of communication on
certain Internet portals. For the Court, the expressions used in the comments, albeit belonging to a low register of style, are common in communication on many Internet portals – a consideration that reduces the impact that can be attributed to those expressions.

(iii) Liability of the authors of the comments

78. As regards the establishment, in the civil proceedings, of the commentators' identities, the Court notes that the domestic authorities did not at all address its feasibility or the lack of it. The Constitutional Court restricted its analysis to stating that the injured party was unlikely to receive any compensation without the liability of the operator of the Internet portal.

At this juncture, the Court notes that there is no appearance that the domestic courts enquired into the conditions of commenting as such or into the system of registration enabling readers to make comments on the applicants' websites.

79. The national courts were satisfied that it was the applicants that bore a certain level of liability for the comments, since they had "disseminated" defamatory statements (see §42 above), however without embarking on a proportionality analysis of the liability of the actual authors of the comments and that of the applicants. For the Court, the conduct of the applicants providing platform for third-parties to exercise their freedom of expression by posting comments is a journalistic activity of a particular nature (see Delphi AS, cited above, §§112-13). Even accepting the domestic courts' qualification of the applicants' conduct as "disseminating" defamatory statements, the applicant's liability is difficult to reconcile with the existing case-law according to which "punishment of a journalist for assisting in the dissemination of statements made by another person in an interview would seriously hamper the contribution of the press to discussion of matters of public interest and should not be envisaged unless there are particularly strong reasons for doing so" (see Jersild, cited above, §35; Thoma v. Luxembourg, no.36432/97, §62, [...] and, mutatis mutandis, Verlagsguppe News GmbH v. Austria, no.76918/01, §31, 14 December 2006, Print Zeitungsverlag GmbH v. Austria, no.26547/07, §39, 10 October 2013; and Delphi AS, cited above, §135).

(iv) Measures taken by the applicants and the conduct of the injured party

80. The Court observes that although the applicants immediately removed the comments in question from their websites upon notification of the initiation of civil proceedings (see §15 above), the Kúria found them liable on the basis of the Civil Code, since by enabling readers to make comments on those websites and in connection to the impugned article, they had assumed objective liability for any injurious or unlawful comments made by those readers. As the Budapest Court of Appeal held, the circumstances of removing the comments were not a matter relevant for the assessment of objective liability but one for the assessment of any compensation (see §20 above).

81. The Court observes that the applicants took certain general measures to prevent defamatory comments on their portals or to remove them. Both applicants had a disclaimer in their General terms and conditions stipulating that the writers of comments – rather than the applicants – were accountable for the comments. The posting of comments injurious to the rights of third parties were prohibited. Furthermore, according to the Rules of moderation of the second applicant, “unlawful comments” were also prohibited. The second applicant set up a team of moderators performing partial follow-up moderation of comments posted on its portal. In addition, both applicants had a notice-and-take-down system in place, whereby anybody could indicate unlawful comments to the service provider so that they be removed. The moderators and the service providers could remove comments deemed unlawful at their discretion (see §§7-10 above).

82. The domestic courts held that, by allowing unfiltered comments, the applicants should have expected that some of those might be in breach of the law. For the Court, this amounts to requiring excessive and impracticable forethought capable of undermining freedom of the right to impart information on the Internet.

83. The Court also observes that the injured company never requested the applicants to remove the comments but opted to seek justice directly in court – an element that did not attract any attention in the domestic evaluation of the circumstances.

Indeed, the domestic courts imposed objective liability on the applicants for “having provided space for injurious and degrading comments” and did not perform any examination of the conduct of either the applicants or the plaintiff.

(v) Consequences of the comments for the injured party

99
84. As the Court has previously held in the context of compensation for the protraction of civil proceedings, juristic persons may be awarded compensation for non-pecuniary damage, where consideration should be given to the company’s reputation (see Comingersoll S.A. v. Portugal [GC], no.35382/97, §35, […]). However, the Court reiterates that there is a difference between the commercial reputational interests of a company and the reputation of an individual concerning his or her social status. Whereas the latter might have repercussions on one’s dignity, for the Court the interests of commercial reputation are primarily of business nature and devoid of the same moral dimension which the reputation of individuals encompasses. In the instant application, the reputational interest at stake is that of a private company; it is thus a commercial one without relevance to moral character (see, mutatis mutandis, Uj, cited above, §22).

85. The consequences of the comments must nevertheless be put into perspective. At the time of the publication of the article and the impugned comments, there were already ongoing inquiries into the plaintiff company’s business conduct (see §17 above). Against this background, the Court is not convinced that the comments in question were capable of making any additional and significant impact on the attitude of the consumers concerned. However, the domestic courts do not appear to have evaluated whether the comments reached the requisite level of seriousness and whether they were made in a manner actually causing prejudice to a legal person’s right to professional reputation (see §57 above).

(vi) Consequences for the applicants
86. The applicants were obliged to pay the court fees, including the fee paid by the injured party for its legal representation (see §22 above), but no awards were made for non-pecuniary damage. However, it cannot be excluded that the court decision finding against the applicants in the present case might produce legal basis for a further legal action resulting a damage award. In any event, the Court is of the view that the decisive question when assessing the consequence for the applicants is not the absence of damages payable, but the manner in which Internet portals such as theirs can be held liable for third-party comments. Such liability may have foreseeable negative consequences on the comment environment of an Internet portal, for example by compelling it to close the commenting space altogether. For the Court, these consequences may have, directly or indirectly, a chilling effect on the freedom of expression on the Internet. This effect could be particularly detrimental for a non-commercial website such as the first applicant (compare and contrast Delfi AS, cited above, §161).

87. The Constitutional Court held that the operation of Internet portals allowing comments without prior moderation was a forum of the exercise of freedom of expression (see §25 above). Indeed, the Court stressed on many occasions the essential role which the press plays in a democratic society (see De Haes and Gijseels v. Belgium, cited above, §37) – a concept which in modern society undoubtedly encompasses the electronic media including the Internet.

88. However, the Court cannot but observe that the Hungarian courts paid no heed to what was at stake for the applicants as protagonists of the free electronic media. They did not embark on any assessment of how the application of civil-law liability to a news portal operator will affect freedom of expression on the Internet. Indeed, when allocating liability in the case, those courts did not perform any balancing at all between this interest and that of the plaintiff. This fact alone calls into question the adequacy of the protection of the applicants’ freedom-of-expression rights on the domestic level.

(vii) Conclusion
89. The Court considers that the rigid stance of the Hungarian courts reflects a notion of liability which effectively precludes the balancing between the competing rights according to the criteria laid down in the Court’s case law (see Von Hannover (no.2), cited above, §107).

90. At this juncture, the Court reiterates that it is not for it to express a view on the appropriateness of methods chosen by the legislature of a respondent State to regulate a given field. Its task is confined to determining whether the methods adopted and the effects they entail are in conformity with the Convention (see Gorzelik and Others v. Poland, cited above, §67).

91. However, in the case of Delfi AS, the Court found that if accompanied by effective procedures allowing for rapid response, the notice-and-take-down-system could function in many cases as an appropriate tool for balancing the rights and interests of all those involved. The Court sees no reason to hold that such a system could not have provided a viable avenue to protect the commercial reputation of the plaintiff. It is true that, in cases where third-party user comments take the form of hate speech and direct threats to the physical integrity of individuals, the rights and
interests of others and of the society as a whole might entitle Contracting States to impose liability on Internet news portals if they failed to take measures to remove clearly unlawful comments without delay, even without notice from the alleged victim or from third parties (see Delfi AS, cited above, §159). However, the present case did not involve such utterances.

The foregoing considerations are sufficient for the Court to conclude that there has been a violation of Article 10 of the Convention.

[...] For these reasons, the Court, unanimously,
1. Declares the application admissible;
2. Holds that there has been a violation of Article 10 of the Convention;
3. Holds
   (a) that the respondent State is to pay the applicants, jointly, within three months from the date on which the judgment becomes final in accordance with Article 44 §2 of the Convention, EUR 5,100 (five thousand one hundred euros), plus any tax that may be chargeable to the applicants, in respect of costs and expenses, to be converted into the currency of the respondent State at the rate applicable at the date of settlement;
   (b) that from the expiry of the above-mentioned three months until settlement simple interest shall be payable on the above amount at a rate equal to the marginal lending rate of the European Central Bank during the default period plus three percentage points.

[...]

Concurring opinion of Judge Kūris
1. Somewhat similarly to Delfi AS v. Estonia (GC) (no.64569/09, [...] ), which was, in the Court’s own words, “the first case in which the Court has been called upon to examine a complaint of this type [regarding the liability of Internet providers for the contents of comments]”, the present case is the first in which the principles set forth in Delfi AS, to the balanced reasoning in which I subscribe, have been called upon to be applied and, at the same time, tested.

2. Together with my colleagues, I voted for the finding of a violation of Article 10 of the Convention. The vulgar and offensive comments dealt with in the present case were value judgments of no value whatsoever; however, they did not incite violence, did not stoop to the level of hate speech and, at least in this most important respect, could not a priori be viewed by the applicants as “clearly unlawful”. This is essentially what distinguishes these comments from the hate speech dealt with in Delfi AS. This decisive difference is rightly noted in, inter alia, §64 of the judgment. Thus, although it results in the opposite conclusion to that found in Delfi AS, the present judgment does not, in my opinion, depart from the Delfi AS principles.

3. Consequently, this judgment should in no way be employed by Internet providers, in particular those who benefit financially from the dissemination of comments, whatever their contents, to shield themselves from their own liability, alternative or complementary to that of those persons who post degrading comments, for failing to take appropriate measures against these envenoming statements. If it is nevertheless used for that purpose, this judgment could become an instrument for (again!) whitewashing the Internet business model, aimed at profit at any cost.

If, alas, such a regrettable turn of events should occur, those in the Internet business would not stand alone in their moral responsibility for further contamination of the public sphere. And we cannot pretend that we do not know who – if not personally, still certainly institutionally – would have to share that responsibility. If things develop in that direction, then Judge Boštjan Zupančič’s pointed remark in his concurring opinion in Delfi AS would become even more pertinent [...] :

“I do not know why the national courts hesitate in adjudicating these kinds of cases and affording strict protection of personality rights and decent compensation to those who have been subject to these kinds of abusive verbal injuries, but I suspect that our own case-law has something to do with it.”

4. This is the first post-Delfi judgment, but, of course, it will not be the last. It is confined to the individual circumstances of this particular case. There will inevitably be other cases dealing with liability for the contents of Internet messages and the administration thereof. Today, it is too early to draw generalising conclusions. One should look forward to these future cases, with the hope that the present judgment, although it may now appear to some as a step back from Delfi AS, will prove to be merely further evidence that the balance to be achieved in cases of this type is a very subtle one.
DISCUSSIONE

1. Il caso in esame richiama più volte il caso Delfi: quali sono le differenze e quali le similitudini?
2. I titolari dei siti web sono considerati come service providers o invece (o anche) come editori delle pubblicazioni on-line?
3. I titolari dei siti web dovrebbero essere responsabile per i commenti dei lettori agli articoli pubblicati sul portale? Se sì, sempre, o solo a certe condizioni? Nel caso, quali?
4. I titolari dei siti web ricoprono un “ruolo attivo” sulla pubblicazione dei commenti dei lettori?
5. Ai titolari dei siti web possono essere ascritte la violazione di un obbligo generalizzato di sorveglianza sui contenuti pubblicati?
6. Nella sentenza viene compiuta una distinzione tra commenti offensivi e volgari e commenti che non costituiscono espressioni chiaramente illegali? Cosa ne pensate?

****

NORME

- artt.8, 10, CEDU
4.4. Ruolo neutro o attivo del service provider

Corte di Giustizia dell’Unione Europea, 23 marzo 2010 (cause da C-236/08 a C-238/08)

1. Le domande di pronuncia pregiudiziale vertono sull’interpretazione dell’art.5, nn.1 e 2, della [...] direttiva [...] 21 dicembre 1988, 89/104/CEE, sul ravvicinamento delle legislazioni degli Stati membri in materia di marchi d’impresa [...], dell’art.9, n.1, del regolamento (CE) [...] 20 dicembre 1993, n.40/94, sul marchio comunitario [...], e dell’art.14 della direttiva [...] 8 giugno 2000, 2000/31/CE, relativa a taluni aspetti giuridici dei servizi della società dell’informazione, in particolare il commercio elettronico, nel mercato interno («Direttiva sul commercio elettronico») [...].


II - Cause principali e questioni pregiudiziali
A – Il servizio di posizionamento «AdWords»

22. La Google gestisce un motore di ricerca su Internet. Quando un utente di Internet effettua una ricerca a partire da una o più parole, il motore di ricerca visualizza, in ordine decrescente di pertinenza, i siti che sembrano meglio corrispondere a tali parole. Si tratta dei risultati cosiddetti «naturali» della ricerca.

23. La Google propone inoltre un servizio di posizionamento a pagamento denominato «AdWords». Tale servizio consente a qualsiasi operatore economico di far apparire un link pubblicitario verso il suo sito mediante la selezione di una o più parole chiave, qualora tale o tali parole coincidano con quella o quelle contenute nella richiesta indirizzata da un utente di Internet al motore di ricerca. Tale link pubblicitario appare nella rubrica «link sponsorizzati», visualizzata sia sul lato destro dello schermo, a destra dei risultati naturali, sia nella parte superiore dello schermo, al di sopra di tali risultati.

24. Detto link pubblicitario è accompagnato da un breve messaggio commerciale. Tale link e tale messaggio costituiscono, insieme, l’annuncio visualizzato nella succitata rubrica.

25. L’inserzionista è tenuto a pagare il servizio di posizionamento per ogni selezione del link pubblicitario. Tale pagamento è calcolato in funzione, in particolare, del «prezzo massimo per click» che, al momento della conclusione del contratto di servizio di posizionamento con la Google, l’inserzionista ha dichiarato di essere disposto a pagare nonché del numero di click su tale link da parte degli utenti di Internet.

26. Più inserzionisti possono selezionare la stessa parola chiave. L’ordine in cui vengono visualizzati i loro link pubblicitari in tal caso sarà determinato, in particolare, in base al prezzo massimo per click, da quanto volte i detti link sono stati selezionati in precedenza, nonché dalla qualità dell’annuncio come valutata dalla Google. In qualunque momento l’inserzionista può migliorare la sua posizione nell’ordine di visualizzazione fissando un prezzo massimo per click più alto oppure provando a migliorare la qualità del suo annuncio.

27. La Google ha messo a punto un processo automatizzato per consentire la selezione di parole chiave e la creazione di annunci. Gli inserzionisti selezionano le parole chiave, redigono il messaggio commerciale e inseriscono il link al loro sito.

B – Causa C-236/08

28. La Vuitton, che commercializza in particolare borse di lusso e altri prodotti di pelletteria, è titolare del marchio comunitario «Vuitton» e dei marchi nazionali francesi «Louis Vuitton» e «LV». È pacifico che tali marchi sono notori.
29. Agli inizi del 2003, la Vuitton ha fatto constatare che, utilizzando il motore di ricerca della Google, l’inserimento da parte degli utenti di Internet dei termini costituenti i suoi marchi faceva apparire, nella rubrica «link sponsorizzati», alcuni link verso siti che offrivano imitazioni di prodotti della Vuitton. È stato inoltre accertato che la Google offriva agli inserzionisti la possibilità di selezionare non solo parole chiave corrispondenti ai marchi della Vuitton, ma anche tali parole chiave associate ad espressioni indicative attività di imitazione, quali «imitazione» e «copia».

30. La Vuitton ha citato in giudizio la Google al fine di far accertare, in particolare, che quest’ultima aveva arrecato pregiudizio ai suoi marchi.

31. La Google è stata condannata per contraffazione dei marchi della Vuitton con sentenza del Tribunal de Grande Instance de Paris (Tribunale di Parigi) 4 febbraio 2005 e, successivamente, in appello con sentenza della Cour d’Appel de Paris (Corte d’appello di Parigi) 28 giugno 2006. Essa ha proposto un ricorso per cassazione contro quest’ultima sentenza.

32. In tale contesto, la Cour de Cassation (Corte di Cassazione francese) ha deciso di sospendere il procedimento e di sottoporre alla Corte le seguenti questioni pregiudiziali:

   «1) Se gli artt.5, n.1, lett.a) e b) della direttiva 89/104, e 9, n.1, lett.a) e b), del regolamento n.40/94, debbano essere interpretati nel senso che il prestatore del servizio di posizionamento a pagamento che mette a disposizione degli inserzionisti parole chiave che riproducono o imitano marchi registrati, e organizza, in forza del contratto di posizionamento, la creazione e la visualizzazione privilegiata, partendo da tali parole chiave, di link pubblicitari verso siti sui quali sono offerti prodotti contraffatti faccia un uso di tali marchi che il [loro] titolare ha il diritto di vietare.

   2) Se, nel caso in cui i marchi siano marchi notori, il titolare possa opporsi ad un tale uso, in forza dell’art.5, n.2, della direttiva [89/104], e dell’art.9, n.1, lett.c), del regolamento [n.40/94].

   3) Nel caso in cui un tale uso non costituisca un uso che può essere vietato dal titolare del marchio in applicazione della direttiva [89/104] e del regolamento [n.40/94], se il prestatore del servizio di posizionamento a pagamento possa essere considerato fornitore di un servizio della società dell’informazione consistente nella memorizzazione delle informazioni fornite da un destinatario del servizio, ai sensi dell’art.14 della direttiva 2000/31, di guisa che non è possibile ravvisare una sua responsabilità prima che egli sia stato informato dal titolare del marchio dell’uso illecito del segno da parte dell’inserzionista».

C – Causa C-237/08

33. La Viaticum è titolare dei marchi francesi «Bourse des Vols», «Bourse des Voyages» e «BDV», registrati per servizi relativi all’organizzazione di viaggi.

34. La Luteciel svolge un’attività di prestazione di servizi informatici per conto di agenzie di viaggi. Essa si occupa della creazione e della gestione del sito Internet della Viaticum.

35. La Viaticum e la Luteciel hanno fatto constatare che, in occasione dell’utilizzo del motore di ricerca della Google da parte degli utenti di Internet, l’inserimento dei termini costituenti i marchi succitati faceva apparire, nella rubrica «link sponsorizzati», alcuni link verso siti di concorrenti della Viaticum. È stato inoltre accertato che la Google offriva agli inserzionisti la possibilità di selezionare a tale scopo parole chiave corrispondenti a detti marchi.

36. La Viaticum e la Luteciel hanno citato in giudizio la Google. Con sentenza 13 ottobre 2003, il Tribunal de Grande Instance de Nanterre (Tribunale di Nanterre) ha dichiarato che la Google aveva commesso atti di contraffazione di marchio e l’ha condannata a risarcire il danno subito dalla Viaticum e dalla Luteciel. La Google ha interposto appello dinanzi alla Cour d’appello de Versailles (Corte d’appello di Versailles). Quest’ultima, con sentenza 13 marzo 2005, ha dichiarato che la Google aveva concorso a commettere atti di contraffazione e ha confermato la sentenza 13 ottobre 2003. La Google ha proposto un ricorso per cassazione contro quest’ultima sentenza.

37. In tale contesto, la Cour de cassation ha deciso di sospendere il procedimento e di sottoporre alla Corte le seguenti questioni pregiudiziali:

   «1) Se l’art.5, n.1, lett.a) e b) della direttiva 89/104 debbano essere interpretati nel senso che il prestatore del servizio di posizionamento a pagamento che mette a disposizione degli inserzionisti parole chiave che riproducono o imitano marchi registrati, e organizza, in forza del contratto di posizionamento, la creazione e la visualizzazione privilegiata, partendo da tali parole chiave, di link pubblicitari verso siti sui quali sono offerti prodotti identici o simili a quelli contraddistinti dal marchio, debbano essere considerati fornitore di un servizio del marchio in applicazione della direttiva [89/104] e del regolamento [n.40/94], se il prestatore del servizio di posizionamento a pagamento possa essere considerato fornitore di un servizio della
società dell’informazione consistente nella memorizzazione delle informazioni fornite da un destinatario del servizio, ai sensi dell’art.14 della direttiva 2000/31, di guisa che non è possibile ravvisare una sua responsabilità prima che egli sia stato informato dal titolare del marchio dell’uso illecito del segno da parte dell’inserzionista».

D – Causa C-238/08


41. In tale contesto, la Cour de Cassation ha deciso di sospendere il procedimento e di sottoporre alla Corte le seguenti questioni pregiudiziali:

«1) Se il fatto che un operatore economico dia in opzione, tramite un contratto di posizionamento a pagamento su Internet, una parola chiave che, se utilizzata per una ricerca, provoca la visualizzazione di un link che offre la possibilità di connettersi ad un sito utilizzato da tale operatore per mettere in vendita prodotti o servizi, e che riproduce o imita un marchio registrato da un terzo per contraddistinguere prodotti identici o simili, senza l’autorizzazione del titolare di tale marchio, leda di per se stesso il diritto esclusivo garantito a quegli enti marchiati», pubblicitari verso siti sui quali sono offerti prodotti identici o simili a quelli contraddistinti dal marchio, la creazione e la visualizzazione privilegiata, partendo da tali parole chiave, di link che riproducono o imitano marchi registrati e organizza, in forza del contratto di posizionamento, la creazione e la visualizzazione privilegiata, partendo da tali parole chiave, di link pubblicitari verso siti sui quali sono offerti prodotti identici o simili a quelli contraddistinti dal marchio registrato fa oggetto di un tali marchi che il loro titolare ha il diritto di vietare.

3) Nel caso in cui un tale uso non costituisca un uso che può essere vietato dal titolare del marchio in app
della direttiva 89/104, la prima questione nella causa C-236/08, che è opportuno esaminare congiuntamente, il giudice del rinvio chiede, in sostanza, se l’art.5, n.1, lett.a) e b), della direttiva 89/104 e l’art.9, n.1, lett.a) e b), del regolamento n.40/94 debbano essere interpretati nel senso che il titolare di un marchio ha il diritto di vietare a un terzo di visualizzare o di permettere la possui delle informazioni fornite da un destinatario del servizio, ai sensi dell’art.14 della direttiva 2000/31, di guisa che non è possibile ravvisare una sua responsabilità prima che egli sia stato informato dal titolare del marchio dell’uso illecito del segno da parte dell’inserzionista». 

III – Sulle questioni pregiudiziali

A – Sull’impiego di parole chiave corrispondenti a marchi altrui nell’ambito di un servizio di posizionamento su Internet

1. Considerazioni preliminari

42. È pacifico che le cause principali scaturiscono dall’impiego, quali parole chiave nell’ambito di un servizio di posizionamento su Internet, di segni corrispondenti a marchi di impresa, senza che i titolari di questi ultimi abbiano prestato il loro consenso. Dette parole chiave sono state scelte da clienti del prestatore del servizio di posizionamento e sono state accettate e memorizzate da quest’ultimo. I clienti in questione commercializzano imitazioni dei prodotti del titolare del marchio (causa C-236/08) oppure sono semplicemente concorrenti di quest’ultimo (cause C-237/08 e C-238/08).

43. Con la prima questione nella causa C-236/08, la prima questione nella causa C-237/08 nonché la prima e la seconda questione nella causa C-238/08, che è opportuno esaminare congiuntamente, il giudice del rinvio chiede, in sostanza, se l’art.5, n.1, lett.a) e b), della direttiva 89/104 e l’art.9, n.1, lett.a) e b), del regolamento n.40/94 debbano essere interpretati nel senso che il titolare di un marchio ha il diritto di vietare a un terzo di visualizzare o di permettere la
visualizzazione di un annuncio, per prodotti o servizi identici o simili a quelli per i quali detto marchio è registrato, a partire da una parola chiave identica o simile a tale marchio, che, senza il consenso di detto titolare, tale terzo ha selezionato o memorizzato nell’ambito di un servizio di posizionamento su Internet.

44. La prima questione nella causa C-236/08, la prima questione nella causa C-237/08 e la seconda questione nella causa C-238/08 si concentrano, in proposito, sulla memorizzazione di una siffatta parola chiave da parte del prestatore del servizio di posizionamento e sull’organizzazione, da parte di quest’ultimo, della visualizzazione dell’annuncio del suo cliente a partire da detta parola, mentre la prima questione nella causa C-238/08 verte sulla selezione del segno come parola chiave da parte dell’inserzionista e sulla visualizzazione dell’annuncio risultante da detta selezione mediante il meccanismo del posizionamento.

[...]

d) Conclusione

99. Alla luce delle suesposte considerazioni, occorre risolvere la prima questione nella causa C-236/08, la prima questione nella causa C-237/08 nonché la prima e la seconda questione nella causa C-238/08, dichiarando che:

– gli artt.5, n.1, lett.a), della direttiva 89/104 e 9, n.1, lett.a), del regolamento n.40/94 devono essere interpretati nel senso che il titolare di un marchio può vietare ad un inserzionista di fare pubblicità – a partire da una parola chiave identica a detto marchio, selezionata da tale inserzionista nell’ambito di un servizio di posizionamento su Internet senza il consenso dello stesso titolare – a prodotti o servizi identici a quelli per cui detto marchio è registrato, qualora la pubblicità di cui trattasi non consenta, o consente soltanto difficilmente, all’utente medio di Internet di sapere se i prodotti o i servizi indicati nell’annuncio provengano dal titolare del marchio o da un’impresa economicamente connessa a quest’ultimo o invece da un terzo; – il prestatore di un servizio di posizionamento su Internet che memorizza come parola chiave un segno identico a un marchio e organizza, a partire da quest’ultimo, la visualizzazione di annunci non fa un uso di tale segno ai sensi dell’art.5, n.1, della direttiva 89/104 o dell’art.9, n.1, lett.a) e b), del regolamento n.40/94.

3. Sull’interpretazione degli artt.5, n.2, della direttiva 89/104 e 9, n.1, lett.c), del regolamento n.40/94

100. Con la sua seconda questione nella causa C-236/08, il giudice del rinvio chiede, in sostanza, se il prestatore di un servizio di posizionamento su Internet, che memorizza come parola chiave un segno identico a un marchio notorio e organizza, a partire dalla stessa parola chiave, la visualizzazione di annunci, faccia un uso di tale segno che il titolare di detto marchio può vietare ai sensi dell’art.5, n.2, della direttiva 89/104 o, qualora detto segno sia identico a un marchio comunitario notorio, ai sensi dell’art.9, n.1, lett.c), del regolamento n.40/94.

101. Secondo le constatazioni del giudice del rinvio, in tale causa è stato accertato che la Google consentiva agli inserzionisti che offrono agli utenti di Internet imitazioni dei prodotti della Vuitton di selezionare parole chiave corrispondenti ai marchi della Vuitton, associate a parole chiave quali «imitazione» e «copia».

102. La Corte ha già avuto modo di dichiarare nel caso di offerta di vendita di imitazioni, che, quando un terzo tenta, mediante l’uso di un segno identico o simile a un marchio notorio, di porsi nel solco tracciato da quest’ultimo, al fine di beneficiare del suo potere attrattivo, della sua reputazione e del suo prestigio, nonché di sfruttare, senza qualsivoglia compensazione economica e senza dover operare sforzi propri a tale scopo, lo sforzo commerciale effettuato dal titolare del marchio per creare e mantenere l’immagine di detto marchio, si deve considerare il vantaggio derivante da siffatto uso come indebitamente tratto dal carattere distintivo o dalla notorietà del marchio in parola (sentenza L’Oréal e a., cit., p.to 49).


104. Tuttavia, per quanto attiene alla questione se il prestatore di un servizio di posizionamento, quando memorizza tali segni associati a termini come «imitazione» e «copia» quali parole chiave e consente la visualizzazione di annunci partendo dagli stessi termini, faccia a sua volta un uso che il titolare di detti marchi può vietare, occorre ricordare, come indicato ai p.ti 55-57 della presente sentenza, che tali atti del prestatore non costituiscono un uso ai sensi degli artt.5 della direttiva 89/104 e 9 del regolamento n.40/94.

106
105. Pertanto, occorre risolvere la seconda questione presentata nella causa C-236/08 dichiarando che il prestatore di un servizio di posizionamento su Internet che memorizza, come parola chiave, un segno identico a un marchio notorio e, a partire dalla stessa, organizza la visualizzazione di annunci, non fa un uso di tale segno ai sensi dell’art.5, n.2, della direttiva 89/104 ovvero dell’art.9, n.1, lett.c), del regolamento n.40/94.

**B – Sulla responsabilità del prestatore del servizio di posizionamento**

106. Con la sua terza questione nella causa C-236/08, la sua seconda questione nella causa C-237/08 e la sua terza questione nella causa C-238/08 il giudice del rinvio chiede, in sostanza, se l’art.14 della direttiva 2000/31 debba essere interpretato nel senso che un servizio di posizionamento su Internet costituisca un servizio della società dell’informazione consistente nella memorizzazione di informazioni fornite dall’inserzionista, di guisa che tali dati sono oggetto di un’attività di “hosting” ai sensi di tale articolo e che, pertanto, non è possibile ravvisare una responsabilità del prestatore del servizio di posizionamento prima che egli sia stato informato del comportamento illecito di detto inserzionista.


108. La Vuitton, la Viaticum e la CNRRH sostengono, tuttavia, che un servizio di posizionamento quale AdWords non è un servizio della società dell’informazione come definito dalle citate disposizioni della direttiva 2000/31, cosicché il prestatore di un tale servizio non può in alcun caso godere di dette limitazioni della responsabilità. La Google e la Commissione europea sostengono il contrario.

109. La limitazione della responsabilità di cui all’art.14, n.1, della direttiva 2000/31 si applica in caso di “prestazione di un servizio della società dell’informazione consistente nella memorizzazione di informazioni fornite da un destinatario del servizio” e significa che il prestatore di un tale servizio non può essere ritenuto responsabile per i dati che ha memorizzato su richiesta di un destinatario del servizio in parola, salvo che tale prestatore, dopo aver preso conoscenza, mediante un’informazione fornita dalla persona lesa o in altro modo, della natura illecita di tali dati o di attività di detto destinatario, abbia omesso di prontamente rimuovere tali dati o disabilitare l’accesso agli stessi.

110. Come indicato ai p.to 14 e 15 della presente sentenza, il legislatore ha definito la nozione di “servizio della società dell’informazione” come comprensivo dei servizi prestati a distanza mediante attrezzature elettroniche di trattamento e di memorizzazione di dati, a richiesta individuale di un destinatario di servizi e, normalmente, dietro retribuzione. Tenuto conto delle caratteristiche del servizio di posizionamento di cui trattasi nelle cause principali, riassunte al p.to 23 della presente sentenza, si deve concludere che tale servizio presenta tutti gli elementi di tale definizione.

111. Non si può contestare, inoltre, il fatto che il prestatore di un servizio di posizionamento trasmette informazioni del destinatario di detto servizio, vale a dire l’inserzionista, su una rete di comunicazione accessibile agli utenti di Internet e memorizza, vale a dire salva sul proprio server, tali dati, quali le parole chiave selezionate dall’inserzionista, il link pubblicitario e il messaggio commerciale che lo accompagna, nonché l’indirizzo del sito dell’inserzionista.

112. È necessario inoltre, affinché la memorizzazione effettuata dal prestatore di un servizio di posizionamento possa rientrare nella previsione dell’art.14 della direttiva 2000/31, che il comportamento di tale prestatore si limiti a quello di un “prestatore intermediario” nel senso voluto dal legislatore nell’ambito della sezione 4 di tale direttiva.

113. Dal quarantaduesimo “considerando” della direttiva 2000/31 risulta, a tal proposito, che le deroghe alla responsabilità previste da tale direttiva riguardano esclusivamente i casi in cui l’attività di prestatore di servizi della società dell’informazione sia di ordine «meramente tecnico, automatico e passivo», con la conseguenza che detto prestatore «non conosce né controlla le informazioni trasmesse o memorizzate». 
114. Pertanto, al fine di verificare se la responsabilità del prestatore del servizio di posizionamento possa essere limitata ai sensi dell’art.14 della direttiva 2000/31, occorre esaminare se il ruolo svolto da detto prestatore sia neutro, in quanto il suo comportamento è meramente tecnico, automatico e passivo, comportante una mancanza di conoscenza o di controllo dei dati che esso memorizza.

115. Per quanto attiene al servizio di posizionamento di cui trattasi nelle cause principali, dal fascicolo e dalla descrizione di cui ai p.ti 23 e seguenti della presente sentenza si evince che la Google, tramite software da essa sviluppati, effettua un trattamento dei dati inseriti dagli inserzionisti ottenendo la visualizzazione di annunci a condizioni stabilite dalla stessa Google. Quest’ultima stabilisce quindi l’ordine di visualizzazione in funzione, in particolare, del pagamento degli inserzionisti.

116. Occorre osservare che la semplice circostanza che il servizio di posizionamento sia a pagamento, che la Google stabilisca le modalità di pagamento, o ancora che essa dia informazioni di ordine generale ai suoi clienti, non può avere come effetto di privare la Google delle deroghe in materia di responsabilità previste dalla direttiva 2000/31.

117. Del pari, il fatto che la parola chiave selezionata e il termine di ricerca inserito da un utente di Internet coincidano non è di per sé sufficiente a ritenere che la Google conosca o controlli i dati inseriti dagli inserzionisti nel suo sistema e memorizzati sul suo server.

118. Nell’ambito dell’esame di cui al p.to 114 della presente sentenza, è invece rilevante il ruolo svolto dalla Google nella redazione del messaggio commerciale che accompagna il link pubblicitario o nella determinazione o selezione di tali parole chiave.

119. Proprio alla luce delle suesposte considerazioni spetta al giudice nazionale, che meglio può conoscere le modalità concrete della fornitura del servizio nella causa principale, valutare se il ruolo svolto dalla Google corrisponda a quello descritto al p.to 114 della presente sentenza.

120. Da ciò consegue che occorre risolvere la terza questione nella causa C-236/08, la seconda questione nella causa C-237/08 e la terza questione nella causa C-238/08 dichiarando che l’art.14 della direttiva 2000/31 deve essere interpretato nel senso che la norma ivi contenuta si applica al prestatore di un servizio di posizionamento su Internet qualora detto prestatore non abbia svolto un ruolo attivo atto a conferirgli la conoscenza o il controllo dei dati memorizzati.

Per questi motivi, la Corte (Grand Sezione) dichiara:

1) Gli artt.5, n.1, lett.a), della […] direttiva […] 21 dicembre 1988, 89/104/CEE, sul ravvivamento delle legislazioni degli Stati membri in materia di marchi d’impresa, e 9, n.1, lett.a), del regolamento (CE) […] 20 dicembre 1993, n.40/94, sul marchio comunitario, devono essere interpretati nel senso che il titolare di un marchio può vietare ad un inserzionista di fare pubblicità – a partire da una parola chiave identica a detto marchio, selezionata da tale inserzionista nell’ambito di un servizio di posizionamento su Internet senza il consenso dello stesso titolare – a prodotti o servizi identici a quelli per cui detto marchio è registrato, qualora la pubblicità di cui trattasi non consenta, o consenta soltanto difficilmente, all’utente medio di Internet di sapere se i prodotti o i servizi indicati nell’annuncio provengano dal titolare del marchio o da un’impresa economicamente connessa a quest’ultimo o invece da un terzo.

2) Il prestatore di un servizio di posizionamento su Internet che memorizza come parola chiave un segno identico a un marchio e organizza, a partire da quest’ultimo, la visualizzazione di annunci non fa un uso di tale segno ai sensi dell’art.5, nn.1 e 2, della direttiva 89/104 o dell’art.9, n.1, del regolamento n.40/94.

3) L’art.14 della direttiva […] 8 giugno 2000, 2000/31/CE, relativa a taluni aspetti giuridici dei servizi della società dell’informazione, in particolare il commercio elettronico, nel mercato interno («Direttiva sul commercio elettronico»), deve essere interpretato nel senso che la norma ivi contenuta si applica al prestatore di un servizio di posizionamento su Internet qualora detto prestatore non abbia svolto un ruolo attivo atto a conferirgli la conoscenza o il controllo dei dati memorizzati. Se non ha svolto un siffatto ruolo, detto prestatore non può essere ritenuto responsabile per i dati che egli ha memorizzato su
richiesta di un inserzionista, salvo che, essendo venuto a conoscenza della natura illecita di tali dati o di attività di tale inserzionista, egli abbia omesso di prontamente rimuovere tali dati o disabilitare l’accesso agli stessi.

*****

DISCUSSIONE

1. Un operatore economico può utilizzare, nell’ambito di un servizio di posizionamento su Internet, un marchio di cui è titolare un diverso soggetto, senza il consenso di questi? Perché? Siete d’accordo?

2. Il prestatore di un servizio di posizionamento su Internet che memorizza come parola chiave un segno identico a un marchio notorio fa un uso di tale segno ai sensi della normativa sul diritto d’autore? Perché? Siete d’accordo?

3. Il servizio di posizionamento su Internet costituisce un servizio della società dell’informazione (hosting)?

4. A quali condizioni il prestatore di tale servizio di hosting può avvalersi delle norme di esenzione della responsabilità previste per i service providers?

*****

NORME

- art.5, nn.1 e 2, direttiva 89/104/CEE
- art.9, regolamento (CE) n.40/94
- art.14, direttiva 2000/31/CE
4.5. Responsabilità del fornitore di rete locale senza fili

Corte di Giustizia dell’Unione Europea, 15 settembre 2016 (causa C-484/14)

1. La domanda di pronuncia pregiudiziale verte sull’interpretazione dell’art.12, §1, della direttiva 2000/31/CE […] dell’8 giugno 2000, relativa a taluni aspetti giuridici dei servizi della società dell’informazione, in particolare il commercio elettronico, nel mercato interno («direttiva sul commercio elettronico») […]


Fatti del procedimento principale e questioni pregiudiziali

22. Il sig. Mc Fadden gestisce un’impresa che vende o noleggia materiali d’illuminazione e audio.

23. Egli sfrutta una rete locale senza fili che offre, nei dintorni della sua impresa, un accesso gratuito e anonimo a Internet. Per fornire tale accesso a Internet, il sig. Mc Fadden utilizza i servizi di un’impresa di telecomunicazioni. L’accesso a detta rete era deliberatamente non protetto al fine di attirare l’attenzione dei clienti dei negozi adiacenti, dei passanti e dei vicini sulla sua attività.


25. Nello stesso periodo, un’opera musicale è stata gratuitamente messa a disposizione del pubblico su Internet, senza il consenso dei titolari dei relativi diritti, attraverso la rete locale senza fili gestita dal sig. Mc Fadden. Quest’ultimo afferma di non aver commesso l’asserita violazione, ma di non poter escludere che sia stata commessa da uno degli utenti della sua rete.

26. La Sony Music è il produttore del fonogramma dell’opera di cui trattasi.


28. In seguito a tale diffida, il sig. Mc Fadden ha proposto dinanzi al giudice del rinvio un’azione di accertamento negativo (negative Feststellungsklage). La Sony Music ha replicato formulando varie domande riconvenziali volte ad ottenere dal sig. Mc Fadden, innanzitutto, il risarcimento dei danni a titolo della sua responsabilità diretta nel caso in cui il giudice del rinvio non avesse riconosciuto la responsabilità diretta del sig. Mc Fadden, condanna di quest’ultimo al risarcimento dei danni sulla base della giurisprudenza tedesca relativa alla responsabilità indiretta (Störerhaftung) dei gestori di reti locali senza fili, e ciò per non avere adottato misure di protezione della sua rete locale senza fili e avere così permesso a soggetti terzi di violare i diritti della Sony Music.


31. Nell’ambito di tale procedimento di opposizione, la Sony Music ha chiesto, in via principale, la conferma di detta sentenza e, in subordine, per il caso in cui il giudice del rinvio non avesse riconosciuto la responsabilità diretta del sig. Mc Fadden, la condanna di quest’ultimo al risarcimento dei danni sulla base della giurisprudenza tedesca relativa alla responsabilità indiretta (Störerhaftung) dei gestori di reti locali senza fili, e ciò per non avere adottato misure di protezione della sua rete locale senza fili e avere così permesso a soggetti terzi di violare i diritti della Sony Music.

32. Nella sua domanda di pronuncia pregiudiziale, il giudice del rinvio osserva di essere propenso a ritenere che la violazione dei diritti della Sony Music non sia stata commessa personalmente dal sig. Mc Fadden, bensì da un utente sconosciuto della sua rete locale senza fili. Tuttavia, detto giudice prospetta l’insorgenza della responsabilità indiretta (Störerhaftung) del sig. Mc Fadden, poiché quest’ultimo non aveva protetto la rete mediante la quale era stato
possibile commettere in modo anonimo la violazione di cui trattasi. Ciò nondimeno, il giudice del rinvio s’interroga sulla questione se l’esonero da responsabilità previsto all’art.12, §1, della direttiva 2000/31, trasposto nel diritto tedesco dall’art.8, §1, prima frase, della legge sui media elettronici, non osti a qualsiasi ipotesi di insorgenza della responsabilità del sig. Mc Fadden.

33. In tale contesto, il Landgericht München I (tribunale regionale I di Monaco di Baviera, Germania) ha deciso di sospendere il procedimento e di sottoporre alla Corte le seguenti questioni pregiudiziali:

«1) Se l’art.12, §1, prima parte della frase, della direttiva 2000/31, in combinato disposto con l’art.2, lett.a), della medesima direttiva e con l’art.1, p.to 2, della direttiva 98/34, debba essere interpretato nel senso che l’espressione “normalmente dietro retribuzione” significa che il giudice nazionale deve accettare se:

a. la persona concretamente interessata, che si avvale della qualifica di prestatore, offra tali specifici servizi di norma dietro retribuzione, oppure

b. esistano sul mercato prestatori che offrono il servizio in parola o servizi analoghi dietro retribuzione, oppure

c. la maggior parte di tali servizi o dei servizi analoghi sia offerta dietro retribuzione.

2) Se l’art.12, §1, prima parte della frase, della direttiva 2000/31 debba essere interpretato nel senso che l’espressione “fornire un accesso alla rete di comunicazione” significa che, perché una fornitura sia conforme alla direttiva, rileva soltanto che si pervenga all’obiettivo, nel senso che sia fornito l’accesso alla rete di comunicazione (ad esempio a Internet).

3) Se l’art.12, §1, prima parte della frase, della direttiva 2000/31, in combinato disposto con l’art.2, lett.b), della medesima direttiva, debba essere interpretato nel senso che per “prestare” ai sensi di detto art.2, lett.b), è sufficiente che sia effettivamente messo a disposizione il servizio della società dell’informazione, nel caso di specie quindi che sia messa a disposizione una [rete locale senza fili] WLAN aperta, o se sia invece necessaria anche, ad esempio, un’attività di “promozione pubblicitaria”.

4) Se l’art.12, §1, prima parte della frase, della direttiva 2000/31 debba essere interpretato nel senso che l’espressione “non sia responsabile delle informazioni trasmesse” indica che eventuali richieste di inibitoria, risarcimento del danno, pagamento di spese di diffida o di spese legali da parte del soggetto leso dalla violazione dei diritti d’autore contro il fornitore dei servizi di accesso sono escluse, in linea di principio o in ogni caso, quando si tratta di una prima violazione accertata del diritto d’autore.

5) Se l’art.12, §1, prima parte della frase, della direttiva 2000/31, in combinato disposto con l’art.12, §3, della medesima direttiva, debba essere interpretato nel senso che gli Stati membri non possono autorizzare i giudici nazionali a emanare, nell’ambito di un procedimento principale contro un fornitore dei servizi di accesso, una diffida con cui intimano a quest’ultimo di astenersi in futuro dal permettere a terzi di rendere disponibile, attraverso una determinata connessione Internet, su una piattaforma Internet di condivisione una specifica opera protetta dal diritto d’autore per una consultazione in linea.

6) Se l’art.12, §1, prima parte della frase, della direttiva 2000/31 debba essere interpretato nel senso che, nelle circostanze di cui al procedimento principale, la disciplina di cui all’art.14, §1, lett.b), della direttiva 2000/31 deve essere applicata per analogia a una domanda inibitoria. […]

9) Se l’art.12, §1, prima parte della frase, della direttiva 2000/31, tenuto conto della tutela riconosciuta alla proprietà intellettuale quale diritto fondamentale e che si ricava dal diritto di proprietà (art.17, §2, della Carta dei diritti fondamentali dell’Unione Europea), tenuto conto altresì delle disposizioni contenute nelle direttive 2001/29 e 2004/48, e considerata la libertà di informazione e il diritto fondamentale della libertà d’impresa sancito dal diritto dell’Unione (art.16 della Carta dei diritti fondamentali dell’Unione Europea), debba essere interpretato nel senso che non osta a una decisione del giudice nazionale (…) con cui il fornitore dei servizi di accesso è condannato, a pena del pagamento di una penalità, ad astenersi dal permettere in futuro a terzi di rendere disponibile, attraverso una determinata connessione Internet, su una piattaforma Internet di condivisione (peer-to-peer) una specifica opera protetta dal diritto d’autore o parti di essa per una consultazione in linea e lascia così libero il fornitore dei servizi di accesso di individuare le concrete misure tecniche da adottare per ottemperare a tale ingiunzione.

10) Se ciò valga anche quando il fornitore dei servizi di accesso può di fatto adeguarsi al divieto giudiziale soltanto chiudendo la connessione Internet o proteggendola mediante password
o controllando tutte le comunicazioni trasmesse attraverso tale connessione, per verificare se la specifica opera protetta dal diritto d’autore sia nuovamente trasmessa illegalmente, quando ciò sia chiaro fin dall’inizio e non emerga soltanto nell’ambito del procedimento esecutivo o di irrogazione delle sanzioni».

**Sulle questioni pregiudiziali**

**Sulla prima questione**

34. Dalla domanda di pronuncia pregiudiziale risulta che, con la sua prima questione, il giudice del rinvio cerca di stabilire se un servizio come quello fornito dal ricorrente nel caso oggetto del procedimento principale, consistente nella messa a disposizione di una rete di comunicazione senza fili pubblica e gratuita, possa rientrare nell’ambito di applicazione dell’art.12, §1, della direttiva 2000/31.

35. In tale contesto, occorre intendere che, mediante la sua prima questione, il giudice del rinvio chiede, in sostanza, se una prestazione come quella oggetto del procedimento principale, fornita dal gestore di una rete di comunicazione e consistente nel mettere quest’ultima a disposizione del pubblico gratuitamente, costituisca un «servizio della società dell’informazione», ai sensi della prima disposizione.

36. Innanzitutto, occorre sottolineare che né l’art.12, §1, della direttiva 2000/31 né l’art.2 della medesima direttiva contengono una definizione della nozione di «servizio della società dell’informazione». Tuttavia, quest’ultimo articolo rinvia a tal fine alla direttiva 98/34.

37. In proposito, da un lato, risulta dai considerando 2 e 19 della direttiva 98/48 che la nozione di «servizio» utilizzata nella direttiva 98/34 deve essere intesa come avente lo stesso significato di quella che appare all’art.57 TFUE. Dunque, ai sensi di detto art.57 sono considerati «servizi», fra l’altro, le prestazioni fornite normalmente dietro retribuzione.

38. Dall’altro lato, ai sensi dell’art.1, p.to 2, della direttiva 98/34, la nozione di «servizio della società dell’informazione» include qualsiasi servizio fornito normalmente dietro retribuzione, a distanza per via elettronica e a richiesta individuale di un destinatario di servizi.

39. In tale contesto, occorre considerare che i servizi della società dell’informazione ai quali si riferisce l’art.12, §1, della direttiva 2000/31 sono soltanto quelli forniti normalmente dietro retribuzione.

40. Detta conclusione è suffragata dal considerando 18 della direttiva 2000/31, a termini del quale i servizi della società dell’informazione non si limitano esclusivamente a quelli che portano a stipulare contratti in linea, ma si estendono ad altri servizi, a condizione che detti servizi costituiscano un’attività economica.

41. Tuttavia, non è possibile inferirne che una prestazione di natura economica effettuata a titolo gratuito non possa mai costituire un «servizio della società dell’informazione» ai sensi dell’art.12, §1, della direttiva 2000/31. Infatti, la remunerazione di un servizio fornito da un prestatore nell’ambito della sua attività economica non è necessariamente versata dai soggetti che ne fruiscono (v., in tal senso, sentenza dell’11 settembre 2014, Papasavvas, C-291/13, […] p.ti 28 e 29).

42. Ciò si verifica, in particolare, nel caso in cui una prestazione effettuata a titolo gratuito sia fornita da un prestatore a fini pubblicitari per beni venduti o servizi forniti dal medesimo prestatore, dato che il costo di tale attività è così integrato nel prezzo di vendita di tali beni o di tali servizi (sentenza del 26 aprile 1988, Bond van Adverteerders e a., 352/85, […] p.to 16, nonché dell’11 aprile 2000, Deliège, C-51/96 e C-191/97, […] p.ti 56).

43. In considerazione di quanto precede, alla prima questione occorre rispondere dichiarando che l’art.12, §1, della direttiva 2000/31, in combinato disposto con l’art.2, lett.a), della medesima direttiva e con l’art.1, p.to 2, della direttiva 98/34, dev’essere interpretato nel senso che una prestazione come quella oggetto del procedimento principale, fornita dal gestore di una rete di comunicazione e consistente nel mettere quest’ultima a disposizione del pubblico gratuitamente, costituisce un «servizio della società dell’informazione» ai sensi della prima disposizione quando è effettuata dal prestatore di cui trattasi a fini pubblicitari per beni venduti o servizi forniti dal medesimo prestatore.

**Sulla seconda e sulla terza questione**

44. Con la seconda e la terza questione, che occorre esaminare congiuntamente, il giudice del rinvio chiede, in sostanza, se l’art.12, §1, della direttiva 2000/31 debba essere interpretato nel...
senso che, al fine di ritenere che sia prestato il servizio previsto in tale disposizione, consistente nel fornire un accesso a una rete di comunicazione, sia sufficiente mettere a disposizione tale accesso oppure se debbano essere soddisfatte ulteriori condizioni.

45. Più in particolare, il giudice del rinvio chiede se, oltre alla fornitura di un accesso a una rete di comunicazione, sia necessario, da un lato, che sussista un rapporto contrattuale tra il destinatario del servizio e il suo prestatore e, dall'altro, che quest'ultimo faccia pubblicità per tale prestazione.

46. A tal riguardo, in primo luogo, dalla formulazione dell'art.12 della direttiva 2000/31, intitolato «Semplice trasporto (“Mere conduit”)», risulta che la fornitura del servizio ivi previsto deve comportare la trasmissione di informazioni su una rete di comunicazione.

47. Inoltre, tale disposizione enuncia che l’esenzione da responsabilità dalla medesima prevista ha ad oggetto soltanto le informazioni trasmesse.


49. Ne deriva che la fornitura di un accesso a una rete di comunicazione non deve andare al di là dell’ambito di un tale processo tecnico, automatico e passivo che assicuri l’esecuzione della trasmissione di informazioni richiesta.

50. In secondo luogo, non risulta né da altre disposizioni della direttiva 2000/31 né dagli obiettivi da essa perseguiti che la fornitura di un accesso a una rete di comunicazione debba soddisfare condizioni ulteriori, quali la sussistenza di un rapporto contrattuale tra il destinatario del servizio e il suo prestatore o la circostanza che quest’ultimo si avvalga di mezzi pubblicitari per promuovere tale prestazione.

54. In considerazione di quanto precede, alla seconda e terza questione occorre rispondere dichiarando che l’art.12, §1, della direttiva 2000/31 deve essere interpretato nel senso che, al fine di ritenere che sia prestato il servizio previsto in tale disposizione, consistente nel fornire un accesso a una rete di comunicazione, detto accesso non deve andare al di là dell’ambito del processo tecnico, automatico e passivo che assicuri l’esecuzione della trasmissione di informazioni richiesta, non dovendo essere soddisfatta alcuna condizione ulteriore.

Sulla sesta questione

55. Con la sesta questione, che occorre esaminare in terzo luogo, il giudice del rinvio chiede, in sostanza, se l’art.12, §1, della direttiva 2000/31 debba essere interpretato nel senso che la condizione prevista all’art.14, §1, lett.b), della medesima direttiva si applica per analogia a detto art.12, §1.

56. A tal riguardo, dalla stessa struttura della direttiva 2000/31 emerge che il legislatore dell’Unione ha voluto distinguere i regimi applicabili alle attività di semplice trasporto («Mere conduit»), di memorizzazione d’informazioni nella forma detta «caching» e in quella di hosting, dato che tali attività sono disciplinate da disposizioni diverse di tale direttiva.

57. In tale contesto, dal confronto tra l’art.12, §1, l’art.13, §1, e l’art.14, §1, di tale direttiva risulta che le esenzioni da responsabilità in essi previste sono soggette a condizioni di applicazione diverse in funzione del tipo di attività.

58. In particolare, l’art.14, §1, della direttiva 2000/31, intitolato «Hosting», dispone, fra l’altro che, per poter beneficiare dell’esenzione da responsabilità ivi enunciata in favore dei prestatori di servizi di hosting di siti Internet, questi ultimi devono agire immediatamente, non appena vengono a conoscenza d’un’informazione illecita, al fine di rimuoverla o di disabilitarne l’accesso.

59. Invece, l’art.12, §1, della direttiva 2000/31 non subordina l’esenzione da responsabilità ivi prevista in favore dei fornitori di accesso a una rete di comunicazione al rispetto di una condizione di questo tipo.

60. Del resto, come rilevato dall’avvocato generale al §100 delle sue conclusioni, le situazioni del prestatore di servizi di hosting di un sito Internet, da un lato, e del fornitore di accesso a una rete di comunicazione, dall’altro, non sono simili per quanto riguarda la condizione fissata all’art.14, §1, della direttiva 2000/31.

61. Infatti, dal considerando 42 della medesima direttiva emerge che le esenzioni da responsabilità in essa stabilite sono state previste tenendo conto del fatto che le attività esercitate dalle varie categorie di prestatori di servizi interessate, in particolare dai fornitori di accesso a una rete di comunicazione e dai prestatori di servizi di hosting di siti Internet, sono tutte di ordine
puramente tecnico, automatico e passivo e che, di conseguenza, tali prestatori di servizi non conoscono né controllano le informazioni trasmesse o memorizzate.

62. Ciò posto, il servizio fornito dal prestatore di servizi di hosting di siti Internet, consistente nella memorizzazione d’informazioni, si caratterizza perché dura nel tempo. Di conseguenza, detto prestatore di servizi di hosting può venire a conoscenza del carattere illecito di talune informazioni da esso immagazzinate in un momento successivo rispetto a quello in cui si procede a detto immagazzinamento e nel quale esso è ancora in grado di intraprendere un’azione volta a rimuoverle o a disabilitarne l’accesso.

63. Invece, nel caso di un fornitore di accesso a unarete di comunicazione, il servizio di trasporto delle informazioni da esso prestato di norma non si prolunga nel tempo, cosicché, dopo aver trasmesso informazioni, esso non esercita più alcun controllo sulle stesse. Pertanto, il fornitore di accesso a una rete di comunicazione, contrariamente al prestatore di servizi di hosting di un sito Internet, spesso non è in grado di intraprendere, in un momento successivo, azioni volte rimuovere dette informazioni o a disabilitarne l’accesso.

64. In ogni caso, dal p.to 54 della presente sentenza risulta che l’art.12, §1, della direttiva 2000/31 non prevede alcuna condizione ulteriore oltre a quella, per il servizio in causa, di fornire un accesso a una rete di comunicazione, accesso che non deve andare al di là dell’ambito del processo tecnico, automatico e passivo che assicuri l’esecuzione della trasmissione di informazioni richiesta.

65. In considerazione di quanto precede, alla sesta questione occorre rispondere dichiarando che l’art.12, §1, della direttiva 2000/31 deve essere interpretato nel senso che la condizione prevista all’art.14, §1, lett.b), della medesima direttiva non si applica per analogia a detto art.12, §1.

[…]

Sulla quarta questione

72. Con la quarta questione, che occorre esaminare in quinto luogo, il giudice del rinvio chiede, in sostanza, se l’art.12, §1, della direttiva 2000/31 debba essere interpretato nel senso che esso non osta a che un soggetto leso dalla violazione dei suoi diritti su un’opera chieda il rimborso delle spese di diffida o delle spese legali sostenute ai fini della prosecuzione di tale violazione, il risarcimento del danno nonché il pagamento delle spese di diffida o delle spese legali nei confronti di un fornitore di accesso ad una rete di comunicazione i cui servizi siano stati utilizzati al fine di commettere la violazione stessa.

73. A tal riguardo, occorre ricordare che l’art.12, §1, della direttiva 2000/31 enuncia che gli Stati membri devono provvedere affinché i reati che consentono un servizio di accesso a una rete di comunicazione non siano responsabili delle informazioni ad essi trasmesse dai destinatari di tale servizio, alla triplice condizione, prevista in tale disposizione, che tali prestatori non diano origine alla trasmissione, che non selezionino il destinatario della trasmissione e che non selezionino né modifichino le informazioni trasmesse.

74. Ne consegue che, qualora le predette condizioni siano soddisfatte, non sorge la responsabilità di un prestatore che fornisce l’accesso a una rete di comunicazione e, pertanto, è in ogni caso escluso che il titolare di un diritto d’autore possa chiedere a tale prestatore di servizi un risarcimento per il motivo che la connessione a tale rete sia stata utilizzata da terzi allo scopo di violare i suoi diritti.

75. Di conseguenza, si deve altresì escludere, in ogni caso, che il titolare di un diritto d’autore possa chiedere il rimborso delle spese di diffida o delle spese legali sostenute ai fini della sua domanda di risarcimento. Infatti, una simile domanda accessoria presuppone, per essere fondata, che la domanda principale sia a sua volta fondata, ciò che è impedito dall’art.12, §1, della direttiva 2000/31.

76. Ciò posto, l’art.12, §3, della direttiva 2000/31 precisa che il medesimo articolo lascia impregiudicata la possibilità che un organo giurisdizionale nazionale o un’autorità amministrativa esiga che un prestatore di servizi ponga fine ad una violazione di diritti d’autore o che la prevenga.

77. Di conseguenza, quando una violazione sia stata commessa da un terzo attraverso la connessione a Internet che è stata messa a sua disposizione da un fornitore di accesso a una rete di comunicazione, l’art.12, §1, di tale direttiva non osta a che il soggetto leso da detta violazione chieda a un’autorità o a un organo giurisdizionale nazionale che a tale fornitore sia inibita la prosecuzione di tale violazione.

78. Per l’effetto, si deve ritenere che, isolatamente considerato, l’art.12, §1, della direttiva 2000/31 non esclude nemmeno che lo stesso soggetto possa chiedere il rimborso delle spese di
diffida o delle spese legali sostenute nel corso di un’azione, come quelle evocate nei punti precedenti.

79. In considerazione di quanto precede, alla quarta questione occorre rispondere dichiarando che l’art.12, §1, della direttiva 2000/31 deve essere interpretato nel senso che esso osta a che un soggetto leso dalla violazione dei suoi diritti su un’opera possa chiedere a un fornitore di accesso a una rete di comunicazione un risarcimento per il motivo che uno di tali accessi è stato utilizzato per terzi allo scopo di violare i suoi diritti, nonché il rimborso delle spese di diffida o delle spese legali sostenute ai fini della sua domanda di risarcimento. Per contro, tale disposizione deve essere interpretata nel senso che essa non osta a che tale persona chieda che sia inibita la prosecuzione di tale violazione nonché il pagamento delle spese di diffida e delle spese legali nei confronti di un fornitore di accesso ad una rete di comunicazione i cui servizi siano stati utilizzati al fine di commettere la violazione stessa, nel caso in cui tali domande siano volte, oppure siano conseguenti, all’adozione da parte di un’autorità o di un organo giurisdizionale nazionale di un’ingiunzione che vieti a detto fornitore di permettere la prosecuzione di siffatta violazione.

Sulla quinta, sulla nona e sulla decima questione

80. Con la quinta, la nona e la decima questione, che occorre esaminare congiuntamente e in sesto luogo, il giudice del rinvio chiede, in sostanza, se l’art.12, §1, della direttiva 2000/31, in combinato disposto con l’art.12, §3, della medesima direttiva debba essere interpretato, tenuto conto delle esigenze connesse alla tutela dei diritti fondamentali, nonché delle regole previste dalle direttive 2001/29 e 2004/48, nel senso che esso osta all’adozione di un’ingiunzione che, come quella in causa nel procedimento principale, imponga a un fornitore di accesso a una rete di comunicazione che consente al pubblico di connettersi a Internet, a pena del pagamento di una pena, di impedire a terzi di rendere disponibile al pubblico, attraverso tale connessione a Internet, su una piattaforma Internet di condivisione (peer-to-peer), una specifica opera protetta dal diritto d’autore o parti di essa, qualora il fornitore abbia sì la possibilità di scegliere le misure tecniche da adottare per conformarsi a tale ingiunzione, ma sia fin da subito stabilito che le sole misure che quest’ultimo potrà sostanzialmente adottare consistono o nel chiudere la connessione o una connessione a Internet, chiudere detta connessione oppure proteggerla mediante password o nell’esaminare tutte le informazioni trasmesse attraverso tale connessione.

81. Preliminarmente, è pacifico che un’ingiunzione come quella preconizzata dal giudice del rinvio nel procedimento principale, in quanto impone a un fornitore di accesso a una rete di comunicazione di prevenire la reiterazione di una violazione di un diritto connesso al diritto d’autore, rientra nella tutela dei diritti fondamentali, nonché delle regole previste dalle direttive 2001/29 e 2004/48, nel senso che essa osta all’adozione di un’ingiunzione che, come quella in causa nel procedimento principale, imponga a un fornitore di accesso a una rete di comunicazione che consente al pubblico di connettersi a Internet, a pena del pagamento di una pena, di impedire a terzi di rendere disponibile al pubblico, attraverso tale connessione a Internet, su una piattaforma Internet di condivisione (peer-to-peer), una specifica opera protetta dal diritto d’autore o parti di essa, qualora il fornitore abbia sì la possibilità di scegliere le misure tecniche da adottare per conformarsi a tale ingiunzione, ma sia fin da subito stabilito che le sole misure che quest’ultimo potrà sostanzialmente adottare consistono o nel chiudere la connessione o la reiterazione di una violazione di un diritto connesso al diritto d’autore o parti di essa, qualora il fornitore abbia sì la possibilità di scegliere le misure tecniche da adottare per conformarsi a tale ingiunzione, ma sia fin da subito stabilito che le sole misure che quest’ultimo potrà sostanzialmente adottare consistono o nel chiudere la connessione o proteggerla mediante password o nell’esaminare tutte le informazioni trasmesse attraverso tale connessione.

82. Inoltre, si deve constatare che la suddetta ingiunzione, lì dove, da un lato, accolla a detto fornitore di accesso un obbligo idoneo ad incidere sulla sua attività economica e, dall’altro, è atta a limitare la libertà dei destinatari di un tale servizio di beneficiare di un accesso a Internet, viola il diritto alla libertà d’impresa del primo, tutelato ai sensi dell’art.16 della Carta, nonché il diritto alla libertà d’informazione dei secondi, la cui protezione è sancita dall’art.11 della Carta.

83. Ebbene, quando diversi diritti fondamentali tutelati dal diritto dell’Unione siano in concorrenza fra loro, spetta alle autorità o all’organo giurisdizionale nazionale interessato provvedere a garantire un giusto equilibrio tra tali diritti (v., in tal senso, sentenza del 29 gennaio 2008, Promusicae, C-275/06, […] p.ti 68 e 70).

84. A tal riguardo, la Corte ha già dichiarato che un’ingiunzione che lasci a un fornitore di accesso a una rete di comunicazione l’onere di determinare le misure concrete da adottare per raggiungere il risultato perseguito può, a certe condizioni, pervenire a tale giusto equilibrio (v., in tal senso, sentenza del 27 marzo 2014, UPC Telekabel Wien, C-314/12, […], p.ti 62 e 63).

85. Nel caso di specie, dalla domanda di pronuncia pregiudiziale emerge che il giudice del rinvio muove dall’ipotesi che le misure che possono essere adottate dal destinatario di un’ingiunzione si limitino, in pratica, a tre, vale a dire esaminare tutte le informazioni trasmessesi attraverso una connessione a Internet, chiudere detta connessione oppure proteggerla mediante password.

86. Pertanto, è unicamente nella prospettiva di tali tre misure considerate dal giudice del rinvio che la Corte esaminerà la compatibilità dell’ingiunzione prevista con il diritto dell’Unione.

87. Anzitutto, riguardo alla sorveglianza dell’insieme delle informazioni trasmesse, una simile misura deve essere da subito esclusa, in quanto contraria all’art.15, §1, della direttiva 2000/31 ai
sensi del quale è vietato imporre, in particolare ai fornitori di accesso a una rete di comunicazione, un obbligo generale di sorveglianza sulle informazioni che trasmettono.

88. Riguardo, poi, alla misura consistente nel chiudere completamente la connessione a Internet, si deve constatare che la sua attuazione comporterebbe una grave violazione della libertà di impresa del soggetto che, anche solo a titolo accessorio, persegue un’attività economica volta a fornire un accesso a Internet, vietandogli totalmente, di fatto, di proseguire tale attività al fine di porre rimedio a una violazione limitata del diritto d’autore senza prevedere l’adozione di misure meno restrittive di tale libertà.

89. In tale contesto, una misura di questo tipo deve considerarsi non conforme all’esigenza di garantire un giusto equilibrio tra i diritti fondamentali che devono essere conciliati (v. in tal senso, relativamente a un’ingiunzione, sentenza del 24 novembre 2011, Scarlet Extended, C-70/10, […] p.to 49, nonché, per analogia, sentenza del 16 luglio 2015, Coty Germany, C-580/13, […] p.ti 35 e 41).

90. Infine, per quanto riguarda la misura consistente nel proteggere la connessione a Internet mediante una password, occorre sottolineare che essa è idonea a restringere sia il diritto alla libertà d’impresa del prestatore che fornisce un servizio di accesso a una rete di comunicazione, sia il diritto alla libertà d’informazione dei destinatari di tale servizio.

91. Ciò posto, va constatato, in primo luogo, che una misura simile non arreca pregiudizio al contenuto essenziale del diritto alla libertà d’impresa del fornitore di accesso a una rete di comunicazione, dato che si limita a regolare in modo marginale una delle modalità tecniche di esercizio dell’attività di tali fornitori.

92. In secondo luogo, una misura volta a proteggere la connessione a Internet non sembra essere tale da violare il contenuto essenziale del diritto alla libertà d’informazione dei destinatari di un servizio di accesso a una rete Internet, in quanto si limita a esigere da questi ultimi la richiesta di ottenere una password, fermo restando, inoltre, che tale connessione costituisce soltanto uno dei tanti mezzi per accedere a Internet.

93. In terzo luogo, è vero che dalla giurisprudenza emerge che la misura adottata dal fornitore deve essere rigorosamente mirata, nel senso che deve servire a porre fine alla violazione arrecata da un terzo al diritto d’autore o a un diritto connesso, senza pregiudizio per la possibilità degli utenti di Internet che ricorrano ai servizi di tale fornitore di accedere legittimamente ad informazioni. Nel caso contrario, l’ingerenza di detto fornitore nella libertà di informazione di tali utenti sarebbe ingiustificata alla luce dell’obiettivo perseguito (sentenza del 27 marzo 2014, UPC Telekabel Wien, C-314/12, […] p.to 56).

94. Tuttavia, una misura adottata da un fornitore di accesso ad una rete di comunicazione consistente nel proteggere la connessione di tale rete a Internet non sembra idonea a compromettere la possibilità di cui dispongono gli utenti di Internet che ricorrano ai servizi di tale fornitore di accedere lecitamente a informazioni, dato che non comporta alcun blocco del sito Internet.

95. In quarto luogo, la Corte ha già dichiarato che le misure adottate dal destinatario di un’ingiunzione, come quella in causa nel procedimento principale, in sede di ottemperanza alla stessa, devono essere abbastanza efficaci da garantire una tutela effettiva del diritto fondamentale in parola, vale a dire che esse devono avere l’effetto di impedire o, almeno, di rendere difficilmente realizzabili le consultazioni non autorizzate dei materiali protetti e di scoraggiare seriamente gli utenti di Internet che ricorrano ai servizi del destinatario di tale ingiunzione dal consultare tali materiali messi a loro disposizione in violazione del suddetto diritto fondamentale (sentenza del 27 marzo 2014, UPC Telekabel Wien, C-314/12, […] p.to 62).

96. A tal proposito, si deve constatare che una misura consistente nel proteggere la connessione a Internet mediante una password può dissuadere gli utenti di tale connessione dal violare un diritto d’autore o diritti connessi, nei limiti in cui tali utenti siano obbligati a rivelare la loro identità al fine di ottenere la password richiesta e non possano quindi agire anonimamente, circostanza che spetta al giudice del rinvio verificare.

97. In quinto luogo, occorre ricordare che, secondo il giudice del rinvio, a parte le tre misure da esso invocate, non esiste alcun’altra misura che un fornitore di accesso ad una rete di comunicazione, come quella di cui trattasi nella fattispecie, possa in pratica attuare al fine di conformarsi a un’ingiunzione come quella oggetto del procedimento principale.

98. Dato che le altre due misure sono state scartate dalla Corte, se si affermasse che un fornitore di accesso a una rete di comunicazione non deve proteggere la sua connessione a
Internet si finirebbe col privare il diritto fondamentale alla proprietà intellettuale di ogni tutela, il che contrasterrebbe con l'idea del giusto equilibrio (v., per analogia, sentenza del 16 luglio 2015, *Coty Germany*, C-580/13, […] p.ti 37 e 38).

99. In tale contesto, una misura volta a proteggere la connessione a Internet mediante una password deve essere considerata necessaria al fine di garantire un'effettiva protezione del diritto fondamentale alla tutela della proprietà intellettuale.

100. Da quanto precede discende che, alle condizioni specificate nella presente sentenza, la misura consistente nel proteggere la connessione deve essere considerata idonea a realizzare un giusto equilibrio tra, da un lato, il diritto fondamentale alla protezione della proprietà intellettuale e, dall'altro, il diritto alla libertà d'impresa del prestatore che fornisce un servizio di accesso a una rete di comunicazione nonché il diritto alla libertà d'informazione dei destinatari di tale servizio.

101. Di conseguenza, alla quinta, nona e decima questione occorre rispondere dichiarando che l’art.12, §1, della direttiva 2000/31, in combinato disposto con l’art.12, §3, della medesima direttiva, deve essere interpretato, tenuto conto delle esigenze connesse alla tutela dei diritti fondamentali nonché delle regole previste dalle direttive 2001/29 e 2004/48, nel senso che esso non osta, in via di principio, all’adozione di un’ingiunzione che, come quella in causa nel procedimento principale, imponga a un fornitore di accesso a una rete di comunicazione che consente al pubblico di connettersi a Internet, pena il versamento di una penalità, di impedire a terzi di rendere disponibile al pubblico, attraverso tale connessione a Internet, su una piattaforma Internet di condivisione (peer-to-peer), una specifica opera protetta dal diritto d’autore o parti di essa, qualora il fornitore abbia la possibilità di scegliere le misure tecniche da adottare per conformarsi a detta ingiunzione, anche se tale scelta si riduca alla sola misura consistente nel proteggere la connessione a Internet mediante una password, nei limiti in cui gli utenti di detta rete siano obbligati a rivelare la loro identità al fine di ottenere la password richiesta e non possano quindi agire anonimamente, circostanza che spetta al giudice del rinvio verificare.

[…]

Per questi motivi, la Corte (Terza Sezione) dichiara:

1) L’art.12, §1, della direttiva 2000/31/CE […] dell’8 giugno 2000, relativa a taluni aspetti giuridici dei servizi della società dell’informazione, in particolare il commercio elettronico, nel mercato interno («direttiva sul commercio elettronico»), in combinato disposto con l’art.2, lett.a), di detta direttiva e con l’art.1, p.to 2, della direttiva 98/34/CE […] del 22 giugno 1998, che prevede una procedura d’informazione nel settore delle norme e delle regolamentazioni tecniche e delle regole relative ai servizi della società dell’informazione, come modificata dalla direttiva 98/48/CE […] del 20 luglio 1998, dev’esser interpretato nel senso che una prestazione come quella oggetto del procedimento principale, fornita dal gestore di una rete di comunicazione e consistente nel mettere quest’ultima a disposizione del pubblico gratuitamente, costituisce un «servizio della società dell’informazione» ai sensi della prima disposizione quando è fornita dal prestatore di cui trattasi a fini pubblicitari per beni venduti o servizi forniti dal medesimo prestatore.

2) L’art.12, §1, della direttiva 2000/31 deve essere interpretato nel senso che, al fine di ritenere che sia prestato il servizio previsto in tale disposizione, consistente nel fornire un accesso a una rete di comunicazione, detto accesso non deve andare al di là dell’ambito del processo tecnico, automatico e passivo che assicuri l’esecuzione della trasmissione di informazioni richiesta, non dovendo essere soddisfatta alcuna condizione ulteriore.

3) L’art.12, §1, della direttiva 2000/31 deve essere interpretato nel senso che la condizione prevista all’art.14, §1, lett.b), della medesima direttiva non si applica per analogia a detto art.12, §1.

4) L’art.12, §1, della direttiva 2000/31, in combinato disposto con l’art.2, lett.b), della medesima direttiva, deve essere interpretato nel senso che non vi sono requisiti ulteriori, oltre a quello menzionato in tale disposizione, ai quali sia soggetto il prestatore di servizi che fornisce l’accesso a una rete di comunicazione.

5) L’art.12, §1, della direttiva 2000/31 deve essere interpretato nel senso che esso osta a che un soggetto leso dalla violazione dei suoi diritti su un’opera possa chiedere a un fornitore accesso a una rete di comunicazione un risarcimento per il motivo che uno di tali accessi è stato utilizzato da terzi allo scopo di violare i suoi diritti, nonché il rimborso delle spese di diffida o delle spese legali sostenute ai fini della sua domanda di risarcimento. Per contro, tale disposizione deve essere interpretata nel senso che essa non osta a che tale
persona chieda che sia inibita la prosecuzione di tale violazione nonché il pagamento delle spese di diffida e delle spese legali nei confronti di un fornitore di accesso ad una rete di comunicazione i cui servizi siano stati utilizzati al fine di commettere la violazione stessa, nel caso in cui tali domande siano volte oppure siano conseguenti all’adozione da parte di un’autorità o di un organo giurisdizionale nazionale di un’ingiunzione che vetti a detto fornitore di permettere la prosecuzione di siffatta violazione.

6) L’art.12, §1, della direttiva 2000/31, in combinato disposto con l’art.12, §3, della medesima direttiva, deve essere interpretato, tenuto conto delle esigenze connesse alla tutela dei diritti fondamentali nonché delle regole previste dalle direttive 2001/29 e 2004/48, nel senso che esso non osta, in via di principio, all’adozione di un’ingiunzione che, come quella in causa nel procedimento principale, imponga a un fornitore di accesso a una rete di comunicazione che consente al pubblico di connettersi a Internet, pena il versamento di una penalità, di impedire a terzi di rendere disponibile al pubblico, attraverso tale connessione a Internet, su una piattaforma Internet di condivisione (peer-to-peer), una specifica opera protetta dal diritto d’autore o parti di essa, qualora il fornitore abbia la possibilità di scegliere le misure tecniche da adottare per conformarsi a detta ingiunzione, anche se tale scelta si riduca alla sola misura consistente nel proteggere la connessione a Internet mediante una password, nei limiti in cui gli utenti di detta rete siano obbligati a rivelare la loro identità al fine di ottenere la password richiesta e non possano quindi agire anonimamente, circostanza che spetta al giudice del rinvio verificare.

*****

DISCUSSIONE

1. Il fornitore di una rete locale senza fili è da considerare, ai sensi della direttiva 2000/31/CE, quale Internet service provider? Di che tipo?

2. Ai sensi della direttiva 2000/31/CE, gli Internet service providers sono soggetti alle medesime regole di responsabilità? Se differiscono, come e perché?

3. La Corte ammette la richiesta di danni nei confronti del fornitore di una rete locale senza fili? Se sì, a quali condizioni?

4. Quali sono le misure che la Corte individua per evitare la continuazione delle violazioni della normativa in materia di copyright da parte degli utenti della rete locale senza fili?

5. Quali sono gli interessi contrapposti? Quale può essere un bilanciamento ragionevole?

6. Quale è il ruolo dell’anonimato, in relazione all’individuazione delle responsabilità?

*****

NORME

- art.12, direttiva 2000/31/CE

119
5. PRIVACY E PROTEZIONE DEI DATI PERSONALI
5.1. Trattamenti e trasferimenti di dati personali in Rete

Corte di Giustizia della Comunità Europea, 6 novembre 2003 (causa C-101/01)

[...] 1. Con ordinanza 23 febbraio 2001, pervenuta in cancelleria il 1° marzo successivo, il Göta hovrätt (Corte d'appello della regione del Götaland) ha sottoposto alla Corte, ai sensi dell'art.234 CE, sette questioni pregiudiziali vertenti, in particolare, sull'interpretazione della direttiva [...] 95/46/CE, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati [...].

2. Tali questioni sono state sollevate nell'ambito di un procedimento penale svoltosi dinanzi al suddetto giudice contro la sig.ra Lindqvist, imputata di aver violato la normativa svedese relativa alla protezione dei dati personali pubblicando nel suo sito Internet dati personali riguardanti un certo numero di persone che lavorano, come lei, in qualità di volontari in una parrocchia della Chiesa protestante di Svezia.

[...] Causa principale e questioni pregiudiziali

12. La sig.ra Lindqvist, oltre ad occupare un posto di lavoro subordinato come agente per la manutenzione, esercitava la funzione di formatrice di comunicandi nella parrocchia di Alsedá (Svezia). Essa ha seguito un corso di informatica nell'ambito del quale doveva in particolare creare una pagina iniziale sui Internet («home page»). Alla fine del 1998 la sig.ra Lindqvist ha creato, a casa sua e con un personal computer, alcune pagine Internet allo scopo di consentire ai parrocchiani che si preparavano alla cresima di ottenere facilmente le informazioni di cui avevano bisogno. A sua richiesta, l'amministratore del sito della Chiesa di Svezia ha creato un collegamento ipertestuale («link») fra tali pagine e il suddetto sito.

13. Le pagine in questione contenevano informazioni sulla sig.ra Lindqvist e su 18 suoi colleghi della parrocchia, compreso il loro nome e cognome o, talvolta, soltanto il loro nome. La sig.ra Lindqvist ha inoltre descritto, in termini leggermente scherzosi, le mansioni dei colleghi e le loro abitudini nel tempo libero. In molti casi, era inoltre descritta la loro situazione familiare ed erano indicati i recapiti telefonici nonché altre informazioni. Per di più, era in particolare riferito il fatto che una collega, essendosi ferita ad un piede, era in congedo parziale per malattia.

14. Dell'esistenza di tali pagine la sig.ra Lindqvist non aveva informato i suoi colleghi, né aveva chiesto il loro consenso, né aveva dichiarato di averle realizzate alla Datainspektion (ente pubblico per la tutela dei dati trasmessi per via informatica). Essa ha eliminato le pagine in questione non appena è venuta a conoscenza del fatto che queste non erano apprezzate da taluni suoi colleghi.

[...] 18. Nutrendo dubbi sull'interpretazione del diritto comunitario applicabile in materia, in particolare della direttiva 95/46/CE, il Göta hovrätt ha deciso di sospendere il procedimento e di sottoporre alla Corte le seguenti questioni pregiudiziali:

«1) Se l'indicazione di una persona - con il nome o con il nome e il numero di telefono - su una pagina iniziale su Internet costituisca un comportamento che rientra nell'ambito di applicazione della direttiva 95/46/CE. Se il realizzare personalmente una pagina iniziale su Internet e l'inserirvi il nome di un certo numero di persone unitamente a dichiarazioni e affermazioni riguardanti, tra l'altro, la situazione lavorativa di queste ultime e gli interessi da esse coltivati nel tempo libero costituisca un "trattamento di dati personali interamente o parzialmente automatizzato".

[...] 3) Se il pubblicare su una pagina iniziale privata, ma accessibile a chiunque ne conosca l'indirizzo, dati del tipo indicato relativi a colleghi di lavoro possa essere considerato un comportamento che non rientra nell'ambito di applicazione della direttiva 95/46/CE in forza di una delle eccezioni di cui all'art.3, n.2, della stessa.

4) Se l'informazione, su una pagina iniziale, che un collega di lavoro, di cui viene specificato il nome, si è ferito ad un piede e si trova in congedo parziale per malattia costituisca un dato personale relativo alla salute che, a norma dell'art.8, n.1, della direttiva, non può essere trattato.»
5) Considerato che in certi casi la direttiva 95/46/CE vieta il trasferimento di dati personali verso Paesi terzi, se una persona che si trova in Svezia e che, servendosi di un computer, pubblica dati personali su una pagina iniziale caricata su un server in Svezia - di modo che tali dati divengono accessibili a cittadini di Paesi terzi - trasferisce dati verso Paesi terzi ai sensi della direttiva 95/46/CE. Se la soluzione di tale questione rimanga la stessa anche nel caso in cui, per quanto si sappia, nessuna persona di un Paese terzo abbia di fatto preso conoscenza dei dati o nel caso in cui il server di cui trattasi si trovi fisicamente in un Paese terzo.

6) Se in un caso come quello di specie si possa ritenere che le disposizioni della direttiva 95/46/CE pongano limiti incompatibili con i principi generali in materia di libertà di espressione, o con altre libertà e diritti, vigenti all'interno dell'Unione Europea e che trovano corrispondenza, tra l'altro, nell'art.10 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali.

Sulla prima questione

19. Con la prima questione il giudice del rinvio chiede se l'operazione consistente nel far riferimento, in una pagina Internet, a diverse persone e nell'identificarle vuoi con il loro nome, vuoi con altri mezzi, ad esempio con il loro numero telefonico, o fornendo informazioni riguardanti la loro situazione lavorativa e gli interessi da esse coltivati nel tempo libero costituisca un «trattamento di dati personali interamente o parzialmente automatizzato» ai sensi dell'art.3, n.1, della direttiva 95/46/CE.

Soluzione della Corte

24. La nozione di «dati personali» accolta nell'art.3, n.1, della direttiva 95/46/CE comprende, conformemente alla definizione che figura nell'art.2, lett.a), di questa, «qualsiasi informazione concernente una persona fisica identificata o identificabile». Tale nozione ricomprende certamente il nome di una persona accostato al suo recapito telefonico o ad informazioni relative alla sua situazione lavorativa o ai suoi passatempi.

25. Quanto alla nozione di «trattamento» di siffatti dati, accolta dall'art.3, n.1, della direttiva 95/46/CE, essa comprende, in conformità alla definizione che figura nell'art.2, lett.b), di questa, «qualsiasi operazione o insieme di operazioni compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali». Quest'ultima disposizione indica diversi esempi di operazioni del genere, tra i quali figurano la comunicazione mediante trasmissione, la diffusione o qualsiasi altra forma di messa a disposizione di dati. Ne consegue che l'operazione consistente nel far comparire in una pagina Internet dati personali va considerata come un trattamento del genere.

26. Resta da stabilire se tale trattamento sia «automatizzato in tutto o in parte». In proposito occorre rilevare che far apparire delle informazioni in una pagina Internet impone, secondo i procedimenti tecnici e informatici attualmente applicati, di realizzare un'operazione di caricamento di questa pagina su un server nonché le operazioni necessarie per rendere questa pagina accessibile a coloro che si sono collegati ad Internet. Tali operazioni vengono effettuate, almeno in parte, in modo automatizzato.

27. La prima questione va quindi risolta nel senso che l'operazione consistente nel fare riferimento, in una pagina Internet, a diverse persone e nell'identificarle vuoi con il loro nome, vuoi con altri mezzi, ad esempio indicando il loro numero di telefono o informazioni relative alla loro situazione lavorativa e ai loro passatempi, costituisce un «trattamento di dati personali interamente o parzialmente automatizzato» ai sensi dell'art.3, n.1, della direttiva 95/46/CE.

Sulla terza questione

29. Con la terza questione il giudice del rinvio chiede in sostanza se un trattamento di dati personali come quello che è oggetto della prima questione rientri in una delle eccezioni previste dall'art.3, n.2, della direttiva 95/46/CE.

Soluzione della Corte

37. L'art.3, n.2, della direttiva 95/46/CE prevede due eccezioni all'ambito di applicazione della stessa.

[...]
45. Ora, attività a titolo religioso o di volontariato, come quelle esercitate dalla sig.ra Lindqvist, non sono equiparabili alle attività indicate nell'art.3, n.2, primo trattino, della direttiva 95/46/CE e non sono quindi comprese in tale eccezione.

46. Per quanto riguarda l'eccezione di cui all'art.3, n.2, secondo trattino, della direttiva 95/46/CE, il dodicesimo "considerando" di questa, relativo a tale eccezione, menziona, a titolo di esempio di trattamento di dati effettuato da una persona fisica nell'esercizio di attività a carattere esclusivamente personale o domestico, la corrispondenza e la compilazione di elenchi di indirizzi.

47. Tale eccezione deve quindi interpretarsi nel senso che comprende unicamente le attività che rientrano nell'ambito della vita privata o familiare dei singoli, il che manifestamente non avviene nel caso del trattamento di dati personali consistente nella loro pubblicazione su Internet in modo da rendere tali dati accessibili ad un numero indefinito di persone.

48. La terza questione va quindi risolta nel senso che un trattamento di dati personali come quello menzionato nella soluzione della prima questione non rientra in alcuna delle eccezioni che figurano nell'art.3, n.2, della direttiva 95/46/CE.

Sulla quarta questione

49. Con la quarta questione il giudice del rinvio chiede se l'indicazione che una persona si è ferita ad un piede e si trova in congedo parziale per malattia costituisca un dato personale relativo alla salute ai sensi dell'art.8, n.1, della direttiva 95/46/CE.

50. In considerazione dell'oggetto di tale direttiva, occorre dare all'espressione «dati relativi alla salute» utilizzata nell'art.8, n.1, un'interpretazione ampia tale da comprendere informazioni riguardanti tutti gli aspetti, tanto fisici quanto psichici, della salute di una persona.

51. La quarta questione va quindi risolta nel senso che l'indicazione che una persona si è ferita ad un piede e si trova in congedo parziale per malattia costituisce un dato personale relativo alla salute ai sensi dell'art.8, n.1, della direttiva 95/46/CE.

Sulla quinta questione

52. Con la quinta questione il giudice del rinvio chiede in sostanza se si configuri un «trasferimento di dati personali verso Paesi terzi» ai sensi dell'art.25 della direttiva 95/46/CE quando una persona che si trova in uno Stato membro inserisce su una pagina Internet - caricata presso una persona fisica o giuridica che ospita il sito Internet sul quale la pagina può essere consultata (in prossimo: il «fornitore di servizi di ospitalità» («web hosting provider») e che risiede nello stesso o in un altro Stato membro - dati personali, rendendoli così accessibili a chiunque si colleghi ad Internet, compresi coloro che si trovano in Paesi terzi. Il giudice del rinvio chiede inoltre se la soluzione di tale questione rimanga la stessa anche quando risulti che nessuna persona di un Paese terzo ha di fatto preso conoscenza di tali dati o quando il server in cui la pagina è caricata si trovi, fisicamente, in un Paese terzo.

[...]

Soluzione della Corte

56. La direttiva 95/46/CE non definisce né all'art.25 né in alcun'altra disposizione, in particolare al suo art.2, la nozione di «trasferimento verso un Paese terzo».

57. Al fine di stabilire se l'inserimento su una pagina Internet di dati personali, per il solo fatto di rendere tali dati accessibili alle persone che si trovano in un Paese terzo, costituisca un «trasferimento» di dati verso un Paese terzo ai sensi dell'art.25 della direttiva 95/46/CE, occorre tener conto, da una parte, della natura tecnica delle operazioni così effettuate e, dall'altra, dell'obiettivo nonché della sistematica del capo IV della suddetta direttiva, in cui figura l'art.25.

58. Le informazioni che si trovano su Internet possono essere consultate da un numero indefinito di persone residenti in molteplici luoghi e in qualsiasi momento. Il carattere ubiquitario di tali informazioni risulta in particolare dal fatto che i mezzi tecnici usati nell'ambito di Internet sono relativamente semplici e sempre meno costosi.

59. Secondo le modalità di uso di Internet, quali sono divenute disponibili a singoli come la sig.ra Lindqvist negli anni '90, l'autore di una pagina destinata ad essere pubblicata su Internet trasmette i dati che costituiscono tale pagina al suo fornitore di servizi di ospitalità («web hosting provider»). Quest'ultimo gestisce l'infrastruttura informatica necessaria per garantire il caricamento di tali dati e la connessione del server che ospita il sito Internet. Ciò consente la successiva trasmissione di tali dati a chiunque sia collegato ad Internet e chieda di ottenere l'. I computer che costituiscono questa infrastruttura informatica possono essere situati, e spesso lo sono, in uno o più Paesi diversi da quello del luogo in cui ha sede il fornitore di servizi di ospitalità, senza che la clientela di questo ne abbia o possa ragionevolmente prenderne conoscenza.
60. Dagli atti di causa risulta che, per ottenere le informazioni che figurano sulle pagine Internet nelle quali la sig.ra Lindqvist aveva inserito dati relativi ai suoi colleghi, un utente di Internet doveva non soltanto collegarsi a questo, ma anche effettuare, con un procedimento personale, le azioni necessarie per consultare le suddette pagine. In altri termini, le pagine Internet della sig.ra Lindqvist non contenevano i meccanismi tecnici che avrebbero consentito l'invio automatico di tali informazioni a persone che non avessero deliberatamente cercato di accedere a dette pagine.

61. Ne consegue che, in circostanze come quelle della fattispecie nella causa principale, i dati personali che giungono al computer di una persona che si trova in un Paese terzo, provenienti da una persona che li ha caricati su un sito Internet, non sono stati trasferiti direttamente tra queste due persone, ma attraverso l'infrastruttura informatica del fornitore di servizi di ospitalità presso il quale la pagina è caricata.

62. È in tale contesto che occorre accertare se il legislatore comunitario avesse l'intenzione, ai fini dell'applicazione del capo IV della direttiva 95/46/CE, di ricoprire nel concetto di «trasferimento verso un Paese terzo di dati personali», ai sensi dell'art.25 della stessa direttiva, operazioni come quelle effettuate dalla sig.ra Lindqvist. Va rilevato che la quinta questione posta dal giudice a quo riguarda solo tali operazioni, restando escluse quelle effettuate dai fornitori di servizi di ospitalità.

63. Il capo IV della direttiva 95/46/CE, nel quale figura l'art.25, predispone un regime speciale, implicante norme precise, che mira a garantire un controllo da parte degli Stati membri sui trasferimenti di dati personali verso i Paesi terzi. Tale capitolo istituisce un regime complementare al regime generale attuato dal capo II della suddetta direttiva, riguardante la liceità dei trattamenti di dati personali.

64. L'obiettivo del capo IV viene definito nei “considerando” da cinquantasei a sessanta della direttiva 95/46/CE, i quali dispongono in particolare che, se la tutela delle persone garantita nella Comunità da questa direttiva non osta al trasferimento di dati personali verso Paesi terzi che garantiscono un livello di protezione adeguato, l'adeguatezza deve essere valutata in funzione di tutte le circostanze relative ad un trasferimento o ad una categoria di trasferimenti. Quando un Paese terzo non offre un livello di protezione adeguato, il trasferimento di dati personali verso tale Paese deve essere vietato.


66. In particolare, l'art.25, n.4, della direttiva 95/46/CE prevede che, qualora la Commissione constatì che un Paese terzo non garantisce un livello di protezione adeguato, gli Stati membri adottino le misure necessarie per impedire ogni trasferimento di dati personali verso il Paese terzo in questione.

67. Il capo IV della direttiva 95/46/CE non contiene alcuna disposizione riguardante l'uso di Internet. Esso non precisa in particolare i criteri che consentono di determinare se, per quanto riguarda le operazioni effettuate mediante fornitori di servizi di ospitalità, occorra basarsi sul luogo di stabilimento del fornitore o sul suo domicilio professionale ovvero sul o sui luoghi in cui sono situati i computer che costituiscono l'infrastruttura informatica del fornitore.

68. Tenuto conto, da una parte, dello stato dello sviluppo di Internet all'epoca dell'elaborazione della direttiva 95/46/CE e, dall'altra, della mancanza, nel suo capo IV, di criteri applicabili all'uso di Internet, non si può presumere che il legislatore comunitario avesse l'intenzione di includere prospettivamente nella nozione di «trasferimenti verso un Paese terzo di dati personali» l'inserimento, da parte di una persona che si trovi nella situazione della sig.ra Lindqvist, di dati in una pagina Internet, anche se questi sono resi accessibili alle persone di Paesi terzi in possesso dei mezzi tecnici per consultarli.

69. Qualora l'art.25 della direttiva 95/46/CE venisse interpretato nel senso che si configura un «trasferimento verso un Paese terzo di dati personali» ogni volta che dati personali vengono caricati su una pagina Internet, tale trasferimento sarebbe necessariamente un trasferimento verso tutti i Paesi terzi in cui esistono i mezzi tecnici necessari per accedere ad Internet. Il regime speciale previsto dal capo IV della suddetta direttiva diverrebbe quindi necessariamente, per quanto riguarda le operazioni su Internet, un regime di applicazione generale. Infatti, non appena la Commissione constatasse, ai sensi dell'art.25, n.4, della direttiva 95/46/CE, che un solo Paese
terzo non garantisce un livello di protezione adeguato, gli Stati membri sarebbero tenuti ad impedire qualsiasi immissione su Internet di dati personali.

70. Di conseguenza, occorre concludere che l'art.25 della direttiva 95/46/CE deve essere interpretato nel senso che operazioni come quelle effettuate dalla sig.ra Lindqvist non costituiscono di per sé un «trasferimento verso un Paese terzo di dati». Non è quindi necessario accertare se una persona di un Paese terzo abbia avuto accesso alla pagina Internet di cui trattasi o se il server di tale fornitore si trovi fisicamente in un Paese terzo.

71. La quinta questione va quindi risolta nel senso che non si configura un «trasferimento verso un Paese terzo di dati» ai sensi dell’art.25 della direttiva 95/46/CE allorché una persona che si trova in uno Stato membro inserisce in una pagina Internet - caricata presso il suo fornitore di servizi di ospitalità («web hosting provider»), stabilito nello Stato stesso o in un altro Stato membro - dati personali, rendendoli così accessibili a chiunque si colleghi ad Internet, compresi coloro che si trovano in Paesi terzi.

**Sulla sesta questione**

72. Con la sesta questione il giudice del rinvio chiede se si debba ritenere che le disposizioni della direttiva 95/46/CE pongano, in un caso come quello della fattispecie nella causa principale, limiti incompatibili con il principio generale della libertà d'espressione o con altre libertà e diritti, vigenti all'interno dell'Unione Europea e che trovano corrispondenza, in particolare, nel diritto sancito dall'art.10 della CEDU.

[...] 

**Soluzione della Corte**

79. Dal settimo "considerando" della direttiva 95/46/CE risulta che l'instaurazione e il funzionamento del mercato interno possono essere gravemente perturbati dal divario esistente tra i regimi nazionali applicabili al trattamento dei dati personali. Secondo il terzo "considerando" della stessa direttiva, l'armonizzazione di tali regimi nazionali deve avere come obiettivi non solo la libera circolazione di tali dati fra Stati membri, ma anche la salvaguardia dei diritti fondamentali delle persone. Tali obiettivi possono evidentemente essere confliggenti.

80. Da una parte, l'integrazione economica e sociale derivante dall'instaurazione e dal funzionamento del mercato interno comporterà necessariamente un sensibile aumento dei flussi di dati personali fra tutti i soggetti della vita economica e sociale degli Stati membri, siano essi imprese o amministrazioni degli Stati membri. I suddetti soggetti hanno, in una certa misura, bisogno di disporre di dati personali per effettuare le loro transazioni o per assolvere i loro compiti nell'ambito dello spazio senza frontiere costituito dal mercato interno.

81. D'altra parte, le persone interessate dal trattamento di dati personali chiedono giustamente che tali dati siano protetti in modo efficace.

82. I meccanismi che consentono di conciliare questi diversi diritti e interessi sono contenuti, in primo luogo, nella stessa direttiva 95/46/CE, in quanto essa prevede norme che determinano in quali situazioni ed in qual misura il trattamento dei dati personali è lecito e quali salvaguardie devono essere previste. In secondo luogo, essi risultano dall'adozione, da parte degli Stati membri, di disposizioni nazionali che garantiscono la trasposizione di tale direttiva e dall'eventuale applicazione di queste da parte delle autorità nazionali.

83. Quanto alla stessa direttiva 95/46/CE, le sue disposizioni sono per forza di cose relativamente generiche, visto che essa deve applicarsi a un gran numero di situazioni molto diverse. Pertanto, contrariamente a quanto assume la sig.ra Lindqvist, giustamente tale direttiva contiene norme caratterizzate da una certa elasticità e lascia in numerosi casi agli Stati membri il compito di decidere dei dettagli o di scegliere tra più opzioni.

84. È vero che gli Stati membri dispongono sotto molti aspetti di un margine di manovra al fine di trasporre la direttiva 95/46/CE. Tuttavia, niente consente di ritenere che il regime che questa contempla manchi di prevedibilità o che le sue disposizioni siano, in quanto tali, in contrasto con i principi generali del diritto comunitario e, in particolare, con i diritti fondamentali tutelati dall'ordinamento giuridico comunitario.

85. È quindi, piuttosto, nella fase dell'attuazione sul piano nazionale della normativa che traspone la direttiva 95/46/CE in singoli casi di specie che deve esser trovato un giusto equilibrio tra i diritti e gli interessi di cui trattasi.

86. In tale contesto, i diritti fondamentali assumono una particolare rilevanza, come dimostra la causa principale, in cui in sostanza è necessario soppesare, da una parte, la libertà di espressione della sig.ra Lindqvist nell'ambito del suo lavoro come formatrice di comunicandi
nonché la libertà di esercitare attività che contribuiscono alla vita religiosa e, dall'altra, la tutela della vita privata delle persone a proposito delle quali la sig.ra Lindqvist ha inserito dati sul suo sito Internet.

87. Di conseguenza, incombe alle autorità e ai giudici degli Stati membri non solo interpretare il loro diritto nazionale in modo conforme alla direttiva 95/46/CE, ma anche provvedere a non fondarsi su un'interpretazione di quest'ultima che entri in conflitto con i diritti fondamentali tutelati dall'ordinamento giuridico comunitario o con gli altri principi generali del diritto comunitario, come, ad esempio, il principio di proporzionalità.

88. Anche se la tutela della vita privata richiede l'applicazione di sanzioni efficaci nei confronti di coloro che trattano dati personali in modo non conforme alla direttiva 95/46/CE, siffatte sanzioni devono pur sempre osservare il principio di proporzionalità. Ciò vale a maggior ragione in quanto l'ambito di applicazione della direttiva 95/46/CE appare molto ampio e gli obblighi delle persone che procedono a trattamenti di dati personali sono numerosi e ingenti.

89. In applicazione del principio di proporzionalità, incombe al giudice a quo prendere in considerazione tutte le circostanze della causa di cui è adito, in particolare la durata della violazione delle norme che attuano la direttiva 95/46/CE nonché la rilevanza, per gli interessati, della tutela dei dati divulgati.

90. La sesta questione va quindi risolta nel senso che le disposizioni della direttiva 95/46/CE non pongono, di per sé, una restrizione incompatibile con il principio generale di libertà di espressione o con altri diritti e libertà, all'interno dell'Unione Europea e che trovano corrispondenza, tra l'altro, nell'art.10 della CEDU. Spetta alle autorità e ai giudici nazionali incaricati di applicare la normativa nazionale che traspone la direttiva 95/46/CE garantire il giusto equilibrio tra i diritti e gli interessi in gioco, ivi compresi i diritti fondamentali tutelati dall'ordinamento giuridico comunitario.

[...]
5.2. Diritti di proprietà intellettuale e tutela della riservatezza

Corte di Giustizia delle Comunità Europee, 29 gennaio 2008 (causa C-275/06)

[...] Causa principale e questione pregiudiziale

29. La Promusicae è un’associazione senza scopo di lucro di cui fanno parte produttori ed editori di registrazioni musicali e di registrazioni audiovisive. Con lettera del 28 novembre 2005, essa ha presentato dinanzi al Juzgado de lo Mercantil n.5 de Madrid (Tribunale commerciale n.5 di Madrid) una domanda di accertamenti preliminari contro la Telefónica, una società commerciale la cui attività consiste, tra l’altro, nella fornitura di servizi di accesso a Internet.

30. La Promusicae ha chiesto di ingiungere alla Telefónica di rivelare l’identità e l’indirizzo fisico di talune persone alle quali quest’ultima fornisce un servizio di accesso ad Internet e il cui “indirizzo IP”, nonché la data e l’ora di connessione, sono noti. Secondo la Promusicae, tali persone utilizzano il programma di scambio di archivi (cosiddetto “peer-to-peer” ovvero “P2P”) denominato “KaZaA” e consentono l’accesso, nelle cartelle condivise del loro computer, a fonogrammi i cui diritti patrimoniali di utilizzo spettano ai soci della Promusicae.

31. Quest’ultima ha affermato dinanzi al giudice del rinvio che gli utilizzatori del programma KaZaA commettono atti di concorrenza sleale e violano i diritti di proprietà intellettuale. Essa ha pertanto richiesto che le fossero comunicate le suddette informazioni per poter esercitare azioni civili contro le persone coinvolte.

32. Con ordinanza 21 dicembre 2005, il Juzgado de lo Mercantil n.5 de Madrid ha accolto la domanda di accertamenti preliminari presentata dalla Promusicae.


34. In tale contesto, il Juzgado de lo Mercantil n.5 de Madrid ha deciso di sospendere il procedimento e di sottoporre alla Corte la seguente questione pregiudiziale:


[...] Sulla direttiva 2002/58/CE

47. Le disposizioni dell’art.5, n.1, della direttiva 2002/58/CE stabiliscono che gli Stati membri devono assicurare la riservatezza delle comunicazioni effettuate tramite una rete pubblica di comunicazione e di servizi di comunicazione elettronica accessibili al pubblico, nonché dei relativi dati sul traffico, e devono in particolare vietare, in linea di principio, alle persone diverse dagli utenti di memorizzare tali dati senza consenso degli utenti interessati. Le uniche eccezioni riguardano le persone autorizzate legalmente ai sensi dell’art.15, n.1, della detta direttiva e la memorizzazione tecnica necessaria alla trasmissione della comunicazione. Inoltre, per quanto riguarda i dati sul traffico, l’art.6, n.1, della direttiva 2002/58/CE prevede che quelli che sono memorizzati devono essere cancellati o resi anonimi quando non sono più necessari ai fini della trasmissione di una comunicazione, fatti salvi i §§2, 3 e 5 dello stesso articolo e l’art.15, n.1, di tale direttiva.

[...]
49. D'altra parte, per quanto attiene all'art.15, n.1, della direttiva 2002/58/CE, occorre ricordare che, ai sensi di tale disposizione, gli Stati membri possono adottare disposizioni legislative volte a limitare la portata, in particolare, dell'obbligo di garantire la riservatezza dei dati sul traffico qualora tale restrizione costituisca una misura necessaria, opportuna e proporzionata all'interno di una società democratica per la salvaguardia della sicurezza nazionale (cioè della sicurezza dello Stato), della difesa, della sicurezza pubblica e per la prevenzione, la ricerca, l'accertamento ed il perseguimento dei reati, ovvero dell'uso non autorizzato del sistema di comunicazione elettronica, come prevede l'art.13, n.1, della direttiva 95/46/CE.

50. L'art.15, n.1, della direttiva 2002/58/CE offre quindi agli Stati membri la possibilità di prevedere deroghe all'obbligo di principio, ad essi incombente ai sensi dell'art.5 della stessa direttiva, di garantire la riservatezza dei dati personali.

51. Nessuna di tali deroghe sembra tuttavia riferirsi a situazioni che richiedono l'apertura di procedimenti civili. Infatti, da una parte esse riguardano la sicurezza nazionale, la difesa e la sicurezza pubblica, le quali costituiscono attività proprie degli Stati o delle autorità statali, estranee ai settori di attività dei singoli (v., in tal senso, sent. Lindqvist, cit., p.to 43), e, dall'altra, il perseguimento dei reati.

52. Quanto all'eccezione relativa agli usi non autorizzati del sistema di comunicazione elettronica, essa sembra riguardare gli utilizzì che mettono in causa l'integrità o la sicurezza stessa di tale sistema, come, in particolare, le ipotesi, riportate all'art.5, n.1, della direttiva 2002/58/CE, di captazione o di sorveglianza delle comunicazioni senza consenso degli utenti interessati. Neppure siffatti utilizzì, che, ai sensi del detto articolo, richiedono l'intervento degli Stati membri, si riferiscono a situazioni idonee a dar luogo a procedimenti civili.

53. Tuttavia, non si può non constatare che l'art.15, n.1, della direttiva 2002/58/CE conclude l'elenco delle suddette deroghe facendo espresso riferimento all'art.13, n.1, della direttiva 95/46/CE. Ebbene, anche quest'ultima disposizione autorizza gli Stati membri a adottare disposizioni intese a limitare la portata dell'obbligo di riservatezza dei dati personali qualora tale restrizione sia necessaria, tra l'altro, per la tutela dei diritti e delle libertà altrui. Poiché non precisano i diritti e le libertà che vengono in tal modo in questione, le dette disposizioni dell'art.15, n.1, della direttiva 2002/58/CE devono essere interpretate nel senso che esprimono la volontà del legislatore comunitario di non escludere dal loro ambito di applicazione la tutela del diritto di proprietà e delle situazioni in cui gli autori mirano ad ottenere tale tutela nel contesto di un procedimento civile.

54. Occorre pertanto constatare che la direttiva 2002/58/CE non esclude la possibilità, per gli Stati membri, di prevedere l'obbligo di divulgare dati personali nell'ambito di un procedimento civile.

55. Tuttavia, l'art.15, n.1, di tale direttiva non può essere interpretato nel senso che, nelle situazioni che elenca, esso vincola gli Stati membri a prevedere siffatto obbligo.

56. Pertanto, occorre verificare se le tre direttive menzionate dal giudice del rinvio impongano a tali Stati, ai fini dell'effettiva tutela del diritto d'autore, di prevedere il suddetto obbligo.

**Sulle tre direttive citate dal giudice del rinvio**

57. A tale proposito, occorre anzitutto rilevare che, come già ricordato al p.to 43 della presente sentenza, le direttive richiamate dal giudice del rinvio sono dirette a far sì che gli Stati membri garantiscono, soprattutto nella società dell'informazione, l'effettiva tutela della proprietà intellettuale e, in particolare, del diritto d'autore. Tuttavia, dagli artt.1, n.5, lett.b), della direttiva 2000/31/CE, 9 della direttiva 2001/29/CE e 8, n.3, lett.e), della direttiva 2004/48/CE risulta che siffatta tutela non può pregiudicare gli obblighi relativi alla tutela dei dati personali.

58. È vero che l'art.8, n.1, della direttiva 2004/48/CE richiede che gli Stati membri assicurino che, nel contesto dei procedimenti riguardanti la violazione di un diritto di proprietà intellettuale e in risposta a una richiesta giustificata e proporzionata del richiedente, l'autorità giudiziaria competente possa ordinare che siano fornite informazioni sull'origine e sulle reti di distribuzione di merci o di prestazione di servizi che violano un diritto di proprietà intellettuale. Tuttavia, da tali disposizioni, che devono essere lette in combinato disposto con quelle del §3, lett.e), dello stesso articolo, non risulta un dovere, in capo agli Stati membri, di prevedere, per garantire l'effettiva tutela del diritto d'autore, l'obbligo di comunicare dati personali nel contesto di un procedimento civile.

60. Quanto agli artt.41, 42 e 47 dell'Accordo ADPIC, fatti valere dalla *Promusicae*, alla luce dei quali devono essere interpretate, nella misura del possibile, le norme comunitarie che disciplinano – al pari delle disposizioni richiamate nella presente domanda di pronuncia pregiudiziale – un settore al quale si applica il detto accordo (v., in tal senso, sentenze 14 dicembre 2000, cause riunite C-300/98 e C-392/98, *Dior e a.* [...], nonché 11 settembre 2007, causa C-431/05, *Merck Genéricos – Produtos Farmacêuticos* [...], p.to 35), se è vero che essi impongono la tutela effettiva della proprietà intellettuale e l'istituzione di diritti di ricorso giurisdizionale per assicurare il rispetto di quest'ultima, essi non contengono tuttavia disposizioni che impongano di interpretare le suddette direttive nel senso che vincolano gli Stati membri ad istituire un obbligo di comunicare dati personali nel contesto di un procedimento civile.

**Sui diritti fondamentali**

61. Occorre osservare che nella sua domanda di pronuncia pregiudiziale il giudice del rinvio fa riferimento agli artt.17 e 47 della Carta, il primo dei quali riguarda la tutela del diritto di proprietà, in particolare della proprietà intellettuale, e il secondo il diritto ad un ricorso effettivo. Occorre ritenere che, così facendo, il detto giudice voglia capire se l'interpretazione delle tre direttive fatte valere – secondo la quale gli Stati membri non sono tenuti ad istituire, per garantire l'effettiva tutela del diritto d'autore, un obbligo di comunicare dati personali nel contesto di un procedimento civile – non comporti una violazione del diritto fondamentale di proprietà e del diritto fondamentale ad una tutela giurisdizionale effettiva.


63. Tuttavia, occorre rilevare che nella controversione in relazione alla quale il giudice del rinvio ha sollevato tale questione risulta coinvolta, oltre ai due suddetti diritti, anche un altro diritto fondamentale, vale a dire quello che garantisce la tutela dei dati personali e, quindi, della vita privata.

64. Ai sensi del secondo “considerando” della direttiva 2002/58/CE, quest'ultima mira a rispettare i diritti fondamentali e si attiene ai principi riconosciuti in particolare dalla Carta. Segnatamente, essa mira a garantire il pieno rispetto dei diritti delineati agli artt.7 e 8 di tale Carta. L'art.7 di quest'ultima riproduce in sostanza l'art.8 della Carta, capitolo III, che garantisce il diritto alla tutela giurisdizionale e l'istituzione di diritti di ricorso giurisdizionale per assicurare il rispetto della sua disposizione e, dalla luce della stessa, che lasciano agli Stati membri il necessario margine di discrezionalità per definire misure di reperimento che possano essere adattate alle diverse situazioni possibili (v., in tal senso, sent. *Lindqvist*, cit., p.to 84).
68. Di conseguenza, gli Stati membri sono tenuti, in occasione della trasposizione delle suddette direttive, a fondarsi su un'interpretazione di queste ultime tale da garantire un giusto equilibrio tra i diversi diritti fondamentali tutelati dall'ordinamento giuridico comunitario. Inoltre, in sede di attuazione delle misure di recepimento di tali direttive, le autorità e i giudici degli Stati membri devono non solo interpretare il loro diritto nazionale in modo conforme alle dette direttive, ma anche provvedere a non fondarsi su un'interpretazione di esse che entri in conflitto con i summenzionati diritti fondamentali o con gli altri principi generali del diritto comunitario, come, ad esempio, il principio di proporzionalità (v., in tal senso, sentenze Lindqvist, cit., p.to 87, e 26 giugno 2007, causa C-305/05, Ordre des barreaux francophones et germanophone e a., […], p.to 28).

69. D'altronde, a tale riguardo occorre ricordare che il legislatore comunitario ha espressamente richiesto, ai sensi dell'art.15, n.1, della direttiva 2002/58/CE, che le misure previste da tale § siano adottate dagli Stati membri nel rispetto dei principi generali del diritto comunitario, compresi quelli di cui all'art.6, nn.1 e 2, UE.

70. Alla luce delle considerazioni che precedono, occorre risolvere la questione sottoposta dichiarando che le direttive 2000/31/CE, 2001/29/CE, 2004/48/CE e 2002/58/CE non impongono agli Stati membri, in una situazione come quella oggetto della causa principale, di istituire un obbligo di comunicare dati personali per garantire l'effettiva tutela del diritto d'autore nel contesto di un procedimento civile. Tuttavia, il diritto comunitario richiede che i detti Stati, in occasione della trasposizione di queste direttive, abbiano cura di fondarsi su un'interpretazione delle medesime tale da garantire un giusto equilibrio tra i diversi diritti fondamentali tutelati dall'ordinamento giuridico comunitario. Inoltre, in sede di attuazione delle misure di recepimento delle dette direttive, le autorità e i giudici degli Stati membri devono non solo interpretare il loro diritto nazionale in modo conforme a tali direttive, ma anche evitare di fondarsi su un'interpretazione di esse che entri in conflitto con i detti diritti fondamentali o con gli altri principi generali del diritto comunitario, come, ad esempio, il principio di proporzionalità.

[...]

*****

DISCUSSIONE

1. I dati delle connessioni degli utenti (in particolare, l'indirizzo IP) sono da considerare quali dati personali?
2. Che differenza esiste tra indirizzo IP statico e dinamico?
3. Quali sono i diritti fondamentali in conflitto in questo caso? Che bilanciamento può essere trovato?
4. Il diritto comunitario impone o consente che i dati sulle connessioni siano messi a disposizione dell'autorità nell'ambito di processi civili? Cosa ne pensate?

*****

NORME

- artt.7, 8, 17, 47, Carta dei diritti fondamentali dell'Unione Europea
- artt.15, n.2, e 18, direttiva 2000/31/CE
- art.8, nn.1 e 2, direttiva 2001/29/CE
- art.8, direttiva 2004/48/CE
6. PRIVACY E COMUNICAZIONI
6.1. Comunicazioni elettroniche e sorveglianza

Corte di Giustizia delle Comunità Europee, 8 aprile 2014 (cause riunite C-293/12 e C-594/12)

[...]


2. La domanda proposta dalla High Court (causa C-293/12) verte su una controversia che contrappone la Digital Rights Ireland Ltd (in prosieguo: la « Digital Rights») al Minister for Communications, Marine and Natural Resources, al Minister for Justice, Equality and Law Reform, al Commissioner of the Garda Síochána, all'Irlanda nonché all'Attorney General, in merito alla legittimità di misure legislative e amministrative nazionali riguardanti la conservazione di dati relativi a comunicazioni elettroniche.

3. La domanda proposta dal Verfassungsgerichtshof (causa C-594/12) è relativa a ricorsi in materia costituzionale proposti dinanzi a tale organo giurisdizionale dalla Kärntner Landesregierung (governo del Land di Carinzia) nonché dai sigg. Seitzlinger, Tschohl e da altri 11.128 ricorrenti, in merito alla compatibilità della legge che attua la direttiva 2006/24 nel diritto interno austriaco con la legge costituzionale federale (Bundes-Verfassungsgesetz).

[...]

Procedimenti principali e questioni pregiudiziali
La causa C-293/12

17. L’11 agosto 2006 la Digital Rights ha presentato dinanzi alla High Court un ricorso nell’ambito del quale sostiene di essere proprietaria di un telefono cellulare che è stato registrato il 3 giugno 2006 e da essa utilizzato a partire da tale data. Essa mette in discussione la legittimità di misure legislative e amministrative nazionali riguardanti la conservazione di dati relativi a comunicazioni elettroniche e chiede, in particolare, al giudice del rinvio di dichiarare la nullità della direttiva 2006/24 e della parte settima della legge del 2005 sulla giustizia penale (reati terroristici) [Criminal Justice (Terrorist Offences) Act 2005], la quale impone ai fornitori di servizi di telefonia di conservare i dati relativi al traffico e all’ubicazione per un lasso di tempo specificato dalla legge a fini di prevenzione, accertamento, indagini o perseguimento dei reati e di protezione della sicurezza dello Stato.

18. Ritenendo di non essere in grado di risolvere le questioni relative al diritto nazionale ad essa sottoposte senza che fosse stata prima esaminata la validità della direttiva 2006/24, la High Court ha deciso di sospendere il giudizio e di sottoporre alla Corte le seguenti questioni pregiudiziali:

«1) Se la limitazione dei diritti della ricorrente in relazione all’utilizzo della telefonia mobile, derivante dalle disposizioni degli artt.3, 4 e 6 della direttiva 2006/24/CE, sia incompatibile con l’art.5, §4, TUE in quanto non proporzionata, non necessaria o non adeguata per il perseguimento dei seguenti obiettivi legittimi:
   a) garantire la disponibilità di determinati dati a fini di indagine, accertamento e perseguimento di reati gravi,
   e/o
   b) garantire il corretto funzionamento del mercato interno dell’Unione Europea.
2) In particolare,
   a) se la direttiva 2006/24/CE sia compatibile con il diritto dei cittadini di circolare e soggiornare liberamente nel territorio degli Stati membri sancito dall’art.21 TFUE;
   b) se la direttiva 2006/24/CE sia compatibile con il diritto al rispetto della vita privata sancito dall’art.7 della [Carta dei diritti fondamentali dell’Unione Europea (in prosieguo: la “Carta”)] e dall’art.8 della [CEDU];
   c) se la direttiva 2006/24/CE sia compatibile con il diritto alla protezione dei dati di carattere personale sancito all’art.8 della Carta;»
d) se la direttiva 2006/24/CE sia compatibile con il diritto alla libertà di espressione sancito dall’art.11 della Carta e dall’art.10 della [CEDU];
e) se la direttiva 2006/24/CE sia compatibile con il diritto ad una buona amministrazione contemplato dall’art.41 della Carta.

3) In che misura i Trattati – e, in particolare, il principio di leale collaborazione di cui all’art.4, §3, TUE – impongono al giudice nazionale di esaminare e valutare la compatibilità delle misure nazionali volte a trasporre la direttiva 2006/24/CE con le garanzie previste dalla [Carta], ivi compreso il suo art.7 (come ispirato dall’art.8 della [CEDU])».

La causa C-594/12


20. Il Verfassungsgerichtshof si chiede, in particolare, se la direttiva 2006/24 sia compatibile con la Carta in quanto permette di immagazzinare una massa di dati relativi ad un numero illimitato di persone per un lungo tempo. La conservazione dei dati riguarderebbe quasi esclusivamente persone il cui comportamento non giustifica affatto la conservazione dei dati che le riguardano. Tali persone sarebbero esposte ad un rischio elevato di vedere le autorità ricercare i loro dati, venire a conoscenza del relativo contenuto, informarsi sulla loro vita privata e utilizzare tali dati per molteplici fini, tenuto conto, segnatamente, del numero incalcolabile di persone che hanno accesso ai dati per un periodo di almeno sei mesi. Secondo il giudice del rinvio, vi sono dubbi, da un lato, circa il fatto che la direttiva sia idonea al raggiungimento degli obiettivi da essa perseguiti e, dall’altro lato, circa la proporzionalità dell’ingerenza nei diritti fondamentali interessati.

21. Il Verfassungsgerichtshof ha pertanto deciso di sospendere il procedimento e di sottoporre alla Corte le seguenti questioni pregiudiziali:

«1) Sulla validità degli atti delle istituzioni dell’Unione:
Se gli articoli da 3 a 9 della direttiva 2006/24 siano compatibili con gli artt.7, 8 e 11 della [Carta].

2) Sull’interpretazione dei Trattati:
   a) Se, alla luce delle spiegazioni relative all’art.8 della Carta che, a norma dell’art.52, §7, della stessa, sono state elaborate al fine di fornire orientamenti per l’interpretazione [di quest’ultima] e di cui il Verfassungsgerichtshof deve tenere debito conto, la direttiva 95/46 e il regolamento (CE) n.45/2001 […], del 18 dicembre 2000, concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati […] debbano essere considerati equivalenti alle condizioni stabilite dall’art.8, §2, e dall’art.52, §1, della Carta per valutare l’ammissibilità delle ingerenze.
   b) Quale sia il rapporto tra il “diritto dell’Unione”, menzionato nell’art.52, §3, ultima frase, della Carta, e le direttive in materia di protezione dei dati.
   c) Se, dato che la direttiva 95/46/CE e il regolamento (…) n.45/2001 pongono condizioni e limiti all’esercizio del diritto fondamentale alla protezione dei dati sancito dalla Carta, nell’interpretare l’art.8 [di quest’ultima] occorra tener conto dei cambiamenti derivanti dalla norme successive di diritto derivato.
   d) Se, in considerazione dell’art.52, §4, della Carta, dal principio della salvaguardia di livelli di protezione più elevati, di cui all’art.53 della Carta, discenda che i limiti che [quest’ultima] pone alle restrizioni che il diritto derivato può legittimamente apportare debbano essere applicati in base a criteri più rigorosi.
   e) Se, tenuto conto dell’art.52, §3, della Carta, del quinto comma del preambolo e delle spiegazioni relative all’art.7 [di quest’ultima], secondo cui i diritti garantiti da tale articolo corrispondono a quelli garantiti dall’art.8 della CEDU, la giurisprudenza della Corte europea dei diritti dell’uomo relativa all’art.8 della CEDU possa fornire indicazioni interpretative rilevanti ai fini dell’interpretazione di quest’ultimo articolo».

22. Con decisione del presidente della Corte dell’11 giugno 2013, le cause C-293/12 e C-594/12 sono state riunite ai fini della fase orale e della sentenza.
Sulle questioni pregiudiziali
Sulla seconda questione, lettere da b) a d), nella causa C-293/12 e sulla prima questione nella causa C-594/12

23. Con la seconda questione, lettere da b) a d), nella causa C-293/12 e la prima questione nella causa C-594/12, che vanno esaminate congiuntamente, i giudici del rinvio chiedono in sostanza alla Corte di esaminare la validità della direttiva 2006/24 alla luce degli artt. 7, 8 e 11 della Carta.

Sulla rilevanza degli artt. 7, 8 e 11 della Carta con riferimento alla questione di validità della direttiva 2006/24

24. Dall’art. 1 e dai considerando 4, 5, da 7 a 11, 21 e 22 della direttiva 2006/24 emerge che l’obiettivo principale di quest’ultima è quello di armonizzare le disposizioni degli Stati membri relative alla conservazione, da parte dei fornitori di servizi di comunicazione elettronica accessibili al pubblico o di una rete pubblica di comunicazione, di determinati dati da essi generati o trattati, allo scopo di garantirne la disponibilità a fini di prevenzione, indagine, accertamento e perseguimento di reati gravi, come quelli legati alla criminalità organizzata e al terrorismo, nel rispetto dei diritti sanciti dagli artt. 7 e 8 della Carta.

25. L’obbligo dei fornitori di servizi di comunicazione elettronica accessibili al pubblico o di una rete pubblica di comunicazione, previsto dall’art. 3 della direttiva 2006/24, di conservare i dati elencati all’art. 5 della stessa al fine di renderli all’occorrenza accessibili alle autorità nazionali competenti solleva questioni relative alla protezione tanto della vita privata quanto delle comunicazioni, sancita dall’art. 7 della Carta, alla tutela dei dati personali, prevista dall’art. 8 della stessa, nonché al rispetto della libertà di espressione, garantita dall’art. 11 della Carta.

26. In proposito, va rilevato che i dati che i fornitori di servizi di comunicazione elettronica accessibili al pubblico o di una rete pubblica di comunicazione debbono conservare, ai sensi degli artt. 3 e 5 della direttiva 2006/24, sono, in particolare, i dati necessari per rintracciare e identificare la fonte di una comunicazione e la destinazione della stessa, per stabilire la data, l’ora, la durata e il tipo di una comunicazione, le attrezzature di comunicazione degli utenti nonché per determinare l’ubicazione delle apparecchiature di comunicazione mobile, dati tra i quali figurano, segnatamente, il nome e l’indirizzo dell’abbonato o dell’utente registrato, il numero telefonico chiamante e quello chiamato, nonché un indirizzo IP per i servizi Internet. I suddetti dati permettono, in particolare, di sapere quale sia la persona con cui un abbonato o un utente registrato ha comunicato e con quale mezzo, così come di stabilire il tempo della comunicazione e il luogo dal quale questa è avvenuta. Inoltre, essi permettono di conoscere la frequenza delle comunicazioni dell’abbonato o dell’utente registrato con talune persone nel corso di un determinato periodo.

27. Questi dati, presi nel loro complesso, possono permettere di trarre conclusioni molto precise riguardo alla vita privata delle persone i cui dati sono stati conservati, come le abitudini quotidiane, i luoghi di soggiorno permanente o temporaneo, gli spostamenti giornalieri e non, le attività svolte, le relazioni sociali di queste persone e gli ambienti sociali da esse frequentati.

28. Di conseguenza, sebbene la direttiva 2006/24 non autorizzi, come emerge dagli artt. 1, §2, e 5, §2 della stessa, la conservazione del contenuto della comunicazione e delle informazioni consultate utilizzando una rete di comunicazione elettronica, non è escluso che la conservazione dei dati di cui trattasi possa incidere sull’utilizzo, da parte degli abbonati o degli utenti registrati, dei mezzi di comunicazione cui fa riferimento la suddetta direttiva e, di conseguenza, sull’esercizio, da parte di questi ultimi, della loro libertà di espressione, garantita dall’art. 11 della Carta.

29. La conservazione dei dati affinché le autorità nazionali competenti possano eventualmente accedervi, come prevista dalla direttiva 2006/24, riguarda in modo specifico e diretto la vita privata e, di conseguenza, i diritti garantiti dall’art. 7 della Carta. Inoltre, tale conservazione dei dati rientra altresì nell’art. 8 di quest’ultima, poiché costituisce un trattamento dei dati di carattere personale ai sensi del suddetto articolo e deve, pertanto, necessariamente rispondere ai requisiti di protezione dei dati derivanti da tale articolo (sentenza Volker und Markus Schecke e Eifert, C-92/09 e C-93/09, […] p.to 47).

30. Benché i rinvii pregiudiziali nelle presenti cause sollevino, in particolare, la questione di principio di stabilire se i dati degli abbonati e degli utenti registrati possano o meno essere conservati, alla luce dell’art. 7 della Carta, essi riguardano altresì la questione se la direttiva 2006/24 risponda alle esigenze di protezione dei dati personali derivanti dall’art. 8 della Carta.
31. Tenuto conto delle considerazioni che precedono, al fine di rispondere alla seconda questione, lettere da b) a d), nella causa C-293/12 e la prima questione nella causa C-594/12, occorre esaminare la validità della direttiva alla luce degli artt. 7 e 8 della Carta.

**Sull’esistenza di un’ingerenza nei diritti sanciti dagli artt. 7 e 8 della Carta**

32. Imponendo la conservazione dei dati elencati all’art. 5, § 1, della direttiva 2006/24 e permettendo l’accesso delle autorità nazionali competenti a questi ultimi, la suddetta direttiva, come rilevato dall’avvocato generale in particolare ai §§39 e 40 delle sue conclusioni, deroga al regime di tutela del diritto al rispetto della vita privata, istituito dalle direttive 95/46 e 2002/58, con riferimento al trattamento dei dati personali nel settore delle comunicazioni elettroniche, in quanto le suddette direttive hanno previsto la riservatezza delle comunicazioni e dei dati relativi al traffico nonché l’obbligo di cancellare o di rendere anonimi i dati stessi quando non siano più necessari alla trasmissione di una comunicazione, a meno che non siano necessari per la fatturazione e solo fintanto che tale necessità perduri.

33. Per accertare l’esistenza di un’ingerenza nel diritto fondamentale al rispetto della vita privata, poco importa che le informazioni relative alla vita privata di cui trattasi abbiano o meno un carattere sensibile o che gli interessati abbiano o meno subito eventuali inconvenienze in seguito a tale ingerenza (v., in tal senso, sentenza Österreichischer Rundfunk e a., C-465/00, C-138/01 e C-139/01, […] p.to 75).

34. Di conseguenza, l’obbligo, imposto dagli artt. 3 e 6 della direttiva 2006/24 ai fornitori di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione elettronica, di conservare per un certo periodo dati relativi alla vita privata di una persona e alle sue comunicazioni, come quelli previsti dall’art. 5 della suddetta direttiva, costituisce di per sé un’ingerenza nei diritti garantiti dall’art. 7 della Carta.

35. Inoltre, l’accesso delle autorità nazionali competenti ai dati costituisce un’ingerenza supplementare in tale diritto fondamentale (v., per quanto riguarda l’art. 8 della CEDU, sentenze della Corte EDU, Leander c. Svezia, del 26 marzo 1987, […], § 48; Rotaru c. Romania [GC], n.28341/95, § 46, […], nonché Weber e Saravia c. Germania (dec.), n.54934/00, § 79, […]). Pertanto, anche gli artt. 4 e 8 della direttiva 2006/24, i quali prevedono regole relative all’accesso delle autorità nazionali competenti ai dati, sono costitutivi di un’ingerenza nei diritti garantiti dall’art. 7 della Carta.

36. Parimenti, la direttiva 2006/24 è costitutiva di un’ingerenza nel diritto fondamentale alla protezione dei dati personali garantito dall’art. 8 della Carta, poiché prevede un trattamento dei dati personali.

37. È giocoforza constatare che l’ingerenza che la direttiva 2006/24 comporta nei diritti fondamentali sanciti dagli artt. 7 e 8 della Carta si rivela essere, come peraltro osserva l’avvocato generale, in particolare ai §§77 e 80 delle sue conclusioni, di vasta portata e va considerata particolarmente grave. Inoltre, il fatto che la conservazione dei dati e l’utilizzo ulteriore degli stessi siano effettuati senza che l’abbonato o l’utente registrato ne siano informati può ingenerare nelle persone interessate, come rilevato dall’avvocato generale ai §§52 e 72 delle sue conclusioni, la sensazione che la loro vita privata sia oggetto di costante sorveglianza.

**Sulla giustificazione dell’ingerenza nei diritti garantiti dagli artt. 7 e 8 della Carta**

38. Conformemente all’art. 52, § 1, della Carta, eventuali limitazioni all’esercizio dei diritti e delle libertà riconosciuti da quest’ultima devono essere previste dalla legge, rispettare il loro contenuto essenziale e, nel rispetto del principio di proporzionalità, possono essere apportate limitazioni a detti diritti e libertà solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall’Unione o all’esigenza di proteggere i diritti e le libertà altrui.

39. Per quanto riguarda il contenuto essenziale del diritto fondamentale al rispetto della vita privata e degli altri diritti sanciti all’art. 7 della Carta, si deve rilevare che, sebbene la conservazione dei dati impostata dalla direttiva 2006/24 costituisca un’ingerenza particolarmente grave in tali diritti, essa non è tale da pregiudicare il suddetto contenuto poiché, come deriva dall’art. 1, § 2, della stessa direttiva, quest’ultima non permette di venire a conoscenza del contenuto delle comunicazioni elettroniche in quanto tale.

40. Tale conservazione dei dati non è neppure idonea a pregiudicare il contenuto essenziale del diritto fondamentale alla protezione dei dati personali, sancito all’art. 8 della Carta, considerato che la direttiva 2006/24 prevede, all’art. 7, una regola relativa alla protezione e alla sicurezza dei dati ai sensi della quale, fatte salve le disposizioni adottate in conformità delle direttive 95/46 e
2002/58, i fornitori di servizi di comunicazione elettronica accessibili al pubblico o di una rete pubblica di comunicazione sono tenuti a rispettare taluni principi di protezione e di sicurezza dei dati, principi in base ai quali gli Stati membri assicurano l’adozione di adeguate misure tecniche e organizzative contro la distruzione accidentale o illecita, la perdita o l’alterazione accidentale dei dati.

41. Quanto alla questione consistente nell’accertare se la suddetta ingerenza risponda a un obiettivo di interesse generale, occorre rilevare che, sebbene la direttiva 2006/24 sia destinata ad armonizzare le disposizioni degli Stati membri relative agli obblighi dei suddetti fornitori in materia di conservazione di taluni dati da essi generati o trattati, l’obiettivo sostanziale della direttiva consiste, come risulta dall’art.1, §1, della stessa, nel garantire la disponibilità dei suddetti dati a fini di indagine, accertamento e perseguimento di reati gravi, quali definiti da ciascuno Stato membro nella propria legislazione nazionale. L’obiettivo sostanziale della direttiva è pertanto quello di contribuire alla lotta contro la criminalità grave e, di conseguenza, in ultima analisi, alla sicurezza pubblica.


43. Al riguardo, dal considerando 7 della direttiva 2006/24 emerge che, a motivo dell’importante aumento delle possibilità offerte dalle comunicazioni elettroniche, il Consiglio «Giustizia e affari interni» del 19 dicembre 2002 ha considerato che i dati relativi all’uso di queste ultime costituiscono uno strumento particolarmente importante e valido nella prevenzione dei reati e nella lotta contro la criminalità, in particolare della criminalità organizzata.

44. È giocoforza constatare quindi che la conservazione dei dati per permettere alle autorità nazionali competenti di disporre di un accesso eventuale agli stessi, come imposto dalla direttiva 2006/24, risponde effettivamente a un obiettivo di interesse generale.

45. Di conseguenza, è necessario verificare la proporzionalità dell’ingerenza constatata.

46. A questo proposito, si deve ricordare che il principio di proporzionalità esige, secondo una costante giurisprudenza della Corte, che gli atti delle istituzioni dell’Unione siano idonei a realizzare gli obiettivi legittimi perseguiti dalla normativa di cui trattasi e non superino i limiti di ciò che è idoneo e necessario al conseguimento degli obiettivi stessi (v., in tal senso, sentenze *Afton Chemical*, C-343/09, […], p.to 45; *Volker und Markus Schecke e Eifert*, […], p.to 74; *Nelson e a., C-581/10 e C-629/10*, […], p.to 71; *Sky Österreich*, C-283/11, […] p.to 50, nonché *Schaible, C-101/12, […], p.to 29*).

47. Per quanto riguarda il controllo giurisdizionale del rispetto delle suddette condizioni, allorché si tratta di ingerenze in diritti fondamentali, la portata del potere discrezionale del legislatore dell’Unione può risultare limitata in funzione di un certo numero di elementi, tra i quali figurano, in particolare, il settore interessato, la natura del diritto di cui trattasi garantito dalla Carta, la natura e la gravità dell’ingerenza nonché la finalità di quest’ultima (v., per analogia, per quanto riguarda l’art.8 della CEDU, sentenza Corte EDU, *S e Marper c. Regno Unito* [GC], nn.30562/04 e 30566/04, §102, […]).

48. Nel caso di specie, tenuto conto, da un lato, del ruolo importante svolto dalla protezione dei dati personali sotto il profilo del diritto fondamentale al rispetto della vita privata e, dall’altro, della portata e della gravità dell’ingerenza in tale suddetto diritto che la direttiva 2006/24 comporta, il potere discrezionale del legislatore dell’Unione risulta ridotto e di conseguenza è necessario procedere ad un controllo stretto.

49. Per quel che riguarda la questione consistente nell’accertare se la conservazione dei dati sia idonea a realizzare l’obiettivo perseguito dalla direttiva 2006/24, si deve constatare che, tenuto conto della crescente importanza dei mezzi di comunicazione elettronica, i dati che debbono essere conservati in attuazione della detta direttiva permettono alle autorità nazionali competenti in materia di perseguimento di reati di disporre di possibilità supplementari di accertamento dei reati gravi e, al riguardo, costituiscono quindi uno strumento utile per le indagini penali. Pertanto, la
conservazione dei suddetti dati può essere considerata come idonea a realizzare l'obiettivo perseguito dalla suddetta direttiva.

[...]

51. Quanto al carattere necessario della conservazione dei dati imposta dalla direttiva 2006/24, si deve constatare che, invero, la lotta contro la criminalità grave, in particolare contro la criminalità organizzata e il terrorismo, è di capitale importanza per garantire la sicurezza pubblica e la sua efficacia può dipendere in larga misura dall'uso delle moderne tecniche di indagine. Tuttavia, simile obiettivo di interesse generale, per quanto fondamentale, non può di per sé giustificare il fatto che una misura di conservazione, come quella istituita dalla direttiva 2006/24, sia considerata necessaria ai fini della suddetta lotta.

52. Per quel che riguarda il rispetto della vita privata, la protezione di tale diritto fondamentale, secondo la costante giurisprudenza della Corte, richiede in ogni caso che le deroghe e le restrizioni alla tutela dei dati personali debbano operare entro i limiti dello stretto necessario (sentenza IPI, C-473/12, [...], p.to 39 e giurisprudenza ivi citata).

53. A questo proposito, occorre ricordare che la tutela dei dati personali, risultante dall'obbligo esplicito previsto all'art.8, §1, della Carta, riveste un'importanza particolare per il diritto al rispetto della vita privata sancito dall'art.7 della stessa.

54. Pertanto, la normativa dell'Unione di cui trattasi deve prevedere regole chiare e precise che disciplinino la portata e l'applicazione della misura de qua e impongano requisiti minimi in modo che le persone i cui dati sono stati conservati dispongano di garanzie sufficienti che permettano di proteggere efficacemente i loro dati personali contro il rischio di abusi nonché contro eventuali accessi e usi illeciti dei suddetti dati (v., per analogia, per quanto riguarda l’art.8 della CEDU, sentenze Corte EDU, Liberty e altri c. Regno Unito, n.58243/00, §§62 e 63, del 1º luglio 2008; Rotaru c. Romania, cit., paragrafi da 57 a 59, nonché S e Marper c. Regno Unito, cit., §99).

55. La necessità di disporre di siffatte garanzie è tanto più importante allorché, come prevede la direttiva 2006/24, i dati personali sono soggetti a trattamento automatico ed esiste un rischio considerevole di accesso illecito ai dati stessi (v., per analogia, con riguardo all’art.8 della CEDU, sentenze Corte EDU, S e Marper c. Regno Unito, cit., §103, nonché M.K. c. Francia, n.19522/09, §35, del 18 aprile 2013).

56. Quanto alla questione consistente nell’accertare se l’ingerenza che la direttiva 2006/24 comporta sia limitata allo stretto necessario, si deve rilevare che tale direttiva impone, conformemente al suo art.3, in combinato disposto con l’art.5, §1, della stessa, la conservazione di tutti i dati relativi al traffico riguardante la telefonia fissa, la telefonia mobile, l’accesso a Internet, la posta elettronica su Internet nonché il traffico di indagine (v., per analogia, con riguardo all’art.8 della CEDU, sentenze Corte EDU, S e Marper c. Regno Unito, cit., §103, nonché M.K. c. Francia, n.19522/09, §35, del 18 aprile 2013).

57. A questo proposito, si deve rilevare, in primo luogo, che la direttiva 2006/24 riguarda in maniera generale qualsiasi persona e qualsiasi mezzo di comunicazione elettronica nonché l’insieme dei dati relativi al traffico senza alcuna distinzione, limitazione o eccezione a seconda dell’obiettivo di lotta contro i reati gravi.

58. Infatti, da un lato, la direttiva 2006/24 riguarda in maniera globale l’insieme delle persone che fanno uso dei mezzi di comunicazione elettronica, senza tuttavia che le persone i cui dati vengono conservati debbano trovarsi, anche indirettamente, in una situazione che possa dar luogo a indagini penali. Essa pertanto si applica anche a persone per le quali non esiste alcun indizio tale da far credere che il loro comportamento possa avere un nesso, ancorché indiretto o lontano, con reati gravi. Inoltre, essa non prevede alcuna deroga, e pertanto si applica anche a persone le cui comunicazioni sono soggette, in base alle norme del diritto nazionale, al segreto professionale.

59. Dall’altro lato, pur mirando a contribuire alla lotta contro la criminalità grave, la suddetta direttiva non impone alcuna relazione tra i dati di cui prevede la conservazione e una minaccia per la sicurezza pubblica e, in particolare, non limita la conservazione dei dati a quelli relativi a un determinato periodo di tempo e/o a un’area geografica determinata e/o a una cerchia di persone determinate che possano essere coinvolti, in un modo o nell’altro, in un reato grave, né alle persone la conservazione dei cui dati, per altri motivi, potrebbe contribuire alla prevenzione, all’accertamento o al perseguimento di reati gravi.
60. In secondo luogo, alla suddetta mancanza generale di limiti si aggiunge il fatto che la direttiva 2006/24 non prevede alcun criterio oggettivo che permetta di delimitare l'accesso delle autorità nazionali competenti ai dati e il loro uso ulteriore a fini di prevenzione, di accertamento o di indagini penali riguardanti reati che possano, con riguardo alla portata e alla gravità dell'ingerenza nei diritti fondamentali sanciti dagli artt. 7 e 8 della Carta, essere considerati sufficientemente gravi da giustificare siffatta ingerenza. Al contrario, la direttiva 2006/24 si limita a rinviare, all'art.1, §1, in maniera generale ai reati gravi come definiti da ciascuno Stato membro nel proprio diritto interno.

61. Inoltre, per quanto riguarda l'accesso delle autorità nazionali competenti ai dati e al loro uso ulteriore, la direttiva 2006/24 non contiene le condizioni sostanziali e procedurali ad esso relative. L'art.4 della direttiva, che regola l'accesso di tali autorità ai dati conservati, non stabilisce espressamente che tale accesso e l'uso ulteriore dei dati di cui trattasi debbano essere strettamente limitati a fini di prevenzione e di accertamento di reati gravi delimitati con precisione o di indagini penali ad essi relative, ma si limita a prevedere che ciascuno Stato membro definisca le procedure da seguire e le condizioni da rispettare per avere accesso ai dati conservati in conformità dei criteri di necessità e di proporzionalità.

62. In particolare, la direttiva 2006/24 non prevede alcun criterio oggettivo che permetta di limitare il numero di persone che dispongono dell'autorizzazione di accesso e di uso ulteriore dei dati conservati a quanto strettamente necessario alla luce dell'obiettivo perseguito. Inoltre, l'accesso ai dati conservati da parte delle autorità nazionali competenti non è subordinato ad un previo controllo effettuato da un giudice o da un'entità amministrativa indipendente la cui decisione sia diretta a limitare l'accesso ai dati e il loro uso a quanto strettamente necessario per raggiungere l'obiettivo perseguito e intervenga a seguito di una richiesta motivata delle suddette autorità presentata nell'ambito di procedure di prevenzione, di accertamento o di indagini penali. Non è neppure stato previsto un obbligo preciso degli Stati membri volto a stabilire simili limitazioni.

63. In terzo luogo, quanto alla durata di conservazione dei dati, la direttiva 2006/24 impone, all'art.6, la conservazione degli stessi per un periodo di almeno sei mesi senza che venga effettuata alcuna distinzione tra le categorie di dati previste all'art. 5 della direttiva a seconda della loro eventuale utilità ai fini dell'obiettivo perseguito o a seconda delle persone interessate.

64. Tale durata, inoltre, si colloca tra un minimo di sei mesi e un massimo di ventiquattro mesi, senza che venga precisato che la determinazione della durata di conservazione debba basarsi su criteri obiettivi al fine di garantire che sia limitata allo stretto necessario.

65. Da quanto precede deriva che la direttiva 2006/24 non prevede norme chiare e precise che regolino la portata dell'ingerenza nei diritti fondamentali sanciti dagli artt. 7 e 8 della Carta. Pertanto, è giocoforza constatare che tale direttiva comporta un'ingerenza nei suddetti diritti fondamentali di vasta portata e di particolare gravità nell'ordinamento giuridico dell'Unione, senza che siffatta ingerenza sia regolamentata con precisione da disposizioni che permettano di garantire che essa sia effettivamente limitata a quanto strettamente necessario.

66. Per di più, per quanto riguarda le norme riguardanti la sicurezza e la protezione dei dati conservati dai fornitori di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione, si deve constatare che la direttiva 2006/24 non prevede garanzie sufficienti, come richieste dall'art.8 della Carta, che permettano di assicurare una protezione efficace dei dati conservati contro i rischi di abuso nonché contro eventuali accessi e usi illeciti dei suddetti dati. Infatti, in primo luogo, l'art.7 della direttiva 2006/24 non prevede norme specifiche e adatte alla vasta quantità di dati di cui la direttiva impone la conservazione, al carattere sensibile dei suddetti dati nonché al rischio di accesso illecito a questi ultimi, norme che servirebbero, in particolare, a regolare in maniera chiara e precisa la protezione e la sicurezza dei dati di cui trattasi, al fine di garantirne la piena integrità e riservatezza. Inoltre, non è stato neppure previsto un obbligo preciso degli Stati membri di stabilire siffatte norme.

67. L'art.7 della direttiva 2006/24, in combinato disposto con gli artt.4, §1, della direttiva 2002/58 e 17, §1, secondo comma, della direttiva 95/46, non garantisce che sia applicato dai detti fornitori un livello particolarmente elevato di protezione e di sicurezza attraverso misure tecniche e organizzative, ma autorizza in particolare i suddetti fornitori a tener conto di considerazioni economiche nel determinare il livello di sicurezza da essi applicato, per quanto riguarda i costi di attuazione delle misure di sicurezza. In particolare, la direttiva 2006/24 non garantisce la distruzione irreversibile dei dati al termine della durata di conservazione degli stessi.
68. In secondo luogo, si deve aggiungere che tale direttiva non impone che i dati di cui trattasi siano conservati sul territorio dell’Unione, e di conseguenza non si può ritenere pienamente garantito il controllo da parte di un’autorità indipendente, esplicitamente richiesto dall’art.8, §3, della Carta, del rispetto dei requisiti di protezione e di sicurezza, quali richiamati ai due punti precedenti. Orbene, siffatto controllo, effettuato in base al diritto dell’Unione, costituisce un elemento essenziale del rispetto della tutela delle persone riguardo al trattamento dei dati personali (v., in tal senso, sentenza Commissione/Austria, C-614/10, […], p.to 37).

69. Alla luce dell’insieme delle osservazioni che precedono, si deve considerare che, adottando la direttiva 2006/24, il legislatore dell’Unione ha ecceduto i limiti imposti dal rispetto del principio di proporzionalità alla luce degli artt.7, 8 e 52, §1, della Carta.

70. Di conseguenza, non vi è motivo di esaminare la validità della direttiva 2006/24 alla luce dell’art.11 della Carta.

71. Occorre pertanto rispondere alla seconda questione, lettere da b) a d), nella causa C-293/12 e alla prima questione nella causa C-594/12 dichiarando che la direttiva 2006/24 è invalida.

Sulla prima questione e sulla seconda questione, lett. a) ed e), nonché sulla terza questione nella causa C-293/12 e sulla seconda questione nella causa C-594/12

72. Da quanto dichiarato al punto precedente deriva che non vi è motivo di rispondere alla prima questione, alla seconda questione, lett.a) ed e), e alla terza questione nella causa C-293/21, né alla seconda questione nella causa C-594/12.

[…]

Per questi motivi, la Corte (Grande Sezione) dichiara:


*****

DISCUSSIONE

1. Quali erano le finalità alla base dell’emanazione della direttiva 2006/24/CE riguardante la conservazione di dati relativi a comunicazioni elettroniche?

2. Quali sono le norme della Carta dei diritti fondamentali dell’Unione Europea che si sostiene siano state violate dalla citata direttiva?

3. In cosa consiste la violazione?

4. Il caso ripropone il difficile bilanciamento tra sicurezza e libertà individuale, in riferimento alle comunicazioni elettroniche. Quali sono i criteri per individuare tale bilanciamento?

*****

NORME

- artt.7, 8, 11, CDFUE
6.2. Posta elettronica non sollecitata

Garante per la protezione dei dati personali, provv. generale 4 luglio 2013

[...]

1. Oggetto e finalità del presente provvedimento generale

[...]

Il Garante ravvisa, quindi, la necessità di adottare le presenti linee guida con le seguenti finalità:
- tenere conto del mutato quadro normativo attualmente vigente in materia, alla luce dell'entrata in vigore del Codice e delle modifiche normative successive, nonché del diritto comunitario (direttive 2002/58/UE e 2009/136/UE), con l'ulteriore obiettivo di assicurare l'uniforme applicazione della stessa normativa e l'osservanza del fondamentale principio di certezza del diritto;
- chiarire alcuni profili problematici relativi alle diverse modalità di spam, affinché gli operatori del settore possano conformarsi alla disciplina sul trattamento dei dati personali;
- inquadrare alcune nuove forme di spam, con l'intento di limitare i rischi connessi alle novità tecnologiche, pur nella necessaria consapevolezza del carattere parziale e non risolutivo dello strumento del diritto rispetto a tecnologie in continua evoluzione, peraltro sempre più avanzate e di rapida diffusione.

2. Il mutato quadro normativo in materia di spam

2.1 Ambito oggettivo dello spam

Anzitutto occorre definire il fenomeno dello spam che, ai fini del Codice, è costituito dalle comunicazioni per l'invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale (v. artt.7, comma 4, lett.b, 130, comma 1 e 140 del Codice) effettuate, in violazione delle norme del Codice, con sistemi automatizzati di chiamata senza operatore (c.d. telefonate preregistrate) oppure con modalità assimilate alle prime (quali: e-mail, fax, sms, mms).

Ai fini dell'applicazione del Codice, non è necessario un invio massiccio e/o simultaneo a una pluralità di indirizzi o numeri di telefono, poiché siffatta modalità rileva solo eventualmente per qualificare il trattamento come sistematico per la quantificazione delle sanzioni.

2.2 Ambito soggettivo dello spam e le tutele azionabili

Considerate le rilevanti novità normative di cui si dirà di seguito, va chiarito anche l'ambito soggettivo delle disposizioni del Codice in materia di spam e quello dei diritti azionabili dai destinatari delle comunicazioni promozionali automatizzate. Mentre le persone fisiche possono esercitare i diritti di cui agli artt.7 e ss. del Codice al fine di tutelare la propria sfera personale da ingerenze illecite, le persone giuridiche sono, allo stato, sprovviste della possibilità di avvalersi dei medesimi mezzi di tutela.

Al riguardo, va infatti considerato l'art.40, comma 2, del d.l. del 6 dicembre 2011, n.201 (c.d. decreto "salva Italia"), convertito con legge del 22 dicembre 2011, n.214, che ha modificato alcune disposizioni contenute nella parte prima del Codice recante le "Disposizioni generali", quali ad esempio l'art.4 relativo, tra l'altro, alle nozioni di "interessato" e di "dato personale", in particolare eliminando ogni riferimento alle persone giuridiche o assimilate, ossia enti e associazioni ed ha mantenuto il riferimento alle sole persone fisiche.

Successivamente, è entrato in vigore anche il d.lgs. 28 maggio 2012, n.69 a seguito del recepimento della direttiva 2009/136/CE, il quale ha parzialmente modificato alcune disposizioni del capo 1 ("Servizi di comunicazione elettronica") del titolo X ("Comunicazioni elettroniche") del Codice, di diretta derivazione comunitaria poiché emanate in attuazione della direttiva 2002/58/CE, nel cui campo applicativo rientrano le comunicazioni promozionali automatizzate, introducendo la qualifica di "contraente" - la quale riguarda certamente anche le persone giuridiche - in luogo di quella di "abbonato".

A seguito delle suddette modifiche normative e delle conseguenti incertezze interpretative, l'Autorità è intervenuta con il provvedimento generale del 20 settembre 2012 [...], sull'applicabilità del Codice alle persone giuridiche, enti e associazioni.
Sulla base di quanto affermato in tale provvedimento interpretativo, si evidenzia che le persone giuridiche ed enti assimilati, destinatarie dello spamming - differentemente dalla persone fisiche - dal 6 dicembre 2011 non possono più presentare segnalazioni, reclami o ricorsi al Garante, né possono esercitare i diritti di cui agli artt.7 ss. del Codice, perché non possono essere più "interessati".

Tuttavia i detti soggetti, in quanto "contraenti", si possono avvalere degli ordinari strumenti di tutela forniti dall'ordinamento, quindi, possono esperire presso l'autorità giudiziaria ordinaria rimedi civilistici quali, ad esempio, l'azione inibitoria e/o l'azione di risarcimento del danno oppure, eventualmente qualora ricorrono gli elementi costitutivi dell'art.167 c.p., anche sporgere denuncia e quindi attivare un procedimento penale con le relative sanzioni. Inoltre, essi possono beneficiare dell'eventuale esercizio dei poteri di iniziativa ex officio - quanto a provvedimenti inibitori, prescrittivi e/o sanzionatori - da parte di questa Autorità, qualora emergano i presupposti di un possibile trattamento illecito di dati.

Con particolare riferimento alla posta elettronica, alcune volte può risultare difficile distinguere se un destinatario sia una persona fisica o giuridica.

Può essere questo il caso dei dipendenti che lavorano in una determinata società che ha fornito loro indirizzi di posta elettronica aziendale contenenti le loro generalità (ad esempio, nome.cognome@azienda.com).

Ebbene - in linea con quanto precisato dal Gruppo art.29 (con i pareri n.4/1997 e n.5/2004) e sulla base dei criteri di "contenuto", "finalità" o "risultato" ivi enunciati per poter definire alcune informazioni sulle persone giuridiche come "concernenti" persone fisiche - tali indirizzi vanno considerati indirizzi "personalì" di posta elettronica e i loro rispettivi assegnatari come "interessati", con la conseguente applicabilità del Codice e del relativo impianto di diritti e tutele. Ciò, fermo restando quanto già stabilito sull'utilizzo della posta elettronica aziendale dai precedenti provvedimenti del Garante in materia di trattamento dei dati dei lavoratori (in particolare, cfr. "Linee guida del Garante per posta elettronica e Internet" del 1 marzo 2007, […]).

2.3 I principi di correttezza, finalità, proporzionalità e necessità del trattamento dati. La neutralità tecnologica

Alle comunicazioni automatizzate sono applicabili, fra le altre norme del Codice, gli artt.3 e 11, in base ai quali i dati personali considerati, in particolare i numeri di telefonia fissa e mobile e gli indirizzi di posta elettronica, vanno utilizzati e conservati secondo i principi di correttezza, finalità, proporzionalità e necessità e, in caso di violazione del Codice, non possono essere più utilizzati.

Con particolare riferimento alle comunicazioni promozionali effettuate mediante posta elettronica, questa Autorità evidenzia la necessità che i provider di posta elettronica assicurino, nel rispetto del principio di neutralità tecnologica, la mutua autenticazione dei rispettivi server al fine di garantire agli utenti il livello più elevato possibile di protezione antispam. Ciò, tanto più se si considera la dannosità di fenomeni quali il c.d. phishing, ossia l'invio di e-mail contraffatte, con la grafica ed i loghi ufficiali di enti privati (in particolare banche e poste) ed istituzioni, che invitano il destinatario a fornire dati personali, motivando tale richiesta con ragioni di natura tecnica od economica, al fine di perseguire scopi illegali, quali, ad esempio, l'accesso alla password del conto corrente o della carta di credito e poter effettuare operazioni disposizionali all'insaputa dell'interessato e pregiudizievoli della sua sfera giuridico-economica.

In particolare, occorre che i provider provvedano all'installazione di appositi filtri che consentano, con ragionevole grado di certezza, di riconoscere lo spam, evitando, tuttavia, che tali dispositivi comportino una lesione della riservatezza degli interessati.

2.4 L'obbligo di un'informazione chiara e completa ai sensi dell'art.13 del Codice

Un imprescindibile obbligo in capo al titolare del trattamento è quello del previo rilascio ai destinatari delle comunicazioni promozionali dell'informativa disciplinata dall'art.13 del Codice, al fine di assicurare un'informazione chiara e completa, dunque adeguata, relativamente al trattamento dei loro dati, nonché un eventuale consenso al medesimo che sia effettivamente consapevole.

Pertanto, l'interessato o la persona presso la quale sono raccolti i dati personali deve essere previamente informato oralmente o per iscritto riguardo a una serie di elementi obbligatori e indefessibili. Fra questi, vanno specificate le modalità che saranno eventualmente utilizzate per il trattamento dati, e in particolare quelle di cui all'art.130, commi 1 e 2, ossia telefonate automatizzate e modalità assimilate (quali fax, e-mail, sms, mms), oltre che quelle tradizionali
come posta cartacea e telefonate con operatore, nonché le finalità del trattamento stesso (ad esempio, ricerca statistica, *marketing* o profilazione).

Pertanto, sulla base dell’applicabilità di tale norma ai trattamenti effettuati ai fini promozionali tramite strumenti automatizzati o a questi equiparati, si ricorda che, se i dati personali dei destinatari di tali comunicazioni non sono raccolti presso l’interessato, l’informativa, comprensiva delle categorie di dati trattati, deve essere data al medesimo all’atto della registrazione dei dati o, quando è prevista la loro comunicazione, non oltre la prima comunicazione (v. art.13, comma 4, del Codice).

### 2.5 L’obbligo del consenso preventivo (c.d. *opt-in*)

Ai trattamenti effettuati ai fini promozionali tramite strumenti automatizzati o a questi equiparati si applica l’art.130, commi 1 e 2, del Codice, in base al quale l’utilizzo di tali strumenti per le finalità di marketing è consentito solo con il consenso preventivo del contraente o utente (c.d. *opt-in*).

Quindi, ai fini della legittimità della comunicazione promozionale effettuata, non è lecito, con la medesima, avvisare della possibilità di opporsi a ulteriori invii, né è lecito chiedere, con tale primo messaggio promozionale, il consenso al trattamento dati per finalità promozionali.

Pertanto, senza il consenso preventivo - come costantemente ribadito dal Garante a partire dal provvedimento generale sullo spamming del 29 maggio 2003 […] - non è possibile inviare comunicazioni promozionali con i predetti strumenti neanche nel caso in cui i dati personali siano tratti da registri pubblici, elenchi, siti web atti o documenti conosciuti o conoscibili da chiunque.

Analogamente, senza il consenso preventivo degli interessati, non è lecito utilizzare per inviare *e-mail* promozionali gli indirizzi pec contenuti nell’”indice nazionale degli indirizzi pec delle imprese e dei professionisti” - di cui al d.l. 18 ottobre 2012, n.179, convertito con modificazioni dalla l. 17 dicembre 2012, n.221, che ha introdotto l’apposito art.6-bis del d.lgs. 7 marzo 2005, n.82 (Codice dell'amministrazione digitale) - istituito per favorire la presentazione di istanze, dichiarazioni e dati, nonché lo scambio di informazioni e documenti tra la pubblica amministrazione e le imprese e i professionisti in modalità telematica.

È possibile, invece, contattare telefonicamente mediante operatore (per chiedere al contraente di esprimere un consenso a ricevere comunicazioni promozionali secondo le modalità di cui all’art.130, commi 1 e 2) i numeri presenti in elenchi telefonici e non iscritti nel Registro pubblico delle opposizioni (istituito con il d.l. 25 settembre 2009, n.135, convertito, con modificazioni, dalla l. 20 novembre 2009, n.166), nonché quelli presenti in elenchi pubblici “con i limiti e le modalità che le leggi, i regolamenti o la normativa comunitaria stabiliscono per la conoscibilità e pubblicità dei dati”, fra i quali “vi è il vincolo di finalità in base al quale i dati sono raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altri trattamenti in termini compatibili con tali scopi (art.11, comma 1, lett.b) del Codice”*: cfr. provvedimento 19 gennaio 2011 […]

Inoltre, va evidenziato, in un’ottica di coerenza sistematica, che il principio del consenso per il trattamento dei dati vige anche nella disciplina sulla protezione dei consumatori nei contratti a distanza secondo la quale l’impiego da parte di un professionista del telefono, della posta elettronica, di sistemi automatizzati di chiamata senza l’intervento di un operatore o di fax richiede il consenso preventivo del consumatore (v. art.58, d.lgs. n.206/2005, c.d. Codice del consumo).

### 2.6 I requisiti di validità del consenso per la finalità di invio di comunicazioni promozionali

Il consenso acquisito per la finalità di invio di comunicazioni promozionali deve essere libero, informato, specifico, con riferimento a trattamenti chiaramente individuati nonché documentato per iscritto (art.23, comma 3, del Codice) ed è pertanto necessaria la presenza contestuale di tutti i menzionati requisiti, per ritenere tale trattamento conforme al Codice.

Sulla base anche di quanto già indicato nel §2.4, gli interessati devono essere messi in grado di esprimere consapevolmente e liberamente le proprie scelte in ordine al trattamento dei loro dati personali (cfr. provvedimento 24 febbraio 2005, p.to 7, […] e a tal fine devono ricevere un’adeguata informativa, chiara e completa come sopra specificato.

Il consenso del contraente per l’attività promozionale deve intendersi libero quando non è pre-impostato e non risulta - anche solo implicitamente in via di fatto - obbligatorio per poter fruire del prodotto o servizio fornito dal titolare del trattamento.

Esemplicando, non è libero il consenso prestato quando la società condiziona la registrazione al suo sito web da parte degli utenti e, conseguentemente, anche la fruizione dei suoi
servizi, al rilascio del consenso al trattamento per la finalità promozionale. In quest'ottica, il Garante ha già espressamente affermato che non può definirsi "libero", e risulta indebitamente necessitato, il consenso a ulteriori trattamenti di dati personali che l'interessato "debba" prestare quale condizione per conseguire una prestazione richiesta (cfr.: provv. 22 febbraio 2007, […] ; provv. 12 ottobre 2005, […] ; provv. 3 novembre 2005, […] ; provv. 10 maggio 2006, […] ; provv. 15 luglio 2010, […] ; più recentemente, provv. 11 ottobre 2012, […] ).

Analogamente, non è corretta la predisposizione di moduli in cui la casella (c.d. "check-box") di acquisizione del consenso risulta pre-compilata con uno specifico simbolo (c.d. flag) (v. provv. "Consenso al trattamento in Internet e utilizzo dei dati per finalità promozionali", 10 maggio 2006, […] ).

Il consenso del contraente deve essere specifico per ciascuna eventuale finalità perseguita e per ciascun eventuale trattamento effettuato, quale in particolare la comunicazione a terzi per l'invio di loro comunicazioni promozionali, secondo le indicazioni e i chiarimenti forniti di seguito nel presente provvedimento.

2.6.1 Finalità del trattamento
Quanto alle finalità del trattamento di dati personali, si ribadisce che il titolare del trattamento deve acquisire un consenso specifico per ciascuna distinta finalità quali ad esempio: marketing, profilazione, comunicazione a terzi dei dati (cfr. provv. 24 febbraio 2005, p.to 7, […] ).

2.6.2 Consenso per le modalità di marketing (quelle tradizionali e quelle di cui all'art.130, commi 1 e 2 del Codice)
Al fine di attuare l'esigenza di semplificazione degli adempimenti connessi al trattamento dei dati personali, questa Autorità ritiene che sia parimenti legittimo interpretare la regola della specificità del consenso rispetto alle modalità utilizzate per le finalità di marketing, prevedendo due appositi e distinti consensi rispettivamente per le modalità tradizionali e per quelle di cui all'art.130, commi 1 e 2 del Codice, oppure, in alternativa, un unico consenso che comprenda i due tipi di modalità.

2.6.3. Consenso specifico per la comunicazione e/o cessione a soggetti terzi a fini di marketing

2.6.4 Consenso documentato per iscritto
È necessario inoltre che il consenso per la finalità promozionale sia documentato per iscritto.

Va evidenziato che la direttiva 2002/58/CE non stabilisce in modo specifico il metodo per ottenere tale consenso (cfr. considerando 17 della stessa direttiva: "… Il consenso può essere fornito secondo qualsiasi modalità appropriata che consenta all'utente di esprimere liberamente e in conoscenza di causa i suoi desideri specifici, compresa la selezione di un'apposita casella nel caso di un sito Internet").

Ne consegue che gli operatori del settore possono ritenersi liberi di scegliere il metodo che ritengono opportuno nell'ambito della propria libertà organizzativa. Inoltre, non è necessario che il consenso acquisito abbia forma scritta, a pena di invalidità del medesimo, ma è comunque necessario che il titolare del trattamento adotti misure idonee a garantire che la volontà dell'interessato di revocare il proprio consenso venga effettivamente rispettata (cfr. provvedimento 30 maggio 2007, […] ).

Appare utile adottare sistemi di verifica della identità del contraente che si è registrato ad un sito web perché interessato a ricevere offerte promozionali. In tal senso, ad esempio, l'invio di una apposita e-mail al suo indirizzo di posta elettronica con la quale si chiede di confermare la propria identità cliccando su un apposito link.

2.7 L'eccezione del "soft spam" per l'invio di posta elettronica promozionale
L'Autorità ricorda che per le comunicazioni di cui all'art.130, commi 1 e 2, non valgono le cause di esonero del consenso di cui all'art.24 del Codice.

Per la sola posta elettronica, tuttavia, può ricorrere l'eccezione del c.d. "soft spam", di cui all'art.130, comma 4, in base al quale, se il titolare del trattamento utilizza, a fini di vendita diretta di propri prodotti o servizi, le coordinate di posta elettronica fornite dall'interessato nel contesto della
vendita di un prodotto o di un servizio, può non richiedere il consenso dell'interessato. Ciò, però, sempre che si tratti di servizi analoghi a quelli oggetto della vendita e che l'interessato, adeguatamente informato, non rifiuti tale uso.

[...]

5. Utilizzo di liste per l'invio di più e-mail o sms

La finalità promozionale talora viene perseguita utilizzando liste di e-mail o numerazioni telefoniche per l'invio simultaneo del medesimo messaggio promozionale a molteplici interessati.

I soggetti che si avvalgono di tale modalità per finalità di marketing devono rispettare principi e norme già sopra indicati nell'ambito del quadro normativo attualmente in vigore, con particolare riferimento agli artt.3, 11, 13, 23 e 130 del Codice per ciascuno degli indirizzi di posta trattato.

Peraltrò, nel caso dell'invio di e-mail, chi si avvale di liste di indirizzi talvolta lascia in chiaro gli indirizzi dei destinatari del messaggio promozionale, che quindi possono venire a conoscenza degli altri destinatari ed eventualmente utilizzare i loro indirizzi per i fini più vari, eventualmente anche alimentando ulteriore spam.

L’attività promozionale effettuata con mailing list in chiaro costituisce di fatto una comunicazione di dati personali (quelli relativi agli altri indirizzi di posta) a terzi, ossia ai molteplici destinatari della promozione.

Risulta necessario pertanto mantenere riservati, magari utilizzando la funzione "ccn" (ossia l'inoltro per conoscenza in "copia conoscenza nascosta"), gli indirizzi di posta utilizzati per l'invio della promozione.

6. Nuove forme di spam

Il Garante, sempre alla luce del descritto quadro normativo, di seguito intende fornire necessarie indicazioni di carattere generale anche in relazione ad alcune nuove forme e modalità di spam prive attualmente di un’espressa disciplina normativa, anche al fine di evitare che le grandi potenzialità di Internet, nonché più in generale della tecnologia, possano in via di fatto consentire un uso indiscriminato e illegittimo dei dati personali.

6.1 Il social spam

Il c.d. "social spam" consiste in un insieme di attività mediante le quali lo spammer veicola messaggi e link attraverso le reti sociali on-line. Ciò si inquadra nel problema dell'indiscriminato e spesso inconsapevole impiego dei propri dati personali da parte degli utenti nell'ambito dei social network, tanto più rispetto a profili di tipo "aperto". Questo impiega si presta alla commercializzazione o ad altri trattamenti dei dati personali a fini di profilazione e marketing da parte di società terze che siano partner commerciali delle società che gestiscono tali siti oppure che approfittino della disponibilità di fatto di tali dati in Internet. Inoltre, essendo i social network reti sociali tra persone reali, lo spam in questo caso può mirare a catturare l'elenco dei contatti dell'utente mirato per aumentare la portata virale del messaggio.

Al riguardo, l'Autorità anzitutto ricorda che l'agevole rintracciabilità di dati personali in Internet (quali numeri di telefono o indirizzi di posta elettronica) non autorizza a poter utilizzare tali dati per inviare comunicazioni promozionali automatizzate senza il consenso dei destinatari.

Riguardo a tale tipo di spam, si fa presente che i messaggi promozionali inviati agli utenti dei social network (come Facebook), in privato come pubblicamente sulla loro bacheca virtuale, sono sottoposti alla disciplina del Codice, e, in particolare, agli artt.3, 11, 13, 23 e 130.

La medesima disciplina è applicabile ai messaggi promozionali inviati utilizzando strumenti o servizi sempre più diffusi tipo Skype, WhatsApp, Viber, Messenger, etc.. Per questi, si ricorda il rischio di proliferazione dello spam dato che, come peraltro indicato nelle relative condizioni di servizio, tali strumenti talora comportano la condivisione indifferenziata di tutti i dati personali presenti negli smart-phone e nei tablet (quali rubrica, contatti, sms, dati della navigazione Internet) o l'accesso della società che li fornisce alla lista dei contatti o alla rubrica presente sul telefono mobile dell'utente per reperire e/o conservare tali dati personali.

Il rischio di ricevere spam, e in particolare il c.d. "spam mirato", basato sulla profilazione degli utenti, si potrebbe aggravare in considerazione della tendenza dei gestori delle piattaforme tecniche a policy privacy sempre più semplificate che, unificando i profili sui diversi servizi resi dalle medesime piattaforme, consentono di pervenire ad una conoscenza sempre più approfondita degli utenti, a cui indirizzare messaggi diversificati sulla base dei gusti rilevabili su molteplici applicazioni.

Se da una parte questa nuova pratica può agevolare il rapporto commerciale tra produttore e consumatore, riducendo per il primo i costi di marketing e per il secondo i costi di ricerca del
prodotto, tuttavia può causare all'interessato che viene profilato a dispetto della sua volontà, oltre alla ricezione dello spam, anche la compressione della sua libertà di fruizione dei servizi della società dell’informazione.

Ciò premesso, ferma restando la liceità dei messaggi a scopo meramente personale, si possono individuare alcune ipotesi sulle quali occorre fornire qualche chiarificazione anche sotto l'aspetto normativo.

Una prima ipotesi è quella in cui l'utente riceva, in privato, in bacheca o nel suo indirizzo di posta e-mail collegato al suo profilo social, un determinato messaggio promozionale relativo a uno specifico prodotto o servizio da un'impresa che abbia tratto i dati personali del destinatario dal profilo del social network al quale egli è iscritto.

Una seconda è quella in cui l'utente sia diventato "fan" della pagina di una determinata impresa o società oppure si sia iscritto a un "gruppo" di follower di un determinato marchio, personaggio, prodotto o servizio (decidendo così di "seguire" le relative vicende, novità o commenti) e successivamente riceva messaggi pubblicitari concernenti i suddetti elementi.

Nel primo caso, il trattamento sarà da considerarsi illecito, a meno che il mittente non dimostri di aver acquisito dall'interessato un consenso preventivo, specifico, libero e documentato ai sensi dell'art.130, commi 1 e 2, del Codice.

Nel secondo caso, l’invio di comunicazione promozionale riguardante un determinato marchio, prodotto o servizio, effettuato dall’impresa a cui fa riferimento la relativa pagina, può considerarsi lecito se dal contesto o dalle modalità di funzionamento del social network, anche sulla base delle informazioni fornite, può evincersi in modo inequivocabile che l'interessato abbia in tal modo voluto manifestare anche la volontà di fornire il proprio consenso alla ricezione di messaggi promozionali da parte di quella determinata impresa. Se invece l'interessato si cancella dal gruppo, oppure smette di "seguire" quel marchio o quel personaggio, o comunque si oppone ad eventuali ulteriori comunicazioni promozionali, il successivo invio di messaggi promozionali sarà illecito, con le relative conseguenze sanzionatorie. Ciò, ferma comunque restando la possibilità, talora fornita dai social network ai loro utenti, di bloccare l'invio di messaggi da parte di un determinato "contatto" o di segnalare quest'ultimo come spammer.

Nell’ipotesi dei “contatti” (i c.d. "amici") dell'utente, dei quali spesso nei social network o nelle comunità degli iscritti ai servizi di cui sopra, sono visualizzabili numeri di telefono o indirizzi di posta elettronica, l'impresa o società che intenda inviare legittimamente messaggi promozionali dovrà aver previamente acquisito, per ciascun "contatto" o "amico", un consenso specifico per l'attività promozionale.

6.2 “Marketing virale”

Il “marketing virale” è una modalità di attività promozionale mediante la quale un soggetto promotore sfrutta la capacità comunicativa di pochi soggetti destinatari diretti delle comunicazioni per trasmettere il messaggio ad un numero elevato di utenti finali. É un'evoluzione del "passaparola", ma se ne distingue per il fatto che fin dall'inizio emerge la volontà dei promotori di avviare una campagna promozionale. Come un "virus", la comunicazione contenente l’idea, il prodotto o il servizio, che può rivelarsi interessante o conveniente per un utente, viene veicolata da questo ad altri contatti, da questi ad altri e così via.

In genere, con la locuzione "marketing virale" si fa riferimento agli utenti di Internet che suggeriscono o raccomandano ad altri l'utilizzo di un determinato prodotto o servizio. Ultimamente, questa tecnica promozionale si sta diffondendo anche per prodotti non strettamente connessi a Internet: veicolo del messaggio resta comunque la comunità del web, che può comunicare in maniera chiara, veloce e gratuita.

Per agevolare la diffusione del messaggio, il soggetto promotore offre un incentivo o un bonus o altro bene economico ai destinatari delle comunicazioni che a loro volta, in cambio, si offrano di inoltrare o comunque far conoscere a terzi (talora con e-mail o sms) la comunicazione promozionale ricevuta.

Ebbene, tale attività, quando viene svolta con modalità automatizzate e per finalità di marketing, può rientrare nello spam se non rispetta principi e norme già sopra indicati nell’ambito del quadro normativo attualmente in vigore, con particolare riferimento agli artt.3, 11, 13, 23 e 130 del Codice.

Non è comunque soggetto al Codice il trattamento dei dati effettuato da chi, ricevendo una proposta promozionale, la inoltrò a sua volta a titolo personale, consigliando il prodotto o il servizio ai propri amici, utilizzando strumenti automatizzati. Il Codice si applica invece al trattamento
effettuato da chi inoltri, o comunque comunichi, il messaggio promozionale ricevuto a una molteplicità di destinatari i cui dati personali (numeri di telefono o indirizzi e-mail) siano stati reperiti su elenchi pubblici o sul web.

7. Le sanzioni
Si ricorda che, in relazione alle varie forme di spamming, in caso di accertata violazione delle norme del Codice, questa Autorità - fatta salva l'eventuale adozione di provvedimenti inibitori o prescrittivi - applica le sanzioni amministrative, quali in particolare quelle previste dagli artt.161 e 162, comma 2-bis del medesimo Codice, finalizzate ad assicurare l'osservanza dei fondamentali obblighi, rispettivamente, dell'informativa e del consenso.

Inoltre, qualora emergano i presupposti di un possibile trattamento illecito di dati personali avente una specifica rilevanza di natura penale, l'Autorità è tenuta a denunciare i fatti configurabili come reati perseguiti d'ufficio all'autorità giudiziaria per l'eventuale applicazione della sanzione penale prevista dall'art.167 del Codice.

*****

DISCUSSIONE

1. Cosa si intende per spam?
2. Le tutele di cui all'art.7 del d.lgs. n.196/2003 spettano sia a persone fisiche che giuridiche?
3. Un indirizzo aziendale del genere nome.cognome@società.it è da considerare quale indirizzo personale?
4. Quali elementi devono essere individuati nell'informativa di cui all'art.13 del d.lgs. n.196/2003?
5. Quale è la differenza tra un sistema di opt-in e un sistema di opt-out?
6. Quali sono i requisiti di validità del consenso per la finalità di invio di materiale pubblicitario?
7. Cosa si intende per “soft spam”?
8. Cosa si intende per “social spam”?
9. Cosa si intende per “marketing virale”?
7. PRIVACY E DIRITTO ALL’OBLIO
7.1. Diritto all’oblio in Rete

Garante per la protezione dei dati personali, provv. 10 novembre 2004

Reti telematiche e Internet - Motori di ricerca e provvedimenti di Autorità indipendenti: le misure necessarie a garantire il cd. "diritto all'oblio"

I ricorrenti affermano di non aver ricevuto idoneo riscontro ad un'istanza formulata all'autorità resistente (Autorità Garante della Concorrenza e del Mercato) ai sensi degli artt.7 e 8 del Codice, con la quale si erano opposti alla diffusione di dati personali che li riguardano (con specifico riferimento alle loro generalità o estremi identificativi) effettuata pubblicando sul sito Internet della medesima autorità due provvedimenti adottati dalla stessa nel 1996 e nel 2002 e che avevano vietato la diffusione di alcuni messaggi pubblicitari ritenuti ingannevoli ai sensi del d.lgs. 74/1992.

I ricorrenti lamentano che tale modalità di pubblicazione delle due decisioni che li riguardano arrecherebbe loro un ingiusto pregiudizio. Ciò, con riferimento alla possibilità che, ricercando il relativo nominativo tramite i motori di ricerca in Internet, le medesime decisioni compaiono costantemente a fianco delle informazioni relative all'attività svolta attualmente dal XT, facendo apparire le decisioni stesse "come attuali" rispetto ai messaggi pubblicitari che lo stesso diffonde oggi via Internet.

L'Autorità resistente ha fornito riscontro osservando che i propri provvedimenti sono pubblicati nel Bollettino dell'Autorità stessa "in ottemperanza ad un obbligo di legge, previsto dall'art.14, comma 1, del d.p.r. 11 luglio 2003, n.284", che impone il regime di pubblicità per i provvedimenti da essa deliberati.

Nel ricorso proposto ai sensi degli artt.145 e ss. del Codice, gli interessati hanno ribadito la propria opposizione, osservando di aver contestato non la liceità della pubblicazione dei provvedimenti in questione sul Bollettino dell'Autorità, quanto la loro diffusione in Internet senza l'adozione di opportune cautele (quali l'oscuramento dei nominativi, oppure la possibilità di consentire l'accesso ai provvedimenti solo mediante una ricerca all'interno del sito e inibendone invece la reperibilità mediante motori di ricerca). Tale modalità di diffusione, trasformandosi in pubblicazione "perpetua", diverrebbe, a loro avviso, "ben più grave di quella a mezzo stampa che pure costituisce una precisa sanzione accessoria, limitata però nel tempo". I ricorrenti hanno chiesto di porre a carico di controparte le spese sostenute per il procedimento.

A seguito dell'invito ad aderire formulato da questa Autorità in data 20 settembre 2004 ai sensi dell'art.149 del Codice, l'Autorità garante della concorrenza e del mercato ha nuovamente risposto con memoria dell'11 ottobre e nell'audizione del 12 ottobre 2004, dichiarando che:
- "l'Autorità diffonde i dati personali contenuti nei provvedimenti da essa adottati in materia di pubblicità ingannevole e comparativa sulla base di specifica previsione normativa: l'art.14 del d.p.r. 284/2003, già art.16 del d.p.r. 627/1996, il quale dispone che il provvedimento finale è "pubblicato, entro venti giorni dalla sua adozione, nel bollettino di cui all'art.26 della legge 10 ottobre 1990, n.287"
- "lo scopo della norma è, evidentemente, quello di assicurare adeguata pubblicità e conoscenza dell'attività svolta dall'Autorità" e che, "stante il suddetto principio di pubblicità, l'Autorità ha sempre dato ampio diffusione alla propria attività istituzionale, avvalendosi anche degli strumenti informatici mediante la pubblicazione del Bollettino sul proprio sito Internet, quale mezzo di comunicazione di grande utilità ed ormai di uso comune ampiamente utilizzato anche dalle pubbliche amministrazioni per assicurare la più ampia e tempestiva conoscibilità dell'azione amministrativa";
- anche il Garante per la protezione dei dati personali, in un parere reso al Dipartimento per gli affari giuridici e legislativi della Presidenza del Consiglio dei ministri nel 1999, osservava che "l'indicazione delle parti interessate nelle decisioni dell'Autorità pubblicate è "in termini generali giustificata e rispettosa del principio di pertinenza" di cui all'art.9 della legge 675/1996" (ora, art.11 del Codice);
- "l'interesse pubblico alla piena conoscibilità delle decisioni dell'Autorità deve ritenersi senz'altro prevalente sull'interesse dell'operatore pubblicitario a non far conoscere al pubblico dei consumatori di essere stato destinatario di un provvedimento dell'Autorità";
- "l'identità personale dell'operatore pubblicitario non è un dato che possa essere sottratto all'obbligo di pubblicazione in quanto la sua omissione finirebbe in sostanza per frustrare il fine stesso della normativa in materia di pubblicità ingannevole soprattutto quando, come nel caso di specie, in mancanza di tale dato non sarebbe possibile identificare il messaggio pubblicitario";
- "attualmente, vengono pubblicati sul sito dell'Autorità tutti i provvedimenti in formato html, nonché la versione del Bollettino in formato pdf" e non viene utilizzato "alcun accorgimento di carattere tecnico idoneo a facilitare la ricerca effettuata dai vari motori di ricerca";
- l'Autorità non si oppone a che, con l'ausilio del Garante per la protezione dei dati personali, possano essere individuate possibili soluzioni tecniche che "da un lato consentano la piena conoscibilità delle decisioni dell'Autorità, stante il regime di pubblicazione normativamente previsto, dall'altro siano idonee ad evitare episodi, sia pure occasionali, come quello che ha dato luogo alla presente controversia".

Con memorie del 10 ottobre e dell'11 ottobre 2004, i ricorrenti hanno ribadito la propria opposizione, rilevando che la pubblicazione delle pronunce in questione, pur connessa a messaggi pubblicitari non più divulgati, assumerebbe "un carattere di eternità, non essendo soggetta a limiti temporali".

ciò premesso il Garante osserva:

Il ricorso concerne un'opposizione per motivi legittimi al trattamento di dati personali da parte di un'autorità indipendente, con riferimento alle modalità di diffusione, via Internet, dei dati personali dei ricorrenti contenuti in alcune decisioni adottate dall'Autorità stessa.

Il trattamento dei dati personali in questione va esaminato alla luce dell'art.19 del Codice, in base al quale la diffusione di dati personali da parte di un soggetto pubblico è consentita solo quando è prevista da una norma di legge o di regolamento.

Le decisioni dell'Autorità garante della concorrenza e del mercato devono essere pubblicate, a norma dell'art.26 della legge 287/1990, "in un apposito bollettino, a cura della Presidenza del Consiglio dei Ministri" e tale obbligo è ribadito, con specifico riferimento ai provvedimenti adottati dall'Autorità in materia di pubblicità ingannevole e comparativa, dall'art.14 del d.p.r. 284/2003.

Nel caso di specie, non è contestata la pubblicazione degli estremi identificativi dei ricorrenti nei provvedimenti adottati dall'Autorità resistente – la cui omissione, come argumentato da quest'ultima, non sarebbe stata peraltro possibile senza vanificare il fine specifico della pubblicazione del provvedimento relativo alla pubblicità ingannevole – bensì la modalità di conoscibilità in Internet delle decisioni medesime, tenuto anche conto che le stesse fanno riferimento a messaggi pubblicitari attualmente non più diffusi dai ricorrenti e che questi ultimi diffondono attualmente on-line altri messaggi pubblicitari ritenuti rispettosi della vigente normativa.

Le richiamate previsioni normative relative alla pubblicazione delle decisioni dell'Autorità garante della concorrenza e del mercato rendono in generale lecita la correlativa diffusione dei dati personali nelle stesse contenuti, e non pongono limiti specifici alle modalità attraverso le quali le decisioni pubblicate sul Bollettino dell'Autorità possano essere oggetto di diffusione contestuale o successiva.

Peraltrò, le modalità di funzionamento della rete Internet consentono, in particolar modo attraverso l'utilizzo di motori di ricerca, di rinvenire un consistente numero di informazioni, riferite a soggetti individuati, più o meno aggiornate e di natura differente.

La questione sollevata dai ricorrenti è di particolare interesse e delicatezza coinvolgendo il dovere di informazione da parte di organi pubblici sulla propria attività, i diritti di utenti e consumatori, ma anche quelli dei soggetti cui si riferiscono i dati diffusi, in particolare del diritto all'oblio una volta che siano state perseguite le finalità alla base del trattamento dei dati (art.11 del Codice).

Decorsi determinati periodi, la diffusione istantanea e cumulativa su siti web di un gran numero di dati personali relativi ad una pluralità di situazioni riferite ad un medesimo interessato può comportare un sacrificio sproporzionato dei suoi diritti e legittimi interessi quando si tratta di provvedimenti risalenti nel tempo e che hanno raggiunto le finalità perseguite.

Varie disposizioni, anche recenti, dell'ordinamento relative alla conoscibilità, ad esempio, dei dati giudiziari e di quelli relativi alle informazioni a contenuto economico-commerciale sono volte a individuare un equilibrio ragionevole tra i vari diritti e interessi coinvolti.

Il Codice in materia di protezione dei dati personali prevede ad esempio che le decisioni e le sentenze dell'autorità giudiziaria possano essere rese accessibili anche attraverso Internet, ma nel rispetto di alcune specifiche cautele (art.51, comma 2, del Codice), tra cui figura la possibilità per
l'interessato di chiedere per motivi legittimi che sia apposta sull'originale del provvedimento un'annotazione volta a precludere la diffusione delle generalità e dei dati identificativi riportati nelle decisioni medesime (art.52, comma 4).

Tale cautela non opera, allo stato, per decisioni di autorità amministrative.

I ricorrenti prefigurano in particolare la possibilità, per l'Autorità garante della concorrenza e del mercato, di scegliere selettivamente, mediante operatori logici, quali parti dei propri documenti possano essere rilevate dai motori di ricerca e proposte, come risultato, a chi faccia uso in Internet di specifiche stringhe di ricerca utilizzando in modo opportuno i suddetti operatori logici booleani (And, Or, Not).

Ciò non riflette, però, il reale funzionamento dei motori di ricerca standard, intendenendo con ciò quelli a maggiore diffusione, la cui azione nella fase di raccolta delle informazioni sulle pagine disponibili nel world wide web (fase di grabbing e di successiva indicizzazione) è influenzabile dal singolo amministratore di un sito web soltanto tramite la compilazione del file robots.txt, previsto dal "Robots Exclusion Protocol", o tramite l'uso del "Robots Meta tag". Si tratta di convenzioni concordate nella comunità Internet dai soggetti che sviluppano i protocolli, e non di standard veri e propri, allo stato largamente accettate nel contesto dei motori di ricerca.

Tali convenzioni prevedono la possibilità per il gestore di un sito web di escludere selettivamente alcuni contenuti dall'azione di uno o più motori di ricerca. Oggetto dell'esclusione o della limitazione di accesso resta, però, sempre la pagina web o l'insieme di pagine web o di link in essa contenuti, anziché singole parole chiave o specifiche clausole di ricerca composte con operatori logici. Ciò, avviene sia con il "Robots Exclusion Protocol", sia con il ricorso ai Robots Meta tag da inserire nel codice delle pagine da visualizzare.

Un'azione su singole parole chiave è possibile, ma soltanto "in positivo", ovvero è possibile per l'amministratore del sito promuovere pagine web inserendo, con opportuni comandi, alcune keywords che possono anche non corrispondere a parole presenti nel documento pubblicato. Tale meccanismo, come richiamato dall'Autorità resistente nella memoria difensiva, non è mai stato utilizzato sul sito dell'Autorità stessa per evidenziare documenti in relazione all'identità delle parti.

Alla luce di quanto sopra considerato, non risulta allo stato tecnicamente praticabile la soluzione volta a far sì che i nominativi degli interessati contenuti nelle decisioni pubblicate sul sito siano rilevabili da motori di ricerca solo mediante l'associazione di più parole chiave che uniscano il nominativo dei ricorrenti alla materia trattati nei provvedimenti.

Tuttavia, la diretta individuabilità in Internet, tramite motori di ricerca esterni, della decisione adottata dalla resistente nel 1996, non risulta più giustificata in rapporto alle finalità perseguite nel caso di specie.

In applicazione del principio di cui all'art.11, comma 1, lett.e), del Codice, l'Autorità resistente potrà continuare a pubblicare i propri provvedimenti sul relativo sito web modulando, però, nel tempo il periodo entro il quale le decisioni riguardanti i ricorrenti saranno direttamente individuabili in Internet tramite comuni motori di ricerca esterni.

A tal fine, ai sensi dell'art.150, comma 2, del Codice, vengono indicate in questa sede due misure necessarie a tutela dei diritti degli interessati.

Entro tre mesi dalla data di ricezione del presente provvedimento l'Autorità resistente istituirà, nell'ambito del proprio sito web, una sezione (nella quale collocare la predetta decisione del 1996) liberamente consultabile telematicamente accedendo allo stesso indirizzo web, ma tecnicamente sottratta alla diretta individuabilità delle decisioni in essa contenute per il tramite dei comuni motori di ricerca esterni.

Entro lo stesso termine dei tre mesi, l'Autorità individuerà, altresì, il periodo temporale entro il quale si potrà ritenere proporzionato, in rapporto alle finalità perseguite, mantenere sul sito provvedimenti (come, allo stato, quello del 2002 relativo ai ricorrenti) direttamente individuabili anche tramite motori di ricerca esterni.

[...]

per questi motivi il Garante:

a) dichiara parzialmente fondato il ricorso e, per l'effetto, prescrive all'autorità resistente di conformare le modalità di diffusione telematica dei dati personali relativi ai ricorrenti nei termini di cui in motivazione;

[...]

****
DISCUSSIONE

1. Come la pubblicazione in Internet, oltre che sul Bollettino cartaceo dell’AGCM, influisce sulle problematiche relative a riservatezza ed oblio?

2. Il Garante ha scelto di intervenire sulla “individuabilità” delle decisioni dell’AGCM in Internet. Quali erano le alternative?

3. Il Garante avrebbe potuto chiedere ai motori di ricerca, nazionali e internazionali, di intervenire per evitare l’individuabilità o per avere la cancellazione di tali risultati?

*****

NORME

- art.26, legge n.287/1990
- art.14, d.p.r. n.284/2003
- artt.11, 18, comma 2, 19, comma 3, 25, d.lgs. n.196/2003
7.2. Diritto all’oblio e responsabilità del motore di ricerca

Corte di Giustizia dell’Unione Europea, 13 maggio 2014 (causa C-131/12)

[...]  
1. La domanda di pronuncia pregiudiziale verte sull’interpretazione degli artt.2, lett.b) e d), 4, §1, lett.a) e c), 12, lett.b), e 14, comma 1, lett.a), della direttiva 95/46/CE [...] del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati ([...]), nonché dell’art.8 della Carta dei diritti fondamentali dell’Unione Europea (in prosieguo: la «Carta»).  
[...]

Procedimento principale e questioni pregiudiziali  
15. Mediante detto reclamo, il sig. Costeja González chiedeva, da un lato, che fosse ordinato a La Vanguardia di sopprimere o modificare le pagine suddette affinché i suoi dati personali non vi comparissero più, oppure di ricorrere a taluni strumenti forniti dai motori di ricerca per proteggere tali dati. Dall’altro lato, egli chiedeva che fosse ordinato a Google Spain o a Google Inc. di eliminare o di occultare i suoi dati personali, in modo che cessassero di comparire tra i risultati di ricerca e non figurassero più nei link di La Vanguardia. Il sig. Costeja González affermava in tale contesto che il pignoramento, che era stato effettuato nei suoi confronti, era stato interamente definito da svariati anni e che la menzione dello stesso era ormai priva di qualsiasi rilevanza.  
16. Con decisione del 30 luglio 2010, l’AEPD ha respinto il suddetto reclamo nella parte in cui era diretto contro La Vanguardia, ritenendo che la pubblicazione da parte di quest’ultima delle informazioni in questione fosse legalmente giustificata, dato che aveva avuto luogo su ordine del Ministero del Lavoro e degli Affari sociali e aveva avuto lo scopo di conferire il massimo di pubblicità alla vendita pubblica, al fine di raccogliere il maggior numero di partecipanti all’asta.  
17. Detto reclamo è stato invece accolto nella parte in cui era diretto contro Google Spain e Google Inc.. L’AEPD ha considerato in proposito che i gestori di motori di ricerca sono assoggettati alla normativa in materia di protezione dei dati, dato che essi effettuano un trattamento di dati per il quale sono responsabili e agiscono quali intermediari della società dell’informazione. L’AEPD ha ritenuto di essere autorizzata ad ordinare la rimozione dei dati nonché il divieto di accesso a taluni dati da parte dei gestori di motori di ricerca, qualora essa ritenga che la localizzazione e la diffusione degli stessi possano ledere il diritto fondamentale alla protezione dei dati e la dignità delle persone in senso ampio, ciò che includerebbe anche la semplice volontà della persona interessata che tali dati non siano conosciuti da terzi. L’AEPD ha affermato che tale obbligo può incombere direttamente ai gestori di motori di ricerca, senza che sia necessario cancellare i dati o le informazioni dal sito web in cui questi compaiono, segnatamente quando il mantenimento di tali informazioni nel sito in questione sia giustificato da una norma di legge.  
18. Google Spain e Google Inc. hanno proposto due ricorsi separati contro la decisione di cui sopra dinanzi all’Audiencia Nacional, dei quali quest’ultima ha disposto la riunione.
19. Detto giudice chiarisce nella decisione di rinvio che i ricorsi sopra menzionati portano a chiedersi quali obblighi incombano ai gestori di motori di ricerca per la tutela dei dati personali delle persone interessate, le quali non desiderino che alcune informazioni, pubblicate sui siti web di terzi e contenenti loro dati personali che consentono di collegare ad esse dette informazioni, vengano localizzate, indicizzate e messe a disposizione degli utenti di Internet in modo indefinito. La risposta a tale quesito dipenderebbe dal modo in cui la direttiva 95/46/CE deve essere interpretata nel contesto di queste tecnologie che sono apparse dopo la sua pubblicazione.

20. Alla luce di tali considerazioni, l’Audiencia Nacional ha deciso di sospendere il procedimento e di sottoporre alla Corte le seguenti questioni pregiudiziali:

«1) Per quanto concerne l’ambito territoriale di applicazione della direttiva [95/46/CE] e, di conseguenza, della normativa spagnola sulla protezione dei dati, si chiede:

a) Se debba ritenersi che esista uno “stabilimento” ai sensi dell’art. 4, §1, lett.a), della direttiva [95/46/CE], qualora ricorrano una o più delle seguenti circostanze:
– l’impresa che gestisce il motore di ricerca apre in uno Stato membro una succursale o una filiale destinata alla promozione e alla vendita degli spazi pubblicitari proposti dal motore di ricerca e l’attività della quale si dirige agli abitanti di tale Stato;
– la società madre designa una filiale situata in tale Stato membro come suo rappresentante e responsabile del trattamento di due file specifici contenenti i dati dei clienti che hanno stipulato contratti con detta società per la fornitura di servizi pubblicitari;
– la succursale o la filiale stabilita in uno Stato membro trasmette alla società madre, avente sede al di fuori dell’Unione Europea, i reclami e le ingiunzioni che le vengono presentati tanto dalle persone interessate quanto dalle autorità competenti perché sia rispettato il diritto alla protezione dei dati, anche quando tale collaborazione abbia carattere volontario.

b) Se l’art. 4, §1, lett.c), della direttiva 95/46/CE debba essere interpretato nel senso che si configura un “ricorso a strumenti situati nel territorio di detto Stato membro” qualora un motore di ricerca:
– utilizzi dei “web spiders” o dei crawler per localizzare e indicizzare le informazioni contenute in pagine web alloggiate su server situati in tale Stato membro
– utilizzi un nome di dominio proprio di uno Stato membro e indirizzi le ricerche e i risultati in funzione della lingua di tale Stato membro.

c) Se possa considerarsi come un ricorso a strumenti, ai sensi dell’art. 4, §1, lett.c), della direttiva [95/46/CE], la memorizzazione temporanea delle informazioni indicizzate dai motori di ricerca su Internet. In caso di risposta affermativa a quest’ultimo quesito, se si possa ritenere soddisfatto tale criterio di collegamento quando l’impresa si rifiuti di rivelare il luogo in cui archivia detti indici, adducendo ragioni di concorrenza.

d) A prescindere dalla risposta ai precedenti quesiti, e specialmente nel caso in cui la Corte ritenesse inapplicabili i criteri di collegamento previsti dall’art. 4 della direttiva [95/46/CE]:
Se, alla luce dell’art. 8 della [Carta], la direttiva [95/46/CE] debba essere applicata nello Stato membro nel quale si trova il centro di gravità del conflitto e nel quale è possibile ottenere una tutela più efficace dei diritti dei cittadini dell’Unione (...).

2) Per quanto concerne l’attività dei motori di ricerca quali fornitori di contenuti in relazione alla direttiva [95/46/CE], si chiede:

a) Riguardo all’attività di Google Search quale fornitore di contenuti, consistente nel localizzare le informazioni pubblicate o messe in rete da terzi, nell’indicizzarle in maniera automatica, nel memorizzarle temporaneamente e infine nel metterle a disposizione degli utenti di Internet secondo un determinato ordine di preferenza, qualora tali informazioni contengano dati personali di terzi:
Se un’attività come quella descritta debba considerarsi rientrante nella nozione di “trattamento di dati” ai sensi dell’art. 2, lett.b), della direttiva 95/46/CE.

b) In caso di risposta affermativa al quesito precedente, e sempre con riferimento ad un’attività come quella sopra descritta:
c) In caso di risposta affermativa al quesito precedente:

Se l'AEPD, al fine di tutelare i diritti enunciati agli artt.12, lett.b), e 14, [comma 1] lett.a), della direttiva [95/46/CE], possa ordinare direttamente [a Google Search] di rimuovere dai propri indici un'informazione pubblicata da terzi, senza rivolgersi previamente o simultaneamente al titolare della pagina web in cui è inserita tale informazione.

d) In caso di risposta affermativa al quesito precedente:

Se i motori di ricerca siano sollevati dall'obbligo di rispettare i diritti di cui sopra qualora l'informazione contenente i dati personali sia stata legittimamente pubblicata da terzi e rimanga sulla pagina web di origine.

3) Per quanto concerne la portata del diritto di cancellazione e/o opposizione al trattamento di dati in relazione al diritto all'oblio, si chiede:

Se si debba ritenere che i diritti di cancellazione e congelamento dei dati, disciplinati dall'art.12, lett.b), e il diritto di opposizione al loro trattamento, regolato dall'art.14, [comma 1] lett.a), della direttiva [95/46/CE], implichi che l'interessato può rivolgersi ai motori di ricerca per impedire l'indicizzazione delle informazioni riguardanti la sua persona pubblicate su pagine web di terzi, facendo valere la propria volontà che tali informazioni non siano conosciute dagli utenti di Internet, ove egli reputi che la loro divulgazione possa arrecargli pregiudizio o desideri che tali informazioni siano dimenticate, anche quando si tratti di informazioni pubblicate da terzi legittimamente».

Sulle questioni pregiudiziali

Sulla seconda questione, lett.a) e b), concernente l'ambito di applicazione materiale della direttiva 95/46/CE

21. Con la sua seconda questione, lett.a) e b), da esaminarsi per prima, il giudice del rinvio chiede, in sostanza, se l'art.2, lett.b), della direttiva 95/46/CE debba essere interpretato nel senso che l'attività di un motore di ricerca quale fornitore di contenuti, consistente nel trovare in Internet, ove egli reputi che la loro divulgazione possa arrecargli pregiudizio o desideri che tali informazioni siano dimenticate, anche quando si tratti di informazioni pubblicate da terzi legittimamente».

25. A questo proposito occorre rilevare come l'art.2, lett.b), della direttiva 95/46/CE definisca il «trattamento di dati personali» come «qualsiasi operazione o insieme di operazioni compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali, come la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione o la modifica, l'estrazione, la consultazione, l'impiego, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, nonché il congelamento, la cancellazione o la distruzione».

26. Per quanto riguarda in particolare Internet, la Corte ha già avuto modo di constatare che l'operazione consistente nel far comparire su una pagina Internet dati personali va considerata come un «trattamento» siffatto ai sensi dell'art.2, lett.b), della direttiva 95/46/CE (v. sentenza Lindqvist, C-101/01, […] p.to 25).

27. Per quanto concerne l'attività in esame nel procedimento principale, non è contestato che tra i dati trovati, indicizzati, memorizzati dai motori di ricerca e messi a disposizione degli utilizzatori di questi ultimi sono presenti anche informazioni riguardanti persone fisiche identificate o identificabili, e dunque «dati personali» ai sensi dell'art.2, lett.a), della direttiva citata.

28. Pertanto, occorre constatare che, esplorando Internet in modo automatizzato, costante e sistematico alla ricerca delle informazioni ivi pubblicate, il gestore di un motore di ricerca «raccoglie» dati siffatti, che egli «estrae», «registra» e «organizza» successivamente nell'ambito dei suoi programmi di indicizzazione, «conserva» nei suoi server e, eventualmente, «comunica» e «mette a disposizione» dei propri utenti sotto forma di elenchi dei risultati delle loro ricerche. Poiché tali operazioni sono contemplate in maniera esplicita e incondizionata all'art.2, lett.b), della direttiva 95/46/CE, esse devono essere qualificate come «trattamento» ai sensi di tale disposizione, senza che rilevi il fatto che il gestore del motore di ricerca applichi le medesime operazioni anche ad altri tipi di informazioni e non distingua tra queste e i dati personali.
29. La constatazione di cui sopra non viene invalidata neppure dal fatto che tali dati abbiano già costituito l’oggetto di una pubblicazione su Internet e non vengano modificati dal suddetto motore di ricerca.

30. Infatti, la Corte ha già constatato che le operazioni contemplate dall’art.2, lett.b), della direttiva 95/46/CE devono essere considerate come un trattamento siffatto anche nell’ipotesi in cui riguardino esclusivamente informazioni già pubblicate tali e quali nei media. La Corte ha infatti rilevato, a questo proposito, che una deroga generale all’applicazione della direttiva 95/46/CE in un’ipotesi siffatta priverebbe in larga parte del suo significato tale direttiva (v., in tal senso, sentenza Satakunnan Markkinapörssi e Satamedia, C-73/07, […], p.ti 48 e 49).

31. Inoltre, discende dalla definizione contenuta nell’art.2, lett.b), della direttiva 95/46/CE che, se indubbiamente la modificazione di dati personali costituisce un trattamento ai sensi della direttiva stessa, le altre operazioni menzionate in tale disposizione non esigono affatto, invece, che i dati suddetti vengano modificati.

32. Quanto alla questione se il gestore di un motore di ricerca debba o no essere considerato come il «responsabile del trattamento» dei dati personali effettuato da tale motore nell’ambito di un’attività come quella oggetto del procedimento principale, occorre ricordare che l’art.2, lett.d), della direttiva 95/46/CE definisce detto responsabile come «la persona fisica o giuridica, l’autorità pubblica, il servizio o qualsiasi altro organismo che, da solo o insieme ad altri, determina le finalità e gli strumenti del trattamento di dati personali».

33. Orbene, è il gestore del motore di ricerca a determinare le finalità e gli strumenti di tale attività e dunque del trattamento di dati personali che egli stesso effettua nell’ambito dell’attività medesima, ed è di conseguenza lui a dover essere considerato come il «responsabile» di tale trattamento a norma del citato art.2, lett.d).

34. Inoltre, occorre constatare che sarebbe contrario non soltanto al chiaro tenore letterale di tale disposizione, ma anche alla sua finalità — consistente nel garantire, mediante un’ampia definizione della nozione di «responsabile», una tutela efficace e completa delle persone interessate — il fatto di escludere dalla nozione di cui sopra il gestore di un motore di ricerca per il motivo che egli non esercita alcun controllo sui dati personali pubblicati sulle pagine web di terzi.

35. A questo proposito, occorre sottolineare che il trattamento di dati personali effettuato nell’ambito dell’attività di un motore di ricerca si distingue da e si aggiunge a quello effettuato dagli editori di siti web, consistente nel far apparire tali dati su una pagina Internet.

36. Inoltre, è pacifico che tale attività dei motori di ricerca svolge un ruolo decisivo nella diffusione globale dei dati suddetti, in quanto rende accessibili questi ultimi a qualsiasi utente di Internet che effetti una ricerca a partire dal nome della persona interessata, anche a quegli utenti che non avrebbero altrimenti trovato la pagina web su cui questi stessi dati sono pubblicati.

37. Per di più, l’organizzazione e l’aggregazione delle informazioni pubblicate su Internet, realizzate dai motori di ricerca allo scopo di facilitare ai loro utenti l’accesso a dette informazioni, possono avere come effetto che tali utenti, quando la loro ricerca viene effettuata a partire dal nome di una persona fisica, ottengono attraverso l’elenco di risultati una visione complessiva strutturata delle informazioni relative a questa persona reperibili su Internet, che consente loro di stabilire un profilo più o meno dettagliato di quest’ultima.

38. Pertanto, nella misura in cui l’attività di un motore di ricerca può incidere, in modo significativo e in aggiunta all’attività degli editori di siti web, sui diritti fondamentali alla vita privata e alla protezione dei dati personali, il gestore di tale motore di ricerca quale soggetto che determina le finalità e gli strumenti di questa attività deve assicurare, nell’ambito delle sue responsabilità, delle sue competenze e delle sue possibilità, che detta attività soddisfi le prescrizioni della direttiva 95/46/CE, affinché le garanzie previste da quest’ultima possano svilupparsi pienamente i loro effetti e possa essere effettivamente realizzata una tutela efficace e completa delle persone interessate, in particolare del loro diritto al rispetto della loro vita privata.

39. Infine, la circostanza che gli editori di siti web abbiano la facoltà di indicare ai gestori di motori di ricerca, con l’aiuto segnatamente di protocolli di esclusione come «robot.txt» o di codici come «noindex» o «noarchive», il loro desiderio che una determinata informazione, pubblicata sul loro sito, venga esclusa in tutto o in parte dagli indici automatici dei motori di ricerca, non significa che la mancanza di un’indicazione siffatta da parte di questi editori liberi il gestore di un motore di ricerca dalla sua responsabilità per il trattamento dei dati personali che egli effettua nell’ambito dell’attività del motore stesso.
40. Infatti, tale circostanza non modifica il fatto che le finalità e gli strumenti del citato trattamento sono determinati da detto gestore. Inoltre, anche supponendo che la summenzionata facoltà degli editori di siti web significhi che costoro determinano insieme con il suddetto gestore gli strumenti di tale trattamento, tale circostanza nulla toglierrebbe alla responsabilità di quest’ultimo, dato che l’art.2, lett.d), della direttiva 95/46/CE prevede espressamente che tale determinazione possa essere effettuata «da solo o insieme ad altri».

41. Alla luce di quanto sopra esposto, occorre rispondere alla seconda questione, lett.a) e b), dichiarando che l’art.2, lett.b) e d), della direttiva 95/46/CE deve essere interpretato nel senso che, da un lato, l’attività di un motore di ricerca consistente nel trovare informazioni pubblicate o inserite da terzi su Internet, nell’indicizzarle in modo automatico, nel memorizzarle temporaneamente e, infine, nel metterle a disposizione degli utenti di Internet secondo un determinato ordine di preferenza, deve essere qualificata come «trattamento di dati personali», ai sensi del citato art.2, lett.b), qualora tali informazioni contengano dati personali, e che, dall’altro lato, il gestore di detto motore di ricerca deve essere considerato come il «responsabile» del trattamento summenzionato, ai sensi dell’art.2, lett.d), di cui sopra.

Sulla prima questione, lettere da a) a d), concernente l’ambito di applicazione territoriale della direttiva 95/46/CE

42. Con la sua prima questione, lettere da a) a d), il giudice del rinvio mira a stabilire se sia possibile applicare la normativa nazionale di recepimento della direttiva 95/46/CE in circostanze quali quelle in esame nel procedimento principale.

43. In tale contesto, il giudice del rinvio ha accertato i seguenti fatti:


– Google Search è gestito da Google Inc., che è la società madre del gruppo Google e la cui sede sociale si trova negli Stati Uniti.

– Google Search indica i siti web del mondo intero, e tra questi i siti ubicati in Spagna. Le informazioni indicizzate dai suoi «web spiders» o dai suoi crawler, ossia programmi informatici utilizzati per reperire e scavare il contenuto delle pagine web in modo metodico e automatizzato, vengono memorizzate temporaneamente in server dei quali si ignora lo Stato di ubicazione, informazione questa che viene mantenuta segreta per ragioni di concorrenza.

– Google Search non si limita a dare accesso ai contenuti ospitati sui siti web indicizzati, ma sfrutta tale attività per includere, dietro pagamento, pubblicità ass.


– Google Inc. ha designato Google Spain come responsabile del trattamento, in Spagna, di due file registrati da Google Inc. presso l’AEPD, tenendo presente che tali file hanno lo scopo di contenere i dati personali dei clienti che hanno concluso contratti di servizi pubblicitari con Google Inc..

44. In concreto, il giudice del rinvio si interroga, in via principale, in merito alla nozione di «stabilimento», ai sensi dell’art.4, §1, lett.a), della direttiva 95/46/CE, e a quella di «ricorso a strumenti situati nel territorio di detto Stato membro», ai sensi dell’art.4, §1, lett.c), della medesima direttiva.

Sulla prima questione, lett.a)

45. Con la sua prima questione, lett.a), il giudice del rinvio chiede, in sostanza, se l’art.4, §1, lett.a), della direttiva 95/46/CE debba essere interpretato nel senso che un trattamento di dati personali viene effettuato nel contesto delle attività di uno stabilimento del responsabile di tale trattamento nel territorio di uno Stato membro, ai sensi della disposizione di cui sopra, qualora una o più delle seguenti tre condizioni siano soddisfatte:
– il gestore di un motore di ricerca apre in uno Stato membro una succursale o una filiale destinata alla promozione e alla vendita degli spazi pubblicitari proposti dal motore di ricerca e l’attività della quale si dirige agli abitanti di tale Stato, oppure
– la società madre designa una filiale situata in tale Stato membro come suo rappresentante e responsabile del trattamento di due file specifici contenenti i dati dei clienti che hanno stipulato contratti con detta società per la fornitura di servizi pubblicitari, oppure
– la succursale o la filiale stabilita in uno Stato membro trasmette alla società madre, avente sede al di fuori dell’Unione, i reclami e le ingiunzioni che le vengono presentati tanto dalle persone interessate quanto dalle autorità competenti perché sia rispettato il diritto alla protezione dei dati personali, anche quando tale collaborazione abbia carattere volontario.

46. Per quanto riguarda la prima di queste tre condizioni, il giudice del rinvio rileva che Google Search è gestito e amministrato da Google Inc., e che non è dimostrato che Google Spain realizzati in Spagna un’attività direttamente connessa all’indicizzazione o alla memorizzazione di informazioni o di dati contenuti nei siti web di terzi. Tuttavia, l’attività di promozione e di vendita degli spazi pubblicitari, di cui si occupa Google Spain per la Spagna, costituirrebbe la parte essenziale dell’attività commerciale del gruppo Google e potrebbe essere considerata come strettamente connessa a Google Search.

[...] 48. A questo proposito occorre anzitutto rilevare che il considerando 19 della direttiva 95/46/CE precisa che «lo stabilimento nel territorio di uno Stato membro implica l’esercizio effettivo e reale dell’attività mediante un’organizzazione stabile», e «che la forma giuridica di siffatto stabilimento, si tratti di una semplice succursale o di una filiale dotata di personalità giuridica, non è il fattore determinante a questo riguardo».

49. Orbene, non è contestato che Google Spain si dedica all’esercizio effettivo e reale di un’attività mediante un’organizzazione stabile in Spagna. Essendo inoltre dotata di una personalità giuridica propria, detta società costituisce in tal modo una filiale di Google Inc. nel territorio spagnolo e, di conseguenza, uno «stabilimento» ai sensi dell’art.4, §1, lett.a), della direttiva 95/46/CE.

50. Al fine di soddisfare il criterio fissato da questa disposizione, è altresì necessario che il trattamento di dati personali ad opera del responsabile dello stesso venga «effettuato nel contesto delle attività» di uno stabilimento di questo responsabile nel territorio di uno Stato membro.

[...] 54. In tali circostanze, occorre rilevare che risulta in particolare dai considerando da 18 a 20 e dall’art.4 della direttiva 95/46/CE che il legislatore dell’Unione ha inteso evitare che una persona venga esclusa dalla protezione garantita da tale direttiva e che tale protezione venga elusa, prevedendo a tal fine un ambito di applicazione territoriale particolarmente esteso.

55. Tenuto conto di tale obiettivo della direttiva 95/46/CE e del tenore letterale del suo art.4, §1, lett.a), occorre affermare che il trattamento di dati personali realizzato per le esigenze di servizio di un motore di ricerca come Google Search, il quale venga gestito da un’impresa con sede in uno Stato terzo ma avente uno stabilimento in uno Stato membro, viene effettuato «nel contesto delle attività» di tale stabilimento qualora quest’ultimo sia destinato a garantire, in tale Stato membro, la promozione e la vendita degli spazi pubblicitari proposti dal suddetto motore di ricerca, che servono a rendere redditizio il servizio offerto da quest’ultimo.

56. Infatti, in circostanze del genere, le attività del gestore del motore di ricerca e quelle del suo stabilimento situato nello Stato membro interessato sono inscindibilmente connesse, dal momento che le attività relative agli spazi pubblicitari costituiscono il mezzo per rendere il motore di ricerca in questione economicamente redditizio e che tale motore è, al tempo stesso, lo strumento che consente lo svolgimento di dette attività.

57. A questo proposito occorre ricordare che, come si è precisato ai p.ti da 26 a 28 della presente sentenza, la visualizzazione stessa di dati personali su una pagina di risultati di una ricerca costituisce un trattamento di dati personali. Orbene, poiché la suddetta visualizzazione di risultati è accompagnata, sulla stessa pagina, da quella di pubblicità correlate ai termini di ricerca, è giocoferza constatare che il trattamento di dati personali in questione viene effettuato nel contesto dell’attività pubblicitaria e commerciale dello stabilimento del responsabile del trattamento nel territorio di uno Stato membro, nella fattispecie il territorio spagnolo.

58. Date tali circostanze, non si può accettare che il trattamento di dati personali effettuato per le esigenze del funzionamento del suddetto motore di ricerca venga sottratto agli obblighi e alle...
garanzie previsti dalla direttiva 95/46/CE, ciò che pregiudicherebbe l’effetto utile di quest’ultima e la tutela efficace e completa delle libertà e dei diritti fondamentali delle persone fisiche che detta direttiva mira a garantire (v., per analogia, sentenza L’Oréal e a., […] p.ti 62 e 63), segnatamente il diritto al rispetto della vita privata, con riguardo al trattamento dei dati personali, al quale detta direttiva riconosce un’importanza particolare, come confermato segnatamente dall’art.1, §1, e dai considerando 2 e 10 della direttiva medesima (v., in tal senso, sentenze Österreichischer Rundfunk e a., C-465/00, C-138/01 e C-139/01, […] p.to 70; Rijkeboer, C-553/07, […] p.to 47, nonché IPI, C-473/12, […] p.to 28 e la giurisprudenza ivi citata).

59. Dal momento che la prima delle tre condizioni elencate dal giudice del rinvio è sufficiente di per sé sola per concludere che uno stabilimento come Google Spain soddisfa il criterio previsto dall’art.4, §1, lett.a), della direttiva 95/46/CE, non è necessario esaminare le altre due condizioni.

60. Alla luce delle considerazioni di cui sopra, occorre rispondere alla prima questione, lett.a), dichiarando che l’art.4, §1, lett.a), della direttiva 95/46/CE deve essere interpretato nel senso che un trattamento di dati personali viene effettuato nel contesto delle attività di uno stabilimento del responsabile di tale trattamento nel territorio di uno Stato membro, ai sensi della disposizione suddetta, qualora il gestore di un motore di ricerca apra in uno Stato membro una successurale o una filiale destinata alla promozione e alla vendita degli spazi pubblicitari proposti da tale motore di ricerca e l’attività della quale si dirige agli abitanti di detto Stato membro.

Sulla prima questione, lettere da b) a d)

61. Tenuto conto della soluzione data alla prima questione, lett.a), non vi è luogo a rispondere alla prima questione, lettere da b) a d).

Sulla seconda questione, lett.c) e d), concernente l’estensione della responsabilità del gestore di un motore di ricerca ai sensi della direttiva 95/46/CE

62. Con la sua seconda questione, lett.c) e d), il giudice del rinvio chiede, in sostanza, se gli artt.12, lett.b), e 14, comma 1, lett.a), della direttiva 95/46/CE debbano essere interpretati nel senso che, per rispettare i diritti previsti da tali disposizioni, il gestore di un motore di ricerca è obbligato a sopprimere, dall’elenco di risultati che appare a seguito di una ricerca effettuata a partire dal nome di una persona, dei link verso pagine web pubblicate da terzi e contenenti informazioni relative a questa persona, anche nel caso in cui tale nome o tali informazioni non vengano previamente o simultaneamente cancellati dalle pagine web di cui trattasi, e ciò eventualmente anche quando la loro pubblicazione su tali pagine sia di per sé lecita.

63. In via preliminare, occorre ricordare che, come risulta dall’art.1 e dal considerando 10 della direttiva 95/46/CE, quest’ultima mira a garantire un livello elevato di protezione delle libertà e dei diritti fondamentali delle persone fisiche, in particolare del diritto alla vita privata, con riguardo al trattamento dei dati personali (v., in tal senso, sentenza IPI, […] p.to 28).

64. A mente del considerando 25 della direttiva 95/46/CE, i principi di tutela previsti da quest’ultima si esprimono, da un lato, nei vari obblighi a carico dei soggetti che trattano dati – obblighi relativi in particolare alla qualità dei dati, alla sicurezza tecnica, alla notificazione all’autorità di controllo, alle circostanze in cui il trattamento può essere effettuato – e, dall’altro, nel diritto delle persone, i cui dati sono oggetto di trattamento, di essere informate, di poter accedere ai dati e di poterne chiedere la rettifica, o anche di opporsi al trattamento in talune circostanze.

65. La Corte ha già statuito che le disposizioni della direttiva 95/46/CE, disciplinando il trattamento di dati personali che possono arrecare pregiudizio alle libertà fondamentali e, segnatamente, al diritto alla vita privata, devono necessariamente essere interpretate alla luce dei diritti fondamentali che, secondo una costante giurisprudenza, formano parte integrante dei principi generali del diritto di cui la Corte garantisce l’osservanza e che sono ormai iscritti nella Carta (v., in particolare, sentenze Connolly/Commissione, C-274/99, […] p.to 37, nonché Österreichischer Rundfunk e a., […] p.to 68).

66. In tal senso, l’art.7 della Carta garantisce il diritto al rispetto della vita privata, mentre l’art.8 della Carta proclama espressamente il diritto alla protezione dei dati personali. I §§2 e 3 di quest’ultimo articolo precisano che i dati suddetti devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge, che ogni persona ha il diritto di accedere ai dati raccolti che li riguardano e di ottenere la rettifica, e che il rispetto di tali regole è soggetto al controllo di un’autorità indipendente. Tali prescrizioni ricevono attuazione in particolare mediante gli artt.6, 7, 12, 14 e 28 della direttiva 95/46/CE.
70. Quanto all’art. 12, lett.b), della direttiva 95/46/CE, esso dispone che gli Stati membri garantiscono a qualsiasi persona interessata il diritto di ottenere dal responsabile del trattamento, a seconda dei casi, la rettifica, la cancellazione o il congelamento dei dati il cui trattamento non sia conforme alle disposizioni di questa direttiva, in particolare a causa del carattere incompleto o inesatto dei dati. Poiché quest’ultima precisazione relativa all’ipotesi del mancato rispetto di talune prescrizioni dettate dall’art. 6, §1, lett.d), della direttiva 95/46/CE risulta avere carattere esemplificativo e non esaustivo, ne consegue che la non conformità del trattamento, atta a conferire alla persona interessata il diritto garantito dall’art. 12, lett.b), di tale direttiva, può derivare anche dal mancato rispetto delle altre condizioni di liceità imposte da quest’ultima al trattamento di dati personali.

71. A questo proposito occorre ricordare che, fatte salve le deroghe ammesse ai sensi dell’art. 13 della direttiva 95/46/CE, qualsiasi trattamento di dati personali deve, da un lato, essere conforme ai principi relativi alla qualità dei dati, enunciati all’art. 6 di detta direttiva, e, dall’altro, rispondere ad uno dei principi relativi alla legittimazione dei trattamenti di dati, elencati all’art. 7 della direttiva stessa (v. sentenze Österreichischer Rundfunk e a., […], p.to 65; ASNEF e FECEMD, C-468/10 e C-469/10, […], p.to 26, nonché Worten, C-342/12, […], p.to 33).

72. A mente del citato art. 6, e fatte salve le disposizioni specifiche che gli Stati membri possono prevedere per trattamenti a scopi storici, statistici o scientifici, spetta al responsabile del trattamento garantire che i dati personali siano «trattati lealmente e lecitamente», che vengano «rilevati per finalità determinate, esplicite e legittime, e successivamente trattati in modo non incompatibile con tali finalità», che siano «adeguati, pertinenti e non eccedenti rispetto alle finalità per le quali vengono rilevati e/o per le quali vengono successivamente trattati», che siano «esatti e, se necessario, aggiornati» e, infine, che siano «conservati in modo da consentire l’identificazione delle persone interessate per un arco di tempo non superiore a quello necessario al conseguimento delle finalità per le quali sono rilevati o sono successivamente trattati». In tale contesto, detto responsabile deve prendere tutte le misure ragionevoli affinché i dati che non soddisfano le prescrizioni dettate dalla disposizione suddetta vengano cancellati o rettificati.

73. Quanto alla legittimazione, ai sensi dell’art. 7 della direttiva 95/46/CE, di un trattamento come quello oggetto del procedimento principale effettuato dal gestore di un motore di ricerca, esso può ricadere sotto il motivo contemplato dal citato art. 7, alla lett.f).

74. Tale disposizione consente il trattamento di dati personali allorché questo è necessario per il perseguimento dell’interesse legittimo del responsabile del trattamento oppure del terzo o dei terzi cui vengono comunicati i dati, a condizione che non prevalgano l’interesse o i diritti e le libertà fondamentali della persona interessata — segnatamente il suo diritto al rispetto della sua vita privata con riguardo al trattamento dei dati personali —, i quali richiedono una tutela ai sensi dell’art. 1, §1, di detta direttiva. L’applicazione del citato art. 7, lett.f), esige dunque una ponderazione dei contrapposti diritti e interessi in gioco, nell’ambito della quale si deve tener conto dell’importanza dei diritti della persona interessata risultanti dagli artt. 7 e 8 della Carta (v. sentenza ASNEF e FECEMD, […], p.ti 38 e 40).

75. Se dunque la conformità del trattamento di dati agli artt. 6 e 7, lett.f), della direttiva 95/46/CE può essere verificata nell’ambito di una domanda ai sensi dell’art. 12, lett.b), di quest’ultima, la persona interessata può inoltre avvalersi, a determinate condizioni, del diritto di opposizione previsto dall’art. 14, comma 1, lett.a), della medesima direttiva.

76. Ai sensi di tale art. 14, comma 1, lett.a), gli Stati membri riconoscono alla persona interessata il diritto — almeno nei casi di cui all’art. 7, lett.e) e f), della citata direttiva — di opporsi in qualsiasi momento, per motivi preminenti e legittimi derivanti dalla sua situazione particolare, al trattamento di dati che la riguardano, salvo disposizione contraria prevista dalla normativa nazionale. La ponderazione da effettuarsi nell’ambito di tale art. 14, comma 1, lett.a), permette così di tener conto in modo più specifico di tutte le circostanze caratterizzanti la situazione concreta della persona interessata. In caso di opposizione giustificata, il trattamento messo in atto dal responsabile di quest’ultimo non può più riguardare tali dati.

77. Le domande ai sensi degli artt. 12, lett.b), e 14, comma 1, lett.a), della direttiva 95/46/CE possono essere direttamente presentate dalla persona interessata al responsabile del trattamento, il quale deve in tal caso procedere al debito esame della loro fondatezza e, eventualmente, porre fine al trattamento dei dati in questione. Qualora il responsabile del trattamento non dia seguito a tali domande, la persona interessata può adire l’autorità di controllo o l’autorità giudiziaria affinché
queste effettuino le verifiche necessarie e ordinino al suddetto responsabile l’adozione di misure precise conseguenti.

78. A questo proposito occorre rilevare che dall’art.28, §§3 e 4, della direttiva 95/46/CE risulta che qualsiasi persona può presentare a un’autorità di controllo una domanda relativa alla tutela dei suoi diritti e delle sue libertà con riguardo al trattamento di dati personali, e che tale autorità dispone di poteri investigativi e di poteri effettivi di intervento che le consentono di ordinare in particolare il congelamento, la cancellazione o la distruzione di dati, oppure di vietare a titolo provvisorio o definitivo un trattamento.

79. È alla luce di tali considerazioni che occorre interpretare e applicare le disposizioni della direttiva 95/46/CE disciplinanti i diritti della persona interessata allorché quest’ultima presenta all’autorità di controllo o all’autorità giudiziaria una domanda quale quella oggetto del procedimento a quo.

80. A questo proposito occorre anzitutto rilevare che, come si è constatato ai punti da 36 a 38 della presente sentenza, un trattamento di dati personali, quale quello in esame nel procedimento principale, effettuato dal gestore di un motore di ricerca, può incidere significativamente sui diritti fondamentali al rispetto della vita privata e alla protezione dei dati personali, nel caso in cui la ricerca con l’aiuto di tale motore venga effettuata a partire dal nome di una persona fisica, dal momento che detto trattamento consente a qualsiasi utente di Internet di ottenere, mediante l’elenco di risultati, una visione complessiva strutturata delle informazioni relative a questa persona reperibili su Internet, che toccano potenzialmente una moltitudine di aspetti della sua vita privata e che, senza il suddetto motore di ricerca, non avrebbero potuto – o solo difficilmente avrebbero potuto – essere connesse tra loro, e consente dunque di stabilire un profilo più o meno dettagliato di tale persona. Inoltre, l’effetto dell’ingerenza nei suddetti diritti della persona interessata risulta moltiplicato in ragione del ruolo importante che svolgono Internet e i motori di ricerca nella società moderna, i quali conferiscono alle informazioni contenute in un siffatto elenco di risultati carattere ubiquitario (v., in tal senso, sentenza eDate Advertising e a., C-509/09 e C-161/10, […], p.to 45).

81. Vista la gravità potenziale di tale ingerenza, è giocoforza constatare che quest’ultima non può essere giustificata dal semplice interesse economico del gestore di un siffatto motore di ricerca in questo trattamento di dati. Tuttavia, poiché la soppressione di link dall’elenco di risultati potrebbe, a seconda dell’informazione in questione, avere ripercussioni sul legittimo interesse degli utenti di Internet potenzialmente interessati ad avere accesso a quest’ultima, occorre ricercare, in situazioni quali quelle oggetto del procedimento principale, un giusto equilibrio segnatamente tra tale interesse e i diritti fondamentali della persona di cui trattasi derivanti dagli artt.7 e 8 della Carta. Se indubbiamente i diritti della persona interessata tutelati da tali articoli prevalgono, di norma, anche sul citato interesse degli utenti di Internet, tale equilibrio può nondimeno dipendere, in casi particolari, dalla natura dell’informazione di cui trattasi e dal suo carattere sensibile per la vita privata della persona suddetta, nonché dall’interesse del pubblico a disporre di tale informazione, il quale può variare, in particolare, a seconda del ruolo che tale persona riveste nella vita pubblica.

82. L’autorità di controllo o l’autorità giudiziaria, all’esito della valutazione dei presupposti di applicazione degli artt.12, lett.b), e 14, comma 1, lett.a), della direttiva 95/46/CE, da effettuarsi allorché ricevono una domanda quale quella oggetto del procedimento principale, possono ordinare al suddetto gestore di sopprimere, dall’elenco di risultati che appare a seguito di una ricerca effettuata a partire dal nome di una persona, dei link verso pagine web pubblicate da terzi e contenenti informazioni relative a tale persona, senza che un’ingiunzione in tal senso presupponga che tale nome e tali informazioni siano, con il pieno consenso dell’editore o su ingiunzione di una delle autorità sopra menzionate, previamente o simultaneamente cancellati dalla pagina web sulla quale sono stati pubblicati.

83. Infatti, come si è constatato ai punti da 35 a 38 della presente sentenza, poiché il trattamento dei dati effettuato nel contesto dell’attività di un motore di ricerca si distingue da e si aggiunge a quello effettuato dagli editori di siti web e incide ulteriormente sui diritti fondamentali della persona interessata, il gestore di tale motore di ricerca quale responsabile del trattamento in questione deve assicurare, nell’ambito delle sue responsabilità, delle sue competenze e delle sue possibilità, che tale trattamento soddisfi le prescrizioni della direttiva 95/46/CE, affinché le garanzie previste da quest’ultima possano svilupparsi pienamente i loro effetti.
84. In proposito occorre rilevare che, tenuto conto della facilità con cui informazioni pubblicate su un sito web possono essere riprodotte su altri siti, nonché del fatto che i responsabili della loro pubblicazione non sempre sono assoggettati alla normativa dell’Unione, non sarebbe possibile realizzare una tutela efficace e completa delle persone interessate nel caso in cui queste dovessero preventivamente o in parallelo ottenere dagli editori di siti web la cancellazione delle informazioni che le riguardano.

85. Inoltre, il trattamento da parte dell’editore di una pagina web, consistente nella pubblicazione di informazioni relative a una persona fisica, può, eventualmente, essere effettuato «esclusivamente a scopi giornalistici» e beneficiare così, a norma dell’art.9 della direttiva 95/46/CE, di deroghe alle prescrizioni dettate da quest’ultima, mentre non sembra integrare tale ipotesi il trattamento effettuato dal gestore di un motore di ricerca. Non si può dunque escludere che la persona interessata possa, in determinate circostanze, esercitare i diritti contemplati dagli artt.12, lett.b), e 14, comma 1, lett.a), della direttiva 95/46/CE contro il suddetto gestore del motore di ricerca, ma non contro l’editore della pagina web.

86. Infine, occorre constatare che non soltanto il motivo giustificante, a norma dell’art.7 della direttiva 95/46/CE, la pubblicazione di un dato personale su un sito web non coincide necessariamente con il motivo che si applica all’attività dei motori di ricerca, ma che, anche quando tale coincidenza sussista, il risultato del bilanciamento degli interessi in gioco da effettuarsi ai sensi degli artt.7, lett.f), e 14, comma 1, lett.a), di detta direttiva può divergere a seconda che si tratti del trattamento effettuato dal gestore di un motore di ricerca o di quello effettuato dall’editore di detta pagina web, in quanto, da un lato, i legittimi interessi che giustificano questi trattamenti possono essere differenti e, dall’altro, le conseguenze che tali trattamenti hanno per la persona interessata, e segnatamente per la sua vita privata, non sono necessariamente le stesse.

87. Infatti, l’inclusione nell’elenco di risultati – che appare a seguito di una ricerca effettuata a partire dal nome di una persona – di una pagina web e delle informazioni in essa contenute relative a questa persona, poiché facilita notevolmente l’accessibilità di tali informazioni a qualsiasi utente di Internet che effettui una ricerca sulla persona di cui trattasi e può svolgere un ruolo decisivo per la diffusione di dette informazioni, è idonea a costituirsi un’ingerenza più rilevante nel diritto fondamentale al rispetto della vita privata della persona interessata che non la pubblicazione da parte dell’editore della suddetta pagina web.

88. Alla luce dell’insieme delle considerazioni sopra esposte, occorre rispondere alla seconda questione, lett.c) e d), dichiarando che gli artt.12, lett.b), e 14, comma 1, lett.a), della direttiva 95/46/CE devono essere interpretati nel senso che, al fine di rispettare i diritti previsti da tali disposizioni, e sempre che le condizioni da queste fissate siano effettivamente soddisfatte, il gestore di un motore di ricerca è obbligato a sopprimere, dall’elenco di risultati che appare a seguito di una ricerca effettuata a partire dal nome di una persona, dei link verso pagine web pubblicate da terzi e contenenti informazioni relative a questa persona, anche nel caso in cui tale nome o tali informazioni non vengano previamente o simultaneamente cancellati dalle pagine web di cui trattasi, e ciò eventualmente anche quando la loro pubblicazione su tali pagine web sia di per sé lecita.

**Sulla terza questione, concernente la portata dei diritti della persona interessata garantiti dalla direttiva 95/46/CE**

89. Con la sua terza questione, il giudice del rinvio chiede, in sostanza, se gli artt.12, lett.b), e 14, comma 1, lett.a), della direttiva 95/46/CE debbano essere interpretati nel senso che consentono alla persona interessata di esigere dal gestore di un motore di ricerca che questi sopprimra dall’elenco di risultati, che appare a seguito di una ricerca effettuata a partire dal nome di questa persona, dei link verso pagine web legittimamente pubblicate da terzi e contenenti informazioni veritiere riguardanti quest’ultima, a motivo del fatto che tali informazioni possono arrecare pregiudizio o che essa desidera l’«oblio» di queste informazioni dopo un certo tempo.

[...]

92. Quanto all’art.12, lett.b), della direttiva 95/46/CE, la cui applicazione è subordinata alla condizione che il trattamento di dati personali sia incompatibile con la direttiva stessa, occorre ricordare che, come si è rilevato al p.to 72 della presente sentenza, un’incompatibilità siffatta può derivare non soltanto dal fatto che tali dati siano inesatti, ma anche segnatamente dal fatto che essi siano inadeguati, non pertinenti o eccessivi in rapporto alle finalità del trattamento, che non siano aggiornati, oppure che siano conservati per un arco di tempo superiore a quello necessario, a meno che la loro conservazione non si imponga per motivi storici, statistici o scientifici.
93. Da tali prescrizioni, dettate dall'art.6, §1, lettere da c) a e), della direttiva 95/46/CE, discende che anche un trattamento inizialmente legittimo di dati esatti può divenire, con il tempo, incompatibile con la direttiva suddetta qualora tali dati non siano più necessari in rapporto alle finalità per le quali sono stati raccolti o trattati. Tale situazione si configura in particolare nel caso in cui i dati risultino inadeguati, non siano o non siano più pertinenti, ovvero siano eccessivi in rapporto alle finalità suddette e al tempo trascorso.

94. Pertanto, nell'ipotesi in cui si constati, in seguito a una domanda della persona interessata ai sensi dell'art.12, lett.b), della direttiva 95/46/CE, che l'inclusione nell'elenco di risultati – che appare a seguito di una ricerca effettuata a partire dal suo nome – dei link verso pagine web, legittimamente pubblicate da terzi e contenenti informazioni veritiere relative alla sua persona, è, allo stato attuale, incompatibile con il citato art.6, §1, lettere da c) a e), a motivo del fatto che tali informazioni appaiono, alla luce dell'insieme delle circostanze caratterizzanti il caso di specie, inadeguate, non pertinenti o non più pertinenti, ovvero eccessive in rapporto alle finalità del trattamento in questione realizzato dal gestore del motore di ricerca, le informazioni e i link in parola di cui al suddetto elenco di risultati devono essere cancellati.

95. Per quanto riguarda le domande ai sensi del suddetto art.12, lett.b), fondate sul presunto mancato rispetto delle condizioni previste dall'art.7, lett.f), della direttiva 95/46/CE, nonché le domande a norma dell'art.14, comma 1, lett.a), della medesima direttiva, occorre rilevare che ciascun trattamento di dati personali deve essere legittimato in virtù di tale art.7 per tutto il tempo in cui viene effettuato.

96. Alla luce di quanto precede, nel valutare domande di questo tipo proposte contro un trattamento di dati quale quello in esame nel procedimento principale, occorre verificare in particolare se l'interessato abbia diritto a che l'informazione riguardante il suo nome non venga più, allo stato attuale, collegata al suo nome da un elenco di risultati che appare a seguito di una ricerca effettuata a partire dal suo nome. In proposito occorre sottolineare che la constatazione di un diritto siffatto non presuppone che l'inclusione dell'informazione in questione nell'elenco di risultati arrechi un pregiudizio all'interessato.

97. Dato che l'interessato può, sulla scorta dei suoi diritti fondamentali derivanti dagli artt.7 e 8 della Carta, chiedere che l'informazione in questione non venga più messa a disposizione del grande pubblico mediante la sua inclusione in un siffatto elenco di risultati, occorre considerare – come risulta in particolare dal p.to 81 della presente sentenza – che i diritti fondamentali di cui sopra prevalgono, in linea di principio, non soltanto sull'interesse economico del gestore del motore di ricerca, ma anche sull'interesse di tale pubblico a trovare l'informazione suddetta in occasione di una ricerca concernente il nome di questa persona. 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, mediante l'inclusione summenzionata, all'informazione di cui trattasi.

98. Relativamente ad una situazione come quella in esame nel procedimento principale, che riguarda la visualizzazione – nell'elenco di risultati che l'utente di Internet ottiene effettuando una ricerca a partire dal nome della persona interessata con l'aiuto di Google Search – di link verso pagine degli archivi on-line di un quotidiano, contenenti annunci che menzionano il nome di tale persona e si riferiscono ad un'asta immobiliare legata ad un pignoramento effettuato per la riscossione coattiva di crediti previdenziali, occorre affermare che, tenuto conto del carattere sensibile delle informazioni contenute in tali annunci per la vita privata di detta persona, nonché del fatto che la loro pubblicazione iniziale era stata effettuata 16 anni prima, la persona interessata vanta un diritto a che tali informazioni non siano più collegate al suo nome attraverso un elenco siffatto. Pertanto, dal momento che nella fattispecie non sembrano sussistere ragioni particolari giustificanti un interesse preponderante del pubblico ad avere accesso, nel contesto di una ricerca siffatta, a dette informazioni – aspetto questo che spetta però al giudice del rinvio verificare –, la persona interessata può esigere, a norma degli artt.12, lett.b), e 14, comma 1, lett.a), della direttiva 95/46/CE, la soppressione dei link suddetti da tale elenco di risultati.

99. Dalle suesposte considerazioni discende che occorre rispondere alla terza questione dichiarando che gli artt.12, lett.b), e 14, comma 1, lett.a), della direttiva 95/46/CE devono essere interpretati nel senso che, nel valutare i presupposti di applicazione di tali disposizioni, si deve verificare in particolare se l'interessato abbia diritto a che l'informazione in questione riguardante la sua persona non venga più, allo stato attuale, collegata al suo nome da un elenco di risultati che appare a seguito di una ricerca effettuata a partire dal suo nome, senza per questo che la
constatazione di un diritto siffatto presuppone che l’inclusione dell’informazione in questione in tale elenco arrechi un pregiudizio a detto interessato. Dato che l’interessato può, sulla scorta dei suoi diritti fondamentali derivanti dagli artt. 7 e 8 della Carta, chiedere che l’informazione in questione non venga più messa a disposizione del grande pubblico in virtù della sua inclusione in un siffatto elenco di risultati, i diritti fondamentali di cui sopra 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.

Per questi motivi, la Corte (Grande Sezione) dichiara:

1) L’art. 2, lett. b) e d), della direttiva 95/46/CE/CE [...] del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, deve essere interpretato nel senso che, da un lato, l’attività di un motore di ricerca consistente nel trovare informazioni pubblicate o inserite da terzi su Internet, nell’indicizzarle in modo automatico, nel memorizzarle temporaneamente e, infine, nel metterle a disposizione degli utenti di Internet secondo un determinato ordine di preferenza, deve essere qualificata come «trattamento di dati personali», ai sensi del citato art. 2, lett. b), qualora tali informazioni contengano dati personali, e che, dall’altro lato, il gestore di detto motore di ricerca deve essere considerato come il «responsabile» del trattamento summenzionato, ai sensi dell’art. 2, lett. d), di cui sopra.

2) L’art. 4, § 1, lett. a), della direttiva 95/46/CE deve essere interpretato nel senso che un trattamento di dati personali viene effettuato nel contesto delle attività di uno stabilimento del responsabile di tale trattamento nel territorio di uno Stato membro, ai sensi della disposizione suddetta, qualora il gestore di un motore di ricerca apra in uno Stato membro una succursale o una filiale destinata alla promozione e alla vendita degli spazi pubblicitari proposti da tale motore di ricerca e l’attività della quale si dirige agli abitanti di detto Stato membro.

3) Gli artt. 12, lett. b), e 14, comma 1, lett. a), della direttiva 95/46/CE devono essere interpretati nel senso che, al fine di rispettare i diritti previsti da tali disposizioni, e sempre che le condizioni da queste fissate siano effettivamente soddisfatte, il gestore di un motore di ricerca è obbligato a sopprimere, dall’elenco di risultati che appare a seguito di una ricerca effettuata a partire dal nome di una persona, dei link verso pagine web pubblicate da terzi e contenenti informazioni relative a questa persona, anche nel caso in cui tale nome o tali informazioni non vengano previamente o simultaneamente cancellati dalle pagine web di cui trattasi, e ciò eventualmente anche quando la loro pubblicazione su tali pagine web sia di per sé lecita.

4) Gli artt. 12, lett. b), e 14, comma 1, lett. a), della direttiva 95/46/CE devono essere interpretati nel senso che, nel valutare i presupposti di applicazione di tali disposizioni, si deve verificare in particolare se l’interessato abbia diritto a che l’informazione in questione riguardante la sua persona non venga più, allo stato attuale, collegata al suo nome da un elenco di risultati che appare a seguito di una ricerca effettuata a partire dal suo nome, senza per questo che la constatazione di un diritto siffatto presupponga che l’inclusione dell’informazione in questione in tale elenco arrechi un pregiudizio a detto interessato. Dato che l’interessato può, sulla scorta dei suoi diritti fondamentali derivanti dagli artt. 7 e 8 della Carta, chiedere che l’informazione in questione non venga più messa a disposizione del grande pubblico in virtù della sua inclusione in un siffatto elenco di risultati, i diritti fondamentali di cui sopra 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 summenzionata 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.
DISCUSSIONE

1. Quando sussiste la giurisdizione di uno Stato membro nei confronti dell’impresa che gestisce un motore di ricerca avente la propria sede principale al di fuori dell’Unione Europea?

2. L’attività propria di un motore di ricerca rientra nella nozione di trattamento di dati ai sensi della normativa sui dati personali?

3. In caso di risposta affermativa alla domanda precedente, il gestore del motore di ricerca è da considerarsi quale “responsabile del trattamento” dei dati, ai sensi della medesima normativa?

4. In caso di risposta affermativa alla domanda precedente, di quali dati?

5. Se il gestore del motore di ricerca è da considerarsi quale “responsabile del trattamento”, può essere ad esso ordinato di rimuovere dai propri indici informazioni pubblicate da terzi dai propri indici? Se sì, deve essere previamente o simultaneamente chiesto al titolare di quella pagina di eliminare il contenuto?

6. Un gestore di motore di ricerca è tenuto a rimuovere dai propri indici informazioni lecitamente pubblicate da terzi e ancora visibili in quella pagina web?

7. L’interessato può chiedere al gestore di motore di ricerca di rimuovere dai propri indici informazioni lecitamente pubblicate da terzi e ancora visibili in quella pagina web?

8. Cosa pensate del diritto all’oblio? In particolare, cosa pensate del rapporto dello stesso con i diritti di informazione e libera espressione e dell’incidenza che la sua connotazione può avere sulla Rete?

NORME

- artt.2, lett.b) e d), 4, §1, lett.a) e c), 12, comma 1, lett.b), e 14, comma 1, lett.a), direttiva 95/46/CE
- artt.7, 8, Carta dei diritti fondamentali dell’Unione Europea
8. PRIVACY E PERSONALITÀ
8.1 Privacy ed espressione della personalità

Consiglio di Stato, sez.III, 21 febbraio 2014, n.848

[...] Fatto

1. Con decreto della Polizia del 23 dicembre 2011, veniva irrogata al Sig. -omissis-, nella qualità di -omissis-, la sanzione della sospensione dal servizio per un mese, con correlata deduzione di tale periodo dal computo di anzianità, perché “evidenziando gravissima mancanza di correttezza nel comportamento, pubblicava su un social network alcune foto ritraenti se stesso in abbigliamenti ed atteggiamenti inopportuni, corredate da informazioni personali di indubbia equivocità, favorendo l’accesso alla visione delle stesse senza particolari precauzioni”.

2. Con ricorso al TAR Lombardia il Sig. -omissis- deduceva tre motivi di impugnazione:
   A) [...];
   B) violazione di legge e falsa applicazione degli artt.2, 3, 14, 15 della Cost., nonché degli artt.8, 10, 14 della CEDU; violazione di legge ed eccesso di potere per violazione degli artt.20 e 22 del d.lgs. n.196/2003 e dell’art.22 della l. 675/1996; violazione di legge ed eccesso di potere con riferimento all’art.2, comma 1, lett.b) del d.lgs. 9 luglio 2003, n.216.
   C) violazione e falsa applicazione degli artt.6 e 4 del d.lgs. n.737/1981 e illogicità della decisione. Difetto di sovraesposizione e riconoscibilità del soggetto del materiale fotografico; eccesso di potere per travisamento dei fatti, erroneità dei presupposti e per abnormità del provvedimento. Difetto di motivazione.

3. La sentenza del TAR Lombardia n.2841/2012 rigettava il ricorso, nonostante lo stesso Tribunale avesse, con ordinanza n.751 del 1° giugno 2012, accolto la domanda cautelare evidenziando l’illegittima pervasività e la carenza delle necessarie autorizzazioni dell’istruttoria svolta.

[...]

Diritto

1. L’appello è fondato.
1.1. Sinteticamente, si premettono i fatti come risultanti dagli atti di causa.

L’11 febbraio 2011, alle ore 12.21, il Sig. -omissis- si è registrato sul social network -omissis- attraverso la creazione di un profilo denominato -omissis-; sul sito era visionabile pubblicamente la foto di un’attrice, ma entrando vi era la possibilità di accedere ad alcune foto personali che lo ritraevano a mezzobusto in abbigliamento femminile, e di accedere, ma solo su sua autorizzazione, ad un’area privata dove erano visionabili altre foto, alcune ritraenti parti del corpo “in abiti succinti”.

Sullo stesso sito, all’incirca un’ora dopo, si è collegato -omissis- ovvero -omissis-, incaricato dal Dirigente superiore dell’appellante, che avviava indagini su segnalazione di dipendenti, mai identificati.

Il 14 febbraio, su richiesta di accesso all’album riservato “solo per pochi”, il -omissis- autorizza -omissis- a visionare altre foto personali, nell’area riservata del profilo, non altrimenti visionabile (doc.13).

In tale area il -omissis- visiona e stampa le foto che “ritraggono una persona in biancheria intima e una solo il volto di una persona vestita che dal Dirigente è stata attribuita all’assistente -omissis-”.

Il 22 febbraio, quindi, il Dirigente contatta -omissis-, Business Development Manager per l’Italia di -omissis-, per acquisire informazioni utili ad “accertamenti amministrativi”.

Dalla risposta fornita risulta l’ora in cui il profilo è stato registrato, che non erano presenti dati anagrafici e che non era possibile stabilire quando e chi ha inserito foto sul profilo; inoltre, vengono comunicati dati riservati, ossia che l’utente ha fornito in chat i suoi numeri di telefono dichiarando di trovarsi in zona San Siro, nonché l’indirizzo di posta elettronica, il relativo indirizzo IP e i successivi IP di accesso.

Il 9 marzo 2011, il Dirigente trasmette relazione al Questore e viene, quindi, avviato il procedimento disciplinare.
La contestazione di addebiti del 19 aprile 2011 (doc. 3) attribuisce al ricorrente di aver tenuto una condotta connotata da fatti antitetici ai doveri richiesti ad un appartenente alla -omissis-
“sintomo di una volontà comportamentale che pur rientrando nell’ambito dell’attività privata e delle
proprie abitudini sessuali, per il veicolo scelto di manifestarsi - social network omissis,... spazio
condivisibile da chiunque ed assimilabile al concetto giuridico di luogo aperto al pubblico - ha
assunto consapevoli e voluti aspetti pubblici che si riflettono inevitabilmente sul prestigio delle
funzioni e degli appartenenti ai ruoli dell’Amministrazione della Pubblica Sicurezza, ripercuotendosi
in senso sfavorevole sul rapporto di servizio”.

La contestazione, in buona sostanza, si fonda sul principio per cui mettere consapevolmente
a disposizione propri dati sensibili o informazioni in generale a persone non conosciute, tramite
network, equivale a renderle pubbliche e siffatto comportamento sarebbe lesivo del “decoro”
dell’Amministrazione di pubblica sicurezza.

Con delibera del Consiglio di disciplina del 26 ottobre 2011, richiamata per relationem nel
decreto del 23 dicembre 2011 impugnato, è stata irrogata la sanzione indicata, in quanto il
comportamento del militare si pone in contrasto con il decoro delle funzioni degli appartenenti ai
ruoli della Pubblica Sicurezza, riconducibile alla mancanza prevista dall’art.6, n.1 in relazione
all’art.4, n.18, del d.p.r. 737/1981.

1.2. Con l’atto di appello il Sig. -omissis-, oltre a dedurre una serie di illegittimità procedurali,
compiute nella fase pre-istruttoria ed istruttoria, erroneamente disattese dal primo giudice,
ripropone la censura di carattere sostanziale (motivo terzo), con cui denunciava che la sanzione
applicata non trova ragionevole giustificazione nei fatti addebitati.

Ad avviso del Collegio, la censura è fondata, nei limiti e nei termini di cui alla presente
motivazione.

1.3. Il primo giudice ha erroneamente ritenuto che la condotta posta in essere dall’appellante
rientri nella fattispecie disciplinare delineata dagli artt.4, n.18, e 6, n.1, d.p.r. 737/1981.

L’ipotesi disciplinare, difatti, si estrinseca in “qualsiasi altro comportamento, anche fuori dal
servizio, non espressamente preveduto nelle precedenti ipotesi, comunque non conforme al
decoro delle funzioni degli appartenenti ai ruoli dell’amministrazione”.

La sentenza impugnata richiama una serie di precedenti giurisprudenziali che sarebbero
accomunati dal considerare oggetto della sanzione condotte caratterizzate dalla “non conformità al
decoro” e a “gravi mancanze attinenti alla disciplina e alle norme di contegno”.

Ha ritenuto, inoltre, che sia fuorviante la valorizzazione di profili attinenti ad una presunta
discriminazione sessuale e che la condotta in contrasto con gli obblighi di decoro debba essere
rilevata in ragione “dell’oggettiva e potenziale diffusione di tali manifestazioni all’esterno, non
idoneamente garantita nei cc.dd. social network”.

Il giudice, sotto il profilo della prova, valorizza le ammissioni dello stesso ricorrente nel corso
dell’udizione del 21 settembre 2011, innanzi al Consiglio di disciplina, da cui si evince che sulla
home page del profilo sarebbe risultata inserita una sola foto di un’attrice famosa, ma che
cliccando col cursore sulla stessa comparivano n.8 icone fotografiche … le altre 5 lo ritraevano
truccato, a mezzobusto” [...].

Si tratterebbe di dichiarazioni dal tenore confesionale, che confermano l’oggettiva lesività per
l’intero corpo di Polizia degli effetti conseguenti al facile accesso alle fotografie riservate.

1.4. L’appellante, di contro, deduce che l’intera condotta posta in essere si è svolta
integralmente in un contesto che rientra, comunque, nello spazio riservato alla vita privata.

Osserva, infatti, come non sia stato dato giusto peso alla circostanza che egli non ha
pubblicato il suo cellulare, non ha inserito foto “compromettenti” in un sito web accessibile
indiscriminatamente (ma solo su richiesta del provocatore in una cartella esclusivamente
accessibile con sua autorizzazione); che non vi è in atti la deduzione di ulteriori contatti da parte di
terzi; che non ha offerto prestazioni sessuali; che il suo status di poliziotto non è in alcun modo
desumibile dal sito, atteso che non sono noti i suoi dati personali.

Egli deduce altresì che gli obblighi di decoro derivanti dall’appartenenza all’amministrazione
non possono legittimamente estendersi financo a limitare le leciti scelte di vita che un dipendente
assume nella riservatezza della propria vita privata.

1.5. Il Collegio osserva che erroneamente il giudice di prime cure ha ritenuto “pubbliche” le
fotografie di cui trattasi, la cui capacità lesiva del decoro delle funzioni di pubblica sicurezza è
comunque fortemente dubbia.
Le questioni cui il collegio è stato chiamato a dare risposta sono sostanzialmente due, ossia se possa ritenersi “pubblica” la foto inserita nel profilo di un social-network, non immediatamente visibile a chiunque, ma accessibile tramite alcune specifiche operazioni e, in particolare, se lo sia la foto accessibile solo tramite autorizzazione del titolare del profilo; se possa ritenersi offensiva del decoro dell’amministrazione della pubblica sicurezza la foto, pubblicata con le dette modalità, che ritrae un dipendente in abbigliamento femminile, rendendo quindi palese la sua inclinazione sessuale, in ambiente non lavorativo.

Sul primo punto, il Collegio osserva che, come emerge anche dalle dichiarazioni rese dall’agente -omissis- (cfr. verbale istruttorio del 27 aprile 2011), dagli atti si evince che nella pagina di presentazione dell’utente, cui il -omissis- ha avuto accesso cliccando sul nickname -omissis- compariva una foto di una nota attrice con “la possibilità di visualizzare altre 8 foto”, di cui 4 sono state stampate e da cui è stata riconosciuta l’immagine del -omissis-, travisato da donna. Altre foto, invece, riproducenti primi piani del ricorrente, travestito da donna, e alcune “parti di un corpo in abiti succinti”, sono state da lui visionate solo su autorizzazione dell’interessato, in area riservata “solo per pochi”.

Sembra al Collegio che, ai fini della integrazione della fattispecie sanzionata, ossia della “lesione al decoro delle funzioni” o della “grave mancanza attinente alla disciplina e alle norme di contegno”, sia essenziale stabilire se le descritte modalità di accesso al profilo personale su social network possano far ritenere pubbliche le fotografie dell’interessato, “in ipotesi” offensive del riserbo e della compostezza che si confà ad un agente della Pubblica Sicurezza, si da raggiungere un numero indefinito di soggetti.

Ad avviso del collegio vanno valutate tutte le circostanze di fatto e le concrete modalità in cui si è svolta la vicenda.

In questo quadro diventa risolutiva la circostanza che l’accesso al profilo personale è possibile solo a chi conosca lo username dell’interessato, il quale funziona da filtro per l’accesso, e che non può ritenersi, pertanto, indiscriminatamente visitabile da chiunque, ma rivolto essenzialmente a “conoscenti”, che abbiano appunto la “chiave” di accesso (lo username). All’apertura del profilo compariva, come già ricordato, una foto di donna non riferibile al Sig.-omissis-, nonché alcune delle altre foto, raffiguranti il mezzobusto del ricorrente (doc. 18) erano visionabili solo dopo l’accesso; a ciò va aggiunta l’altra modalità, ossia che altre foto, che presentano “parti di corpo in abiti succinti”, queste senza dubbio più suscettibili di urtare la riservatezza ed il pudore, erano visionabili solo su specifica autorizzazione dell’interessato.

In nessun caso, né nella parte “pubblica” del profilo, né nell’area “privata”, era riconoscibile lo status di poliziotto, né era reso pubblico il nome, il recapito o altri dati personali. La comunicazione, dunque, anche se utilizza un mezzo (Internet) che si rivolge al pubblico, si svolge in “luogo” non aperto a tutti, ma riservato, essendo l’accesso al profilo personale possibile solo a chi conosce lo username dell’interessato, come dire, per esempio, in ambito diverso dalla rete, il suo indirizzo di casa e il suo nome, o tutt’al più conosce alcuni elementi selezionati dallo stesso (interessi, città di abitazione, categorie preferenziali di interlocutori, etc.) in grado di far risalire al suo profilo.

A maggior ragione, la riservatezza delle immagini è garantita per quelle inserite nell’area “per pochi”, la cui visione necessita di specifica autorizzazione dell’interessato, successiva all’accesso.

Pur non disconoscendo che chiunque eserciti la propria libertà di espressione si assume “doveri e responsabilità”, la cui ampiezza dipende dalla sua situazione e dai mezzi tecnici che utilizza, il Collegio ritiene che, nella fattispecie, la comunicazione rientra nelle legittime manifestazioni della libertà di espressione, in quanto afferisce esclusivamente alla vita privata del ricorrente, e si svolge in modo da proteggere sufficientemente il proprio ruolo professionale, fuori dall’ambiente di lavoro e di riferimenti anche casuali allo stesso.

1.6. Rimanendo ancora alla prima delle due questioni che la delicata vicenda pone, per il collegio va preso seriamente in considerazione quanto il primo giudice ha ritenuto a proposito del fatto che la valutazione della “pubblicità” debba essere svolta “oggettivamente” e “potenzialmente”. Va premesso che in una materia così delicata, nella quale si confrontano interessi parimenti importanti e di rango costituzionale - per uno verso, la libertà di espressione e il diritto alla “vita privata”, per altro verso, interessi pubblici afferenti alla sicurezza dei cittadini ed al buon andamento dell’amministrazione che la garantisce,- non si possa rinunciare, anzi va fatta con scrupolo maggiore, alla verifica se in concreto vi sia una oggettiva pubblicità, potenzialmente lesiva dell’ordine di appartenenza del militare sanzionato.
Orbene, nel caso di specie, a ben vedere, va esclusa anche la potenziale lesività del corpo di appartenenza, in quanto le foto (semmai volesse ritenersi idonea a tal fine la modalità di comunicazione utilizzata) sono rimaste sempre nel dominio delle parti del presente processo, in quanto il profilo dell’appellante non era stato visionato da altro utente se non dal Sig. -omissis- fino al 14 febbraio (com’è evidente dal doc. 18 depositato, dove l’indice di accesso al sito è indicato “molo basso”= 0) ed è stato cancellato il successivo 28 febbraio; né vi è agli atti la deduzione o la prova della consultazione da parte di terzi. Tanto più che la pericolosità deve valutarsi in concreto e non in astratto.

1.7. Quanto alla seconda questione che si pone, a parte quanto testé osservato, il Collegio avanza qualche dubbio circa la portata lesiva delle fotografie del ricorrente, visionabili sulla parte liberamente accessibile del suo profilo.

In altri termini, a parte l’esclusione in concreto della integrazione della fattispecie disciplinarmente rilevante, sorge il problema se il costume della società attuale, di cui il giudice deve essere interpretare nell’applicazione di clausole generali, consideri offensivo per il decoro dell’amministrazione, e se sia qualificabile come “condotta connotata da fatti antitetici ai doveri richiesti ad un appartenente alla -omissis-” l’immagine di travestimento femminile, che palesa l’incarico omosessuale, utilizzata nella vita privata, in ambiente non lavorativo e senza riferimenti all’attività lavorativa svolta. Ma, soprattutto, va valutato se ciò possa costituire efficace strumento di ricatto per quei militari che ammettono la propria inclinazione sessuale, che è poi alla base della norma incriminatrice e della giusta cautela mostrata in proposito dall’amministrazione militare.

1.8. A proposito dell’ultimo profilo testé indicato, il collegio rileva come correttamente nella sentenza impugnata si faccia riferimento alla ricattabilità dell’appellante a causa dell’episodio incriminato.

Premesso che molti aspetti della vita personale di un individuo possono essere oggetto di manipolazione e usati a fini distorti, non sembra particolarmente esposto in tal senso l’agente di polizia per il fatto di palesare la propria identità sessuale con le modalità descritte.

La circostanza che, in concreto, sia da escludere l’avvenuta diffusione pubblica delle immagini rafforza l’inconcludenza anch’essa di questo rilievo.

E’ utile premettere altresì che l’idea di “decoro” appartiene alla “morale”, che varia nel tempo e nello spazio, specialmente nella nostra epoca caratterizzata da una rapida e costante evoluzione delle opinioni circa la vita sessuale delle persone.

Il concetto di “decoro”, invero, dal punto di vista giuridico, è una clausola indeterminata ed elastica, la definizione dei cui confini è affidata all’interprete in un determinato contesto storico-sociale, e che risente dell’evoluzione dei costumi e della cultura, tanto che la condotta che poteva essere avvertita come contraria al sentimento pubblico della decenza e offensiva per la sensibilità e moralità sociale alcuni decenni or sono, oggi ha mutato la sua portata lesiva essendo tollerata o accettata dalla coscienza sociale.

In conformità con il disposto di cui agli artt.2 e 3 della Costituzione, la vita sessuale è riconosciuta come condizione dell’uomo degna di tutela, in quanto riguarda l’identità della persona e il diritto alla realizzazione della propria personalità, e secondo l’art.10 della Convenzione dei diritti dell’Uomo rientra nella libertà di espressione la possibilità di palesare opinioni e comportamenti che rivelano l’incarico sessuale.

Come afferma da tempo la CEDU, “La libertà di espressione costituisce una delle fondamenta essenziali della società, una delle condizioni sostanziali per il suo progresso e per lo sviluppo di ogni uomo. Sottraendo al §2 dell’art.10, vale non solo per le «informazioni» o «idee» che sono favorevolmente accolte o considerate inoffensive o indifferenti, ma anche per quelle che offendono, scuotono o disturbano lo Stato o un qualunque settore della popolazione. Così richiedono il pluralismo, la tolleranza e lo spirito di apertura, senza i quali non esiste una «società democratica». Da ciò deriva, in particolare, che ogni «formalità», «condizione», «restrizione» o «sanzione» imposta in materia di libertà di espressione deve essere proporzionata allo scopo legittimo perseguito” (CEDU n.24 del 7 dicembre 1976). Inoltre, sempre la Corte ha affermato che lo stesso tipo di divieto non costituisce violazione dell’art.10 della Convenzione, nonostante le restrizioni sull’abbigliamento ben possano integrare violazioni della libertà di espressione, in quanto “ai fini della configurabilità della violazione, deve essere inequivoco che attraverso gli abiti si voglia comunicare una specifica idea o convinzione” (Kara c. Regno Unito 22 ottobre 1998).
Sicché, per il diritto vivente, il travestimento in abiti femminili non può, quindi, qualificarsi in sé “indecoroso” se l’atteggiamento assunto non consiste in pose sconvenienti o contrastanti col comune senso del pudore, del rispetto della propria o altrui persona.

Orbene, per il collegio ciò vale anche se trattasi di agente di pubblica sicurezza, che agisce nella sfera della sua vita privata, senza riconoscibilità del suo status e senza alcun riferimento all’amministrazione di appartenenza.

Infatti, proprio in virtù del cambiamento dei costumi, l’inclinazione sessuale, anche degli appartenenti alle forze dell’ordine, non costituisce materia di ricatto o di possibili ritorsioni specifiche, o almeno non più di altri aspetti della vita della persona. E ciò vale anche nell’ipotesi in cui, ma nel caso di specie è stato già escluso, coloro i quali sono venuti in contatto con l’agente di polizia vengano successivamente a sapere del suo status.

2. In conclusione, l’appello va accolto e, per l’effetto, in riforma della sentenza appellata, va accolto il ricorso di primo grado con l’annullamento del provvedimento impugnato.

3. Le spese di giudizio si compensano tra le parti, attesa la novità delle questioni trattate.

4. In conformità all’art.52 del d.lgs. 30 giugno 2003, n.196, il collegio dispone che venga omessa l’indicazione delle generalità e di altri dati identificativi dell’interessato riportati sulla sentenza

[...]
9. LIBERTA’ DI ESPRESSIONE IN RETE
9.1. Linguaggio offensivo e indecente in Rete e libertà di parola

Supreme Court of the United States, 26 June 1997, n.96/511 (Reno v. ACLU)

[syllabus]

[...]

Two provisions of the Communications Decency Act of 1996 (CDA or Act) seek to protect minors from harmful material on the Internet, an international network of interconnected computers that enables millions of people to communicate with one another in "cyberspace" and to access vast amounts of information from around the world. Title 47 U.S.C.A. \$223(a)(1)(B)(ii) [...] criminalizes the "knowing" transmission of "obscene or indecent" messages to any recipient under 18 years of age. Section 223(d) prohibits the "knowing" sending or displaying to a person under 18 of any message "that, in context, depicts or describes, in terms patently offensive as measured by contemporary community standards, sexual or excretory activities or organs." Affirmative defenses are provided for those who take "good faith, ..., effective, ..., actions" to restrict access by minors to the prohibited communications, \$223(e)(5)(A), and those who restrict such access by requiring certain designated forms of age proof, such as a verified credit card or an adult identification number, \$223(e)(5)(B). A number of plaintiffs filed suit challenging the constitutionality of \$\$223(a)(1) and 223(d). After making extensive findings of fact, a three-judge District Court convened pursuant to the Act entered a preliminary injunction against enforcement of both challenged provisions. The Court's judgment enjoins the Government from enforcing \$223(a)(1)(B)'s prohibitions insofar as they relate to "indecent" communications, but expressly preserves the Government's right to investigate and prosecute the obscenity or child pornography activities prohibited therein. The injunction against enforcement of \$223(d) is unqualified because that section contains no separate reference to obscenity or child pornography. The Government appealed to this Court under the Act's special review provisions, arguing that the District Court erred in holding that the CDA violated both the First Amendment because it is overbroad and the Fifth Amendment because it is vague.

Held: The CDA's "indecent transmission" and "patently offensive display" provisions abridge "the freedom of speech" protected by the First Amendment.

(a) Although the CDA's vagueness is relevant to the First Amendment overbreadth inquiry, the judgment should be affirmed without reaching the Fifth Amendment issue.

(b) A close look at the precedents relied on by the Government - Ginsberg v. New York [...]; FCC v. Pacifica Foundation [...] and Renton v. Playtime Theatres, Inc. [...] raises, rather than relieves, doubts about the CDA's constitutionality. The CDA differs from the various laws and orders upheld in those cases in many ways, including that it does not allow parents to consent to their children's use of restricted materials; is not limited to commercial transactions; fails to provide any definition of "indecent" and omits any requirement that "patently offensive" material lack socially redeeming value; neither limits its broad categorical prohibitions to particular times nor bases them on an evaluation by an agency familiar with the medium's unique characteristics; is punitive; applies to a medium that, unlike radio, receives full First Amendment protection; and cannot be properly analyzed as a form of time, place, and manner regulation because it is a content-based blanket restriction on speech. These precedents, then, do not require the Court to uphold the CDA and are fully consistent with the application of the most stringent review of its provisions.

[...]

(d) Regardless of whether the CDA is so vague that it violates the Fifth Amendment, the many ambiguities concerning the scope of its coverage render it problematic for First Amendment purposes. For instance, its use of the undefined terms "indecent" and "patently offensive" will provoke uncertainty among speakers about how the two standards relate to each other and just what they mean. The vagueness of such a content-based regulation, see, e.g., Gentile v. State Bar of Nev. [...], coupled with its increased deterrent effect as a criminal statute, see, e.g., Dombrowski v. Pfister [...], raise special First Amendment concerns because of its obvious chilling effect on free speech. Contrary to the Government's argument, the CDA is not saved from vagueness by the fact that its "patently offensive" standard repeats the second part of the three-prong obscenity test set
forth in *Miller v. California* [...]. The second *Miller* prong reduces the inherent vagueness of its own "patently offensive" term by requiring that the proscribed material be "specifically defined by the applicable state law." In addition, the CDA applies only to "sexual conduct," whereas, the CDA prohibition extends also to "excretory activities" and "organs" of both a sexual and excretory nature. Each of *Miller*’s other two prongs also critically limits the uncertain sweep of the obscenity definition. Just because a definition including three limitations is not vague, it does not follow that one of those limitations, standing alone, is not vague. The CDA’s vagueness undermines the likelihood that it has been carefully tailored to the congressional goal of protecting minors from potentially harmful materials.

(e) The CDA lacks the precision that the First Amendment requires when a statute regulates the content of speech. Although the Government has an interest in protecting children from potentially harmful materials, see, *e.g.*, *Ginsberg* [...], the CDA pursues that interest by suppressing a large amount of speech that adults have a constitutional right to send and receive, see, *e.g.*, *Sable* [...]. Its breadth is wholly unprecedented. The CDA’s burden on adult speech is unacceptable if less restrictive alternatives would be at least as effective in achieving the Act’s legitimate purposes. See, *e.g.*, *Sable* [...]. The Government has not proved otherwise. On the other hand, the District Court found that currently available *user-based* software suggests that a reasonably effective method by which *parents* can prevent their children from accessing material which the *parents* believe is inappropriate will soon be widely available. Moreover, the arguments in this Court referred to possible alternatives such as requiring that indecent material be "tagged" to facilitate parental control, making exceptions for messages with artistic or educational value, providing some tolerance for parental choice, and regulating some portions of the Internet differently than others. Particularly in the light of the absence of any detailed congressional findings, or even hearings addressing the CDA’s special problems, the Court is persuaded that the CDA is not narrowly tailored.

(f) The Government’s three additional arguments for sustaining the CDA’s affirmative prohibitions are rejected. First, the contention that the Act is constitutional because it leaves open ample "alternative channels" of communication is unpersuasive because the CDA regulates speech on the basis of its content, so that a "time, place, and manner" analysis is inapplicable. See, *e.g.*, *Consolidated Edison Co. of N.Y. v. Public Serv. Comm’n of N.Y.* [...]. Second, the assertion that the CDA’s "knowledge" and "specific person" requirements significantly restrict its permissible application to communications to persons the sender knows to be under 18 is untenable, given that most Internet forums are open to all comers and that even the strongest reading of the "specific person" requirement would confer broad powers of censorship, in the form of a "heckler’s veto," upon any opponent of indecent speech. Finally, there is no textual support for the submission that material having scientific, educational, or other redeeming social value will necessarily fall outside the CDA’s prohibitions.

(g) The §223(e)(5) defenses do not constitute the sort of "narrow tailoring" that would save the CDA. The Government’s argument that transmitters may take protective "good faith action" by "tagging" their indecent communications in a way that would indicate their contents, thus permitting recipients to block their reception with appropriate software, is illusory, given the requirement that such action be "effective": the proposed screening software does not currently exist, but, even if it did, there would be no way of knowing whether a potential recipient would actually block the encoded material. The Government also failed to prove that §223(b)(5)’s verification defense would significantly reduce the CDA’s heavy burden on adult speech. Although such verification is actually being used by some commercial providers of sexually explicit material, the District Court’s findings indicate that it is not economically feasible for most noncommercial speakers.

(i) The Government’s argument that its "significant" interest in fostering the Internet’s growth provides an independent basis for upholding the CDA’s constitutionality is singularly unpersuasive. The dramatic expansion of this new forum contradicts the factual basis underlying this contention: that the unregulated availability of "indecent" and "patently offensive" material is driving people away from the Internet.

****
DISCUSSIONE

1. La decisione parla di Internet e cyberspace: in che termini?
2. Perché il CDA è stato ritenuto dalla Corte in violazione del Primo Emendamento?
3. Lo scopo del Governo era quello di tutelare i minori da linguaggio indecente ed offensivo. Come pensate che questo sia possibile, in Internet?

*****

NORME

- Primo Emendamento, Costituzione degli Stati Uniti
9.2. Pedopornografia virtuale e libertà di parola

Supreme Court of the United States, 16 April 2002, n.00-795 (Ashcroft v. Free Speech Coalition) [syllabus]

The Child Pornography Prevention Act of 1996 (CPPA) expands the federal prohibition on child pornography to include not only pornographic images made using actual children, 18 U.S.C. §2256(8)(A), but also “any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture” that “is, or appears to be, of a minor engaging in sexually explicit conduct,” §2256(8)(B), and any sexually explicit image that is “advertised, promoted, presented, described, or distributed in such a manner that conveys the impression” it depicts “a minor engaging in sexually explicit conduct,” §2256(8)(D). Thus, §2256(8)(B) bans a range of sexually explicit images, sometimes called “virtual child pornography,” that appear to depict minors but were produced by means other than using real children, such as through the use of youthful-looking adults or computer-imaging technology. Section 2256(8)(D) is aimed at preventing the production or distribution of pornographic material pandered as child pornography. Fearing that the CPPA threatened their activities, respondents, an adult-entertainment trade association and others, filed this suit alleging that the “appears to be” and “conveys the impression” provisions are overbroad and vague, chilling production of works protected by the First Amendment. The District Court disagreed and granted the Government summary judgment, but the Ninth Circuit reversed. Generally, pornography can be banned only if it is obscene under Miller v. California […], but pornography depicting actual children can be proscribed whether or not the images are obscene because of the State’s interest in protecting the children exploited by the production process, New York v. Ferber […], and in prosecuting those who promote such sexual exploitation […]. The Ninth Circuit held the CPPA invalid on its face, finding it to be substantially overbroad because it bans materials that are neither obscene under Miller nor produced by the exploitation of real children as in Ferber.

Held: The prohibitions of §§2256(8)(B) and 2256(8)(D) are overbroad and unconstitutional. […]

(a) Section 2256(8)(B) covers materials beyond the categories recognized in Ferber and Miller, and the reasons the Government offers in support of limiting the freedom of speech have no justification in this Court’s precedents or First Amendment law. […]

(1) The CPPA is inconsistent with Miller. It extends to images that are not obscene under the Miller standard, which requires the Government to prove that the work in question, taken as a whole, appeals to the prurient interest, is patently offensive in light of community standards, and lacks serious literary, artistic, political, or scientific value […]. Materials need not appeal to the prurient interest under the CPPA, which proscribes any depiction of sexually explicit activity, no matter how it is presented. It is not necessary, moreover, that the image be patently offensive. Pictures of what appear to be 17-year-olds engaging in sexually explicit activity do not in every case contravene community standards. The CPPA also prohibits speech having serious redeeming value, proscribing the visual depiction of an idea - that of teenagers engaging in sexual activity - that is a fact of modern society and has been a theme in art and literature for centuries. A number of acclaimed movies, filmed without any child actors, explore themes within the wide sweep of the statute’s prohibitions. If those movies contain a single graphic depiction of sexual activity within the statutory definition, their possessor would be subject to severe punishment without inquiry into the literary value of the work. This is inconsistent with an essential First Amendment rule: A work’s artistic merit does not depend on the presence of a single explicit scene. See, e.g., Book Named “John Cleland’s Memoirs of a Woman of Pleasure” v. Attorney General of Mass. […]. Under Miller, redeeming value is judged by considering the work as a whole. Where the scene is part of the narrative, the work itself does not for this reason become obscene, even though the scene in isolation might be offensive. See Kois v. Wisconsin […]. The CPPA cannot be read to prohibit obscenity, because it lacks the required link between its prohibitions and the affront to community standards prohibited by the obscenity definition. […]

(2) The CPPA finds no support in Ferber. The Court rejects the Government's argument that speech prohibited by the CPPA is virtually indistinguishable from material that may be banned
under *Ferber*. That case upheld a prohibition on the distribution and sale of child pornography, as well as its production, because these acts were “*intrinsically related*” to the sexual abuse of children in two ways. [...] First, as a permanent record of a child’s abuse, the continued circulation itself would harm the child who had participated. [...] Second, because the traffic in child pornography was an economic motive for its production, the State had an interest in closing the distribution network. [...] Under either rationale, the speech had what the Court in effect held was a proximate link to the crime from which it came. In contrast to the speech in *Ferber*, speech that is itself the record of sexual abuse, the CPPA prohibits speech that records no crime and creates no victims by its production. Virtual child pornography is not “*intrinsically related*” to the sexual abuse of children. While the Government asserts that the images can lead to actual instances of child abuse, the causal link is contingent and indirect. The harm does not necessarily follow from the speech, but depends upon some unquantified potential for subsequent criminal acts. The Government’s argument that these indirect harms are sufficient because, as *Ferber* acknowledged, child pornography rarely can be valuable speech [...] suffers from two flaws. First, *Ferber’s* judgment about child pornography was based upon how it was made, not on what it communicated. The case reaffirmed that where the speech is neither obscene nor the product of sexual abuse, it does not fall outside the First Amendment’s protection. [...] Second, *Ferber* did not hold that child pornography is by definition without value. It recognized some works in this category might have significant value, [...] but relied on virtual images – the very images prohibited by the CPPA – as an alternative and permissible means of expression [...]. Because *Ferber* relied on the distinction between actual and virtual child pornography as supporting its holding, it provides no support for a statute that eliminates the distinction and makes the alternative mode criminal as well. [...] (3) The Court rejects other arguments offered by the Government to justify the CPPA’s prohibitions. The contention that the CPPA is necessary because pedophiles may use virtual child pornography to seduce children runs afoul of the principle that speech within the rights of adults to hear may not be silenced completely in an attempt to shield children from it. See, *Sable Communications of Cal., Inc. v. FCC* [...]. That the evil in question depends upon the actor’s unlawful conduct, defined as criminal quite apart from any link to the speech in question, establishes that the speech ban is not narrowly drawn. The argument that virtual child pornography whets pedophiles’ appetites and encourages them to engage in illegal conduct is unavailing because the mere tendency of speech to encourage unlawful acts is not a sufficient reason for banning it, *Stanley v. Georgia* [...], absent some showing of a direct connection between the speech and imminent illegal conduct, see, *Brandenburg v. Ohio* [...]. The argument that eliminating the market for pornography produced using real children necessitates a prohibition on virtual images as well is somewhat implausible because few pornographers would risk prosecution for abusing real children if fictional, computerized images would suffice. Moreover, even if the market deterrence theory were persuasive, the argument cannot justify the CPPA because, here, there is no underlying crime at all. Finally, the First Amendment is turned upside down by the argument that, because it is difficult to distinguish between images made using real children and those produced by computer imaging, both kinds of images must be prohibited. The overbreadth doctrine prohibits the Government from banning unprotected speech if a substantial amount of protected speech is prohibited or chilled in the process. See *Broadrick v. Oklahoma* [...]. The Government’s rejoinder that the CPPA should be read not as a prohibition on speech but as a measure shifting the burden to the accused to prove the speech is lawful raises serious constitutional difficulties. The Government misplaces its reliance on §2252A(c), which creates an affirmative defense allowing a defendant to avoid conviction for nonpossession offenses by showing that the materials were produced using only adults and were not otherwise distributed in a manner conveying the impression that they depicted real children. Even if an affirmative defense can save a statute from First Amendment challenge, here the defense is insufficient because it does not apply to possession or to images created by computer imaging, even where the defendant could demonstrate no children were harmed in producing the images. Thus, the defense leaves unprotected a substantial amount of speech not tied to the Government’s interest in distinguishing images produced using real children from virtual ones. [...] (b) Section 2256(8)(D) is also substantially overbroad. The Court disagrees with the Government’s view that the only difference between that provision and §2256(8)(B)’s “*appears to be*” provision is that §2256(8)(D) requires the jury to assess the material at issue in light of the
manner in which it is promoted, but that the determination would still depend principally upon the prohibited work’s content. The “conveys the impression” provision requires little judgment about the image’s content; the work must be sexually explicit, but otherwise the content is irrelevant. Even if a film contains no sexually explicit scenes involving minors, it could be treated as child pornography if the title and trailers convey the impression that such scenes will be found in the movie. The determination turns on how the speech is presented, not on what is depicted. The Government’s other arguments in support of the CPPA do not bear on §2256(8)(D). The materials, for instance, are not likely to be confused for child pornography in a criminal trial. Pandering may be relevant, as an evidentiary matter, to the question whether particular materials are obscene. See Ginzburg v. United States […]. Where a defendant engages in the “commercial exploitation” of erotica solely for the sake of prurient appeal, id., at 466, the context created may be relevant to evaluating whether the materials are obscene. Section 2256(8)(D), however, prohibits a substantial amount of speech that falls outside Ginzburg’s rationale. Proscribed material is tainted and unlawful in the hands of all who receive it, though they bear no responsibility for how it was marketed, sold, or described. The statute, furthermore, does not require that the context be part of an effort at “commercial exploitation”. Thus, the CPPA does more than prohibit pandering. It bans possession of material pandered as child pornography by someone earlier in the distribution chain, as well as a sexually explicit film that contains no youthful actors but has been packaged to suggest a prohibited movie. Possession is a crime even when the possessor knows the movie was mislabeled. The First Amendment requires a more precise restriction. […]

(c) In light of the foregoing, respondents’ contention that §§2256(8)(B) and 2256(8)(D) are void for vagueness need not be addressed.

[...] Affirmed.

*****

DISCUSSIONE

1. Quali sono le differenze tra pedopornografia e pedopornografia virtuale?

2. Perché il CPPA è stato ritenuto contrario al Primo Emendamento?

3. Il Governo sostiene che la pedopornografia virtuale può essere utilizzata per sedurre minori e che può, in ogni caso, stimolare l’appetito sessuale dei pedofili. Perché la Corte non ritiene valide o sufficienti queste ragioni?

*****

NORME

- Primo Emendamento, Costituzione degli Stati Uniti
9.3. Minacce in Rete e libertà di espressione

Corte di Appello degli Stati Uniti, 9th Circuit, 16 May 2002, n.99-35320 (Planned Parenthood of the Columbia/Willamette Inc. v. ACLA)

[...]

Anti-abortion activists intimidated abortion providers by publishing their names and addresses. A jury awarded more than $100 million in actual and punitive damages against the activists, and the District Court enjoined their speech. We consider whether such speech is protected by the First Amendment.

I

During a 1995 meeting called to mark the anniversary of Roe v. Wade [...], the American Coalition of Life Activists (ACLA) unveiled a poster listing the names and addresses of the "Deadly Dozen," a group of doctors who perform abortions. In large print, the poster declared them guilty of "crimes against humanity" and offered $ 5,000 for information leading to the "arrest, conviction and revocation of license to practice medicine". The poster was later published in an affiliated magazine, Life Advocate, and distributed at ACLA events.

Later that year, in front of the St. Louis federal courthouse, ACLA presented a second poster, this time targeting Dr. Robert Crist. The poster accused Crist of crimes against humanity and various acts of medical malpractice, including a botched abortion that caused the death of a woman. Like the Deadly Dozen List, the poster included Crist's home and work addresses, and in addition, featured his photograph. The poster offered $ 500 to "any ACLA organization that successfully persuades Crist to turn from his child killing through activities within ACLA guidelines" (which prohibit violence).

In January 1996, at its next Roe anniversary event, ACLA unveiled a series of dossiers it had compiled on doctors, clinic employees, politicians, judges and other abortion rights supporters. ACLA dubbed these the "Nuremberg Files", and announced that it had collected the pictures, addresses and other information in the files so that Nuremberg-like war crimes trials could be conducted in "perfectly legal courts once the tide of this nation's opinion turns against the wanton slaughter of God's children". ACLA sent hard copies of the files to Neal Horsley, an anti-abortion activist, who posted the information on a website. The website listed the names of doctors and others who provide or support abortion and called on visitors to supply additional names. The website marked the names of those already victimized by anti-abortion terrorists, striking through the names of those who had been murdered and graying out the names of the wounded. Although ACLA's name originally appeared on the website, Horsley removed it after the initiation of this lawsuit.

Neither the posters nor the website contained any explicit threats against the doctors. But the doctors knew that similar posters prepared by others had preceded clinic violence in the past. By publishing the names and addresses, ACLA robbed the doctors of their anonymity and gave violent anti-abortion activists the information to find them. The doctors responded to this unwelcome attention by donning bulletproof vests, drawing the curtains on the windows of their homes and accepting the protection of U.S. Marshals.

Some of the doctors went on the offensive. Along with two Portland-based health centers, the doctors sued ACLA, twelve activists and an affiliated organization, alleging that their threatening statements violated state and federal law, including the Freedom of Access to Clinic Entrances Act of 1994 (FACE), 18 U.S.C. §248. Because the doctors claimed they were harmed by defendants' speech, the District Court instructed the jury that defendants could only be liable if their statements were "true threats" and therefore unprotected by the First Amendment. In a special verdict, the jury found that all the statements were true threats and awarded the doctors $107 million in actual and punitive damages. The District Court then issued an injunction barring defendants from making or distributing the posters, the webpage or anything similar. ACLA and the other defendants appeal, claiming that their statements are protected by the First Amendment.

II

A.
Extreme rhetoric and violent action have marked many political movements in American history. Patriots intimidated loyalists in both word and deed as they gathered support for American independence. John Brown and other abolitionists, convinced that God was on their side, committed murder in pursuit of their cause. In more modern times, the labor, anti-war, animal rights and environmental movements all have had their violent fringes. As a result, much of what was said even by nonviolent participants in these movements acquired a tinge of menace.

The Supreme Court confronted this problem in *NAACP v. Claiborne Hardware Co.* [...]. There, a group of white-owned businesses sued the NAACP and others who organized a civil rights boycott against the stores. To give the boycott teeth, activists wearing black hats stood outside the stores and wrote down the names of black patrons. After these names were read aloud at meetings and published in a newspaper, sporadic acts of violence were committed against the persons and property of those on the list. At one public rally, Charles Evers, a boycott organizer, threatened that boycott breakers would be "disciplined" and warned that the sheriff could not protect them at night. [...] At another rally, Evers stated, "If we catch any of you going in any of them racist stores, we're gonna break your damn neck" [...]. The Mississippi courts held the boycott organizers liable based on Evers's statements and the activities of the black-hatted activists.

The Supreme Court acknowledged that Evers's statements could be interpreted as inviting violent retaliation, "or at least as intending to create a fear of violence whether or not improper discipline was specifically intended" [...]. Nevertheless, it held that the statements were protected because there was insufficient evidence that Evers had "authorized, ratified, or directly threatened acts of violence" [...]. Nor was publication of the boycott violators' names a sufficient basis for liability, even though collecting and publishing the names contributed to the atmosphere of intimidation that had harmed plaintiffs. [...] While Charles Evers and the defendants in our case pursued very different political goals, the two cases have one key thing in common: political activists used words in an effort to bend opponents to their will.

The First Amendment protects ACLA's statements no less than the statements of the NAACP. Defendants can only be held liable if they "authorized, ratified, or directly threatened" violence. If defendants threatened to commit violent acts, by working alone or with others, then their statements could properly support the verdict. But if their statements merely encouraged unrelated terrorists, then their words are protected by the First Amendment.

Political speech may not be punished just because it makes it more likely that someone will be harmed at some unknown time in the future by an unrelated third party. In *Brandenburg v. Ohio*, [...], the Supreme Court held that the First Amendment protects speech that encourages others to commit violence, unless the speech is capable of "producing imminent lawless action" [...]. It doesn't matter if the speech makes future violence more likely; advocating "illegal action at some indefinite future time" is protected. *Hess v. Indiana* [...]. If the First Amendment protects speech advocating violence, then it must also protect speech that does not advocate violence but still makes it more likely. Unless ACLA threatened that its members would themselves assault the doctors, the First Amendment protects its speech.

B.

ACLA's speech no doubt frightened the doctors, but the constitutional question turns on the source of their fear. The doctors might have understood the statements as veiled threats that ACLA's members (or others working with ACLA) would inflict bodily harm on the doctors unless they stopped performing abortions. So interpreted, the statements are unprotected by the First Amendment, regardless of whether the activists had the means or intent to carry out the threats. See *United States v. Orozco-Santillan* [...]. So long as they should have foreseen that the doctors would take the threats seriously, the speech is unlawful. [...]

But the statements might also have scared the doctors in another way. By singling out the plaintiffs from among the thousands across the country who are involved in delivering abortion services, ACLA called them to the unfriendly attention of violent anti-abortion activists. And by publishing the doctors' addresses, ACLA made it easier for any would-be terrorists to carry out their gruesome mission. From the doctors' point of view, such speech may be just as frightening as a direct threat, but it remains protected under *Claiborne Hardware*.

The jury would be entitled to hold defendants liable if it understood the statements as expressing their intention to assault the doctors but not if it understood the statements as merely encouraging or making it more likely that others would do so. But the jury instruction was
ambiguous on this critical point. The instruction provided that "a statement is a 'true threat' when a reasonable person making the statement would foresee that the statement would be interpreted by those to whom it is communicated as a serious expression of an intent to bodily harm or assault" […]. This instruction was consistent with our previous threat cases. See Lovell v. Powell […]. But in those previous cases, there was no need to emphasize that threats must be direct because the speakers themselves made it perfectly clear that they would be the ones to carry out the threats. Under the instruction in this case, the jury could have found the anti-abortion activists liable based on the fact that, by publishing the doctors' names, the activists made it more likely that the doctors would be harmed by third parties.

This is not a fanciful possibility. The record contains much evidence that the doctors were frightened, at least in part, because they anticipated that their unwelcome notoriety could expose them to physical attacks from third parties unrelated to defendants. For example, plaintiff Dr. Elizabeth Newhall testified, "I feel like my risk comes from being identified as a target. And … all the John Salvis in the world know who I am, and that's my concern". Testimony of Elizabeth Newhall, Planned Parenthood of the Columbia/Willamette, Inc. v. American Coalition of Life Activists […]; ("Up until January of '95, I felt relatively diluted by the … you know, in the pool of providers of abortion services. I didn't feel particularly visible to the people who were … you know, to the John Salvis of the world, you know. I sort of felt one of a big, big group"). Likewise, Dr. Warren Martin Hern, another plaintiff, testified that when he heard he was on the list, "I was terrified … It's hard to describe the feeling that - that you are on a list of people to - who have been brought to public attention in this way. I felt that this was a list of doctors to be killed". Testimony of Warren Martin Hern, Planned Parenthood […].

Were the instruction taken literally, the jury could have concluded that ACLA's statements contained "a serious expression of intent to harm," not because they authorized or directly threatened violence, but because they put the doctors in harm's way. However, the First Amendment does not permit the imposition of liability on that basis.

C.

Although the jury instruction was ambiguous, we need not decide whether the ambiguity was so great as to require us to set aside the verdict. Even if the jury drew only the permissible inference, we must evaluate the record for ourselves to ensure that the judgment did not trespass on the defendants' First Amendment rights. Specifically, we must determine whether ACLA's statements could reasonably be construed as saying that ACLA (or its agents) would physically harm doctors who did not stop performing abortions. Because the District Court rejected the First Amendment claim, we conduct a de novo review of both the law and the relevant facts. See Lovell, […]. The question therefore is not whether the facts found below are supported by the record but whether we, looking at the record with fresh eyes, make the same findings. If we disagree with the District Court, our findings prevail. See Eastwood v. National Enquirer, Inc. […].

We start by noting that none of the statements ACLA is accused of making mention violence at all. While pungent, even highly offensive, ACLA's statements carefully avoid threatening the doctors with harm "in the sense that there are no `quotable quotes' calling for violence against the targeted providers". Planned Parenthood of the Columbia/Willamette, Inc. v. American Coalition of Life Activists […]. Instead, ACLA offers rewards to those who take nonviolent measures against the doctors, such as seeking the revocation of their medical licenses and protesting their activities. One poster talks about persuading Crist to "turn from his child killing," but stops short of suggesting any violence or other criminal conduct against him. The website seeks to gather information about abortion supporters and encourages others to do the same. ACLA also speaks of future "perfectly legal" Nuremberg-like trials, to be held at a time when public opinion has turned in its favor.

We recognize that the words actually used are not dispositive, because a threat may be inferred from the context in which the statements are made. However, there are at least two kinds of ambiguity that context can resolve. The first deals with statements that call for violence on their face, but are unclear as to who is to commit the violent acts - the speaker or a third party. All cases of which we are aware fall into this category: They hold that, where the speaker expressly mentions future violence, context can make it clear that it is the speaker himself who means to carry out the threat. […]

A more difficult problem arises when the statements, like the ones here, not only fail to threaten violence by the defendants, but fail to mention future violence at all. Can context supply the violent message that language alone leaves out? While no case answers this question, we
note important theoretical objections to stretching context so far. Context, after all, is often not of the speaker's making. For example, the District Court in this case admitted evidence of numerous acts of violence surrounding the abortion controversy, almost none of them committed by the defendants or anyone connected with them. In the jury's eyes, then, defendants' statements were infused with a violent meaning, at least in part, because of the actions of others. If this were a permissible inference, it could have a highly chilling effect on public debate on any cause where somebody, somewhere has committed a violent act in connection with that cause. A party who does not intend to threaten harm, nor say anything at all suggesting violence, would risk liability by speaking out in the midst of a highly charged environment.

In considering whether context could import a violent meaning to ACLA's non-violent statements, we deem it highly significant that all the statements were made in the context of public discourse, not in direct personal communications. Although the First Amendment does not protect all forms of public speech, such as statements inciting violence or an imminent panic, the public nature of the speech bears heavily upon whether it could be interpreted as a threat. As we held in McCalden v. California Library Ass'n [...], "public speeches advocating violence" are given substantially more leeway under the First Amendment than "privately communicated threats" [...]; see also Orozco-Santillan [...] ("Although a threat must be distinguished from what is constitutionally protected speech, this is not a case involving statements with a political message" [...].)

There are two reasons for this distinction: First, what may be hyperbole in a public speech may be understood (and intended) as a threat if communicated directly to the person threatened, whether face-to-face, by telephone or by letter. In targeting the recipient personally, the speaker leaves no doubt that he is sending the recipient a message of some sort. In contrast, typical political statements at rallies or through the media are far more diffuse in their focus because they are generally intended, at least in part, to shore up political support for the speaker's position.

Second, and more importantly, speech made through the normal channels of group communication, and concerning matters of public policy, is given the maximum level of protection by the Free Speech Clause because it lies at the core of the First Amendment. See Claiborne Hardware [...] ("Since respondents would impose liability on the basis of a public address - which predominantly contained highly charged political rhetoric lying at the core of the First Amendment - we approach this suggested basis of liability with extreme care"). With respect to such speech, we must defer to the well-recognized principle that political statements are inherently prone to exaggeration and hyperbole. See Watts [...] ("The language of the political arena ... is often vituperative, abusive, and inexact" [...]). If political discourse is to rally public opinion and challenge conventional thinking, it cannot be subdued. Nor may we saddle political speakers with implications their words do not literally convey but are later "discovered" by judges and juries with the benefit of hindsight and by reference to facts over which the speaker has no control.

Our guiding light, once again, is Claiborne Hardware. There, Charles Evers expressly threatened violence when he warned the boycott violators that "we're gonna break your damn necks," and that the sheriff could not protect them from retribution. [...] Evers made these statements at a time when there had already been violence against the boycott breakers. Evers did not himself identify specific individuals to be disciplined, but his associates had gathered and published the names, and there's no doubt that the black community in the small Mississippi county where the boycott was taking place knew whom Evers was talking about. The Supreme Court held that, despite his express call for violence, and the context of actual violence, Evers's statements were protected, because they were quintessentially political statements made at a public rally, rather than directly to his targets. [...]

If Charles Evers's speech was protected by the First Amendment, then ACLA's speech is also protected. Like Evers, ACLA did not communicate privately with its targets; the statements were made in public fora. And, while ACLA named its targets, it said nothing about planning to harm them; indeed, it did not even call on others to do so. This stands in contrast to the words of Charles Evers, who explicitly warned his targets that they would suffer broken necks and other physical harm. Under the standard of Claiborne Hardware, the jury's verdict cannot stand.

**Vacated and Remanded** with instructions that the District Court dissolve the injunction and enter judgment for the defendants on all counts.

[...]

192
DISCUSSIONE

1. Perché i dossier sui medici abortisti sono stati chiamati “Nuremberg files”?
2. Quale elemento, in casi come questo, è necessario per far cadere la protezione del Primo Emendamento?
3. Quali sono le similitudini e quali sono le differenze tra questo caso e Claiborne Hardware?

NORME

- Primo Emendamento, Costituzione degli Stati Uniti
9.4. Libertà di espressione e hate speech

Code of conduct on countering illegal hate speech online

Facebook, Microsoft, Twitter and YouTube (hereinafter "the IT Companies") – also involved in the EU Internet Forum – share, together with other platforms and social media companies, a collective responsibility and pride in promoting and facilitating freedom of expression throughout the online world;

The IT Companies also share the European Commission's and EU Member States' commitment to tackle illegal hate speech online. Illegal hate speech, as defined by the Framework Decision 2008/913/JHA of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law and national laws transposing it, means all conduct publicly inciting to violence or hatred directed against a group of persons or a member of such a group defined by reference to race, colour, religion, descent or national or ethnic origin. The IT Companies and the European Commission also stress the need to defend the right to freedom of expression, which, as the European Court of Human Rights has stated, "is applicable not only to "information" or "ideas" that are favourably received or regarded as inoffensive or as a matter of indifference, but also to those that offend, shock or disturb the State or any sector of the population".

Broader society and in particular civil society organisations (CSOs) also have a crucial role to play in the field of preventing the rise of hatred online, by developing counter-narratives promoting non-discrimination, tolerance and respect, including through awareness-raising activities.

The IT Companies support the European Commission and EU Member States in the effort to respond to the challenge of ensuring that online platforms do not offer opportunities for illegal online hate speech to spread virally. The spread of illegal hate speech online not only negatively affects the groups or individuals that it targets, it also negatively impacts those who speak out for freedom, tolerance and non-discrimination in our open societies and has a chilling effect on the democratic discourse on online platforms.

The Joint Statement issued by the extraordinary Justice and Home Affairs Council of 24 March 2016 on the terrorist attacks in Brussels underlines that "the Commission will intensify work with IT companies, notably in the EU Internet Forum, to counter terrorist propaganda and to develop by June 2016 a code of conduct against hate speech online".

In order to prevent the spread of illegal hate speech, it is essential to ensure that relevant national laws transposing the Council Framework Decision 2008/913/JHA are fully enforced by Member States in the online as well as the in the offline environment. While the effective application of provisions criminalising hate speech is dependent on a robust system of enforcement of criminal law sanctions against the individual perpetrators of hate speech, this work must be complemented with actions geared at ensuring that illegal hate speech online is expeditiously acted upon by online intermediaries and social media platforms, upon receipt of a valid notification, in an appropriate time-frame. To be considered valid in this respect, a notification should not be insufficiently precise or inadequately substantiated.

The IT Companies underline that the present code of conduct is aimed at guiding their own activities as well as sharing best practices with other internet companies, platforms and social media operators.

---

† Microsoft-hosted consumer services, as relevant.
‡ Handyside v. the United Kingdom judgment of 7 December 1976, §49.
Article 16 of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ("Directive on electronic commerce", OJ L 178, 17.7.2000), indicates that Member States and the Commission shall encourage the drawing up of codes of conduct at Union level, by trade, professional and consumer associations or organisations designed to contribute to the implementation of its Articles 5 to 15.
The IT Companies, taking the lead on countering the spread of illegal hate speech online, have agreed with the European Commission on a code of conduct setting the following public commitments:

- The IT Companies to have in place clear and effective processes to review notifications regarding illegal hate speech on their services so they can remove or disable access to such content. The IT companies to have in place Rules or Community Guidelines clarifying that they prohibit the promotion of incitement to violence and hateful conduct.
- Upon receipt of a valid removal notification, the IT Companies to review such requests against their rules and community guidelines and where necessary national laws transposing the Framework Decision 2008/913/JHA, with dedicated teams reviewing requests.
- The IT Companies to review the majority of valid notifications for removal of illegal hate speech in less than 24 hours and remove or disable access to such content, if necessary.
- In addition to the above, the IT Companies to educate and raise awareness with their users about the types of content not permitted under their rules and community guidelines. The notification system could be used as a tool to do this.
- The IT companies to provide information on the procedures for submitting notices, with a view to improving the speed and effectiveness of communication between the Member State authorities and the IT Companies, in particular on notifications and on disabling access to or removal of illegal hate speech online. The information is to be channelled through the national contact points designated by the IT companies and the Member States respectively. This would also enable Member States, and in particular their law enforcement agencies, to further familiarise themselves with the methods to recognise and notify the companies of illegal hate speech online.
- The IT Companies to encourage the provision of notices and flagging of content that promotes incitement to violence and hateful conduct at scale by experts, particularly via partnerships with CSOs, by providing clear information on individual company, Rules and Community Guidelines and rules on the reporting and notification processes. The IT Companies to endeavour to strengthen partnerships with CSOs by widening the geographical spread of such partnerships and, where appropriate, to provide support and training to enable CSO partners to fulfil the role of a “trusted reporter” or equivalent, with due respect to the need of maintaining their independence and credibility.
- The IT Companies to rely on support from Member States and the European Commission to ensure access to a representative network of CSO partners and “trusted reporters” in all Member States to help provide high quality notices. IT Companies to make information about “trusted reporters” available on their websites.
- The IT Companies to provide regular training to their staff on current societal developments and to exchange views on the potential for further improvement.
- The IT Companies to intensify cooperation between themselves and other platforms and social media companies to enhance best practice sharing.
- The IT Companies and the European Commission, recognizing the value of independent counter speech against hateful rhetoric and prejudice, aim to continue their work in identifying and promoting independent counter-narratives, new ideas and initiatives and supporting educational programs that encourage critical thinking.
- The IT Companies to intensify their work with CSOs to deliver best practice training on countering hateful rhetoric and prejudice and increase the scale of their proactive outreach to CSOs to help them deliver effective counter speech campaigns. The European Commission, in cooperation with Member States, to contribute to this endeavour by taking steps to map CSOs’ specific needs and demands in this respect.
- The European Commission in coordination with Member States to promote the adherence to the commitments set out in this code of conduct also to other relevant platforms and social media companies.

The IT Companies and the European Commission agree to assess the public commitments in this code of conduct on a regular basis, including their impact. They also agree to further discuss how to promote transparency and encourage counter and alternative narratives. To this end, regular meetings will take place and a preliminary assessment will be reported to the High Level Group on Combating Racism, Xenophobia and all forms of intolerance by the end of 2016.
DISCUSSIONE

1. Quale è il valore giuridico del Code of conduct?
2. Quale è la definizione di hate speech illegale?
3. Che ruolo svolgono gli operatori privati nel quadro del Code of conduct?
4. Quali sono i meccanismi utilizzati dal Code of conduct per contrastare
5. Il Code of conduct può portare a forme di censura? Perché?
10. LIBERTA’ DI INFORMAZIONE IN RETE
10.1. Diritto all’oblio e aggiornamento delle notizie in Rete

Corte di Cassazione, sez.III civile, 5 aprile 2012, n.5525

[...]

Con sentenza del 6 aprile 2010 il Tribunale di Milano respingeva l'opposizione proposta dal sig. M.T. nei confronti del provvedimento del Garante per la protezione dei beni personali di rigetto dell'istanza di "blocco dei dati personali che lo riguardavano contenuti nell'articolo intitolato Arrestato per corruzione M.T., PSI ex presidente della municipalizzata di Seregno pubblicato sul [...] del [...]", ora "consultabile nell'archivio storico del [...]", anche in versione informatica, mediante accesso al sito [...]", in ordine al quale aveva chiesto la "rimozione dei dati giudiziari".

[...]

Con unico complesso motivo il ricorrente denunzia violazione del d.lgs. n.196/2003, artt.2, 7, 11, 99, 102, 150 e 152, artt.3, 5, 7 del Codice di deontologia e buona condotta per i trattamenti di dati personali per scopi storici [...], in riferimento all'art.360 c.p.c., comma 1, n.3; nonché omessa, insufficiente e contraddittoria motivazione su punto decisivo della controversia, in riferimento all'art.360 c.p.c., comma 1, n.5.

Si duole che il giudice abbia rigettato la domanda di "spostamento di un articolo pubblicato molti anni prima in un'area di un sito web non indizzicabile dai motori di ricerca", erroneamente argomentando dai rilievi che "l'articolo di cui si discute non può essere tecnicamente inteso come una nuova pubblicazione" e che "la ricerca effettuata attraverso i comuni motori - non direttamente legata all'articolo del [...] - dà, in realtà, contenzioso degli esiti processualmente favorevoli".

Lamenta che l'articolo in questione "non reca, in sé, la notizia distinta e successiva che l'inchiesta giudiziaria che aveva condotto all'arresto del ricorrente si sia poi conclusa con il proscioglimento del medesimo, sicché, ancora oggi, il sig. M. è soggetto allo stigma derivante dalla continua riproposizione di una notizia che, al momento della sua pubblicazione era senz'altro vera ed attuale, ma che oggi, a distanza di un così grande lasso di tempo ed in ragione delle sopravvenute vicende favorevoli, getta un intollerabile alone di discredito sulla persona del ricorrente, vittima di una vera a propria gogna mediatica".

Si duole che, movendo dalla considerazione che "l'inserimento di una sorta di sequel nell'articolo contenuto in archivio... farebbe venir meno il valore di documento del testo stesso, vanificandone così la funzione storico-documentaristica", il giudice di merito non abbia considerato che relativamente ad un "trattamento svolto per finalità storico-archivistiche, normate all'art.97 e ss. del medesimo T.U." ai sensi dell'art.7 l'interessato ha diritto all'aggiornamento, alla rettificazione ovvero alla integrazione dei dati che lo riguardano.

Lamenta che, escludendo la sussistenza di "una normativa" quand'anche di "rango secondario ponendo in capo all'editore un onere di aggiornamento degli articoli in archivio", il giudice è erroneamente pervenuto a rigettare anche la domanda di "integrazione dell'articolo in questione con le notizie inerenti gli sviluppi successivi della vicenda narrata, con apposite modalità tecniche, anche non modificative della struttura originaria dello scritto", ritenendo inconfigurabile un suo interesse al riguardo.

Il motivo è fondato e va accolto nei termini di seguito indicati.

Atteso che ogni libertà civile trova il proprio limite nell'altrui libertà e nell'interesse pubblico idoneo a fondare l'eventuale sacrificio dell'interesse del singolo, deve anzitutto osservarsi che la tutela del diritto alla riservatezza va contemperata in particolare con il diritto di ed alla informazione, nonché con i diritti di cronaca, di critica, di satire e di caricatura, questi ultimi trovanti a loro volta limite nel diritto all'identità personale o morale del soggetto cui l'informazione si riferisce.

Con il d.lgs. n.196/2003, il legislatore ha introdotto un sistema informato al prioritario rispetto dei diritti e delle libertà fondamentali e della dignità della persona, e in particolare della riservatezza e del diritto alla protezione dei dati personali nonché dell'identità personale o morale del soggetto (d.lgs. n.196/2003, art.2).

In tale quadro, imprescindibile rilievo assume il bilanciamento tra contrapposti diritti e libertà fondamentali, doendo al riguardo teneresi conto del rango di diritto fondamentale assunto dal diritto alla protezione dei dati personali, tutelato agli artt.21 e 2 Cost., nonché all'art.8 Carta dei diritti fondamentali dell'Unione Europea, quale diritto a mantenere il controllo sulle proprie informazioni che, spettando a "chiunque" (d.lgs. n.196/2003, art.1) e ad "ogni persona" (art.8 Carta), nei diversi contesti ed ambienti di vita, "concorre a delinear l'assetto di una società rispettosa dell’altro e della sua dignità in condizioni di eguaglianza" (così Cass., 4 gennaio 2011, n.186).

Il d.lgs. n.196/2003, ha pertanto sancito il passaggio da una concezione statica a una concezione dinamica della tutela della riservatezza, tesa al controllo dell'utilizzo e del destino dei dati.

L'interessato è divenuto compartenre nell'utilizzazione dei propri dati personali.

I dati personali oggetto di trattamento debbono essere: a) trattati in modo lecito e secondo correttezza; b) raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi; c) esatti e, se necessario, aggiornati; d) pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati; e) conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

La liceità del trattamento trova fondoamento anche nella finalità del medesimo, quest'ultima costituendo un vero e proprio limite intrinseco del trattamento lecito dei dati personali, che fonda l'attribuzione all'interessato del potere di relativo controllo (tanto con riferimento alle finalità originarie che ai successivi impieghi), con facoltà di orientarne la selezione, la conservazione e l'utilizzazione.

L'interessato ha diritto a che l'informazione oggetto di trattamento risponda ai criteri di proporzionalità, necessità, pertinenza allo scopo, esattezza e coerenza con la sua attuale ed effettiva identità personale o morale (c.d. principi di proporzionalità, pertinenza e non eccedenza) (d.lgs. n.196/2003, art.11). Gli è pertanto attribuito il diritto di conoscere in ogni momento chi possiede i suoi dati personali e come li adopera, nonché di opporsi al trattamento dei medesimi, ancorché pertinenti allo scopo della raccolta, ovvero diingerirsii al riguardo, chiedendone la cancellazione, la trasformazione, il blocco, ovvero la rettificazione, l'aggiornamento, l'integrazione (d.lgs. n.196/2003, art.7).

Al di là delle specifiche fonti normative, è in ogni caso il principio di correttezza […] a fondare in termini generali l'esigenza del bilanciamento in concreto degli interessi, e, conseguentemente, il diritto dell'interessato ad opporsi al trattamento, quand'anche lecito, dei propri dati.

Se l'interesse pubblico sotteso al diritto all'informazione (art.21 Cost.) costituisce un limite al diritto fondamentale alla riservatezza (artt.21 e 2 Cost.), al soggetto cui i dati pertengono è correttamente attribuito il diritto all'oblio (v. Cass., 9 aprile 1998, n.3679), e cioè a che non vengano ulteriormente divulgate notizie che per il trascorrere del tempo risultino ormai dimenticate o ignote alla generalità dei consociati.

Atteso che il trattamento dei dati personali può avere ad oggetto anche dati pubblici o pubblicati (v. Cass., 25 giugno 2004, n.11864), il diritto all'oblio salvaguarda in realtà la proiezione sociale dell'identità personale, l'esigenza del soggetto di essere tutelato dalla divulgazione di informazioni (potenzialmente) lesive in ragione della perdita (stante il lasso di tempo intercorso dall'accadimento del fatto che costituisce l'oggetto) di attualità delle stesse, sicché il relativo trattamento viene a risultare non più giustificato ed anzi suscettibile di ostacolare il soggetto nell'esplicazione e nel godimento della propria personalità.

Il soggetto cui l'informazione oggetto di trattamento si riferisce ha in particolare diritto al rispetto della propria identità personale o morale, a non vedere cioè "travisato o alterato all'esterno il proprio patrimonio intellettuale, politico, sociale, religioso, ideologico, professionale" (v. Cass., 22 giugno 1985, n.7769), e pertanto alla verità della propria immagine nel momento storico attuale.

Rispetto all'interesse del soggetto a non vedere ulteriormente divulgate notizie di cronaca che lo riguardano si pone peraltro l'ipotesi che sussista o subentri l'interesse pubblico alla relativa
conoscenza o divulgazione per particolari esigenze di carattere storico, didattico, culturale o più in generale deponenti per il persistente interesse sociale riguardo ad esse.

Un fatto di cronaca può, a tale stregua, assumere rilevanza quale fatto storico, il che può giustificare la permanenza del dato mediante la conservazione in archivi e diversi (es., archivio storico) da quello in cui esso è stato originariamente collocato.

Ai sensi del d.lgs. n.196/2003, art.11, comma 1, lett.b), i dati raccolti e trattati per una determinata finalità possono essere in effetti successivamente utilizzati per altri scopi, con la prima compatibilità.

Anche in tale ipotesi essi debbono essere peraltro trattati in modo lecito e secondo correttezza (d.lgs. n.196/2003, art.11, comma 1 lett.c) nonché conservati in forma che consente l'identificazione del soggetto cui gli stessi pertengono per un periodo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti e trattati (d.lgs. n.196/2003, art.11, comma 1 lett.e).

Atteso che come sopra indicato il principio di finalità costituisce un vero e proprio limite intrinseco del trattamento lecito dei dati personali, emerge allora la necessità, a salvaguardia dell'attuale identità sociale del soggetto cui la stessa afferisce, di garantire al medesimo la contestualizzazione e l'aggiornamento della notizia già di cronaca che lo riguarda, e cioè il collegamento della notizia ad altre informazioni successivamente pubblicate concernenti l'evoluzione della vicenda, che possano completare o financo radicalmente mutare il quadro evincendosi dalla notizia originaria, a fortiori se trattasi di fatti oggetto di vicenda giudiziaria, che costituisce anzi emblematico e paradigmatico esempio al riguardo.

Si pone peraltro in proposito la questione di delineare il quomodo della tutela, le modalità di relativa attuazione.

Va al riguardo altresì considerato che la notizia, sia essa collocata o meno in un archivio, può da soggetto che effettua il trattamento essere memorizzata anche nella rete Internet.

Deve allora prodromicamente distinguersi tra archivio e memoria della rete Internet.

Mentre l'archivio si caratterizza per essere ordinato secondo criteri determinati, con informazioni intercorrelate volte ad agevolare l'accesso e a consentirne la consultazione, la rete Internet costituisce in realtà un ente ove le informazioni non sono archiviate ma solo memorizzate.

Esso è dotato di una memoria illimitata e senza tempo, emblematico essendo al riguardo il comune riferimento al "mare di Internet", all'"oceano di memoria" in cui gli internauti "navigano".

La memoria della rete Internet non è un archivio, ma un deposito di archivi.

Nella rete Internet le informazioni non sono in realtà organizzate e strutturate, ma risultano isolate, poste tutte al medesimo livello ("appiattite"), senza una valutazione del relativo peso, e prive di contestualizzazione, prive di collegamento con altre informazioni pubblicate (come segnalato anche in dottrina, lo stesso pagerank indica quando una pagina è collegata da link, non a quali informazioni essa debba essere correlata, né fornisce alcun dato sulla qualità dell'informazione).

Si pone allora l'esigenza di attribuzione della fonte dell'informazione ad un soggetto, della relativa affidabilità, della qualità e della correttezza dell'informazione.

Al riguardo, a parte il rilievo che come osservato anche in dottrina sul piano pratico la pur possibile attività di cancellazione può essere ad esempio chiesta al motore di ricerca Google la rimozione di una pagina [...] o di un intero URL [...] non è comunemente posta in essere, non può invero nemmeno prescindersi dalla considerazione della circostanza della sussistenza di siti che memorizzano i dati scomparsi da altri siti (come, ad es., [...] il quale presta un servizio denominato Wayback machine).

Gli archivi sono dunque quelli dei singoli utenti che accedono alla Rete, dei titolari dei siti, che costituiscono infine la fonte dell'informazione (c.d. siti sorgente).

Il motore di ricerca è infatti un mero intermediario telematico, che offre un sistema automatico di reperimento di dati e informazioni attraverso parole chiave, un mero database che indica i testi sulla Rete e offre agli utenti un accesso per la relativa consultazione.

Esso è un mero fornitore del servizio di fruizione della rete, limitandosi a rendere accessibili sul sito web i dati dei c.d. siti sorgente, assolvendo ad un'attività di mero trasporto delle informazioni (ad eccezione dell'ipotesi in cui compia un'attività di trasformazione delle medesime, a tale stregua divenendone anch'esso produttore diretto, con conseguente assoggettamento a responsabilità in caso di illecito d.lgs. n.70/2003, ex art.14 e ss., [...]).
In particolare, come posto in rilievo nella giurisprudenza di merito, Google è notoriamente un motore di ricerca, che si limita a offrire ospitalità sui propri server a siti Internet gestiti dai relativi titolari in piena autonomia, i quali negli stessi immettono e memorizzano le informazioni oggetto di trattamento (cfr. Trib. Milano, 24 marzo 2011).

Al riguardo il motore di ricerca non svolge dunque un ruolo attivo (avendo peraltro il potere doveroso di impedirne la indicizzazione ed il posizionamento una volta venuto a conoscenza del contenuto illecito delle medesime contenute nei siti sorgente).

Il trascorrere del tempo assume d’altro canto rilievo con riferimento sia agli archivi del soggetto che accede alla rete Internet sia alla memoria di quest’ultima. Decisivo si appalesa al riguardo l’interesse pubblico alla conoscenza della notizia, sia essa di cronaca o storica.

A fronte dell’esigenza di garantire e mantenere la memoria dell’informazione si pone infatti, come detto, il diritto all’oblio del soggetto cui l’informazione si riferisce.

Se del dato è consentita la conservazione per finalità anche diversa da quella che ne ha originariamente giustificato il trattamento, con passaggio da un archivio ad un altro, nonché ammessa la memorizzazione (anche) nella rete di Internet (es., pubblicazione on-line degli archivi storici dei giornali), per altro verso al soggetto cui esso pertiene spetta un diritto di controllo a tutela della proiezione dinamica delle informazioni, che può tradursi, anche quando trattasi di notizia vera - e a fortiori se di cronaca - nella pretesa alla contestualizzazione e aggiornamento della notizia, e se del caso, avuto riguardo alla finalità della conservazione nell’archivio e all’interesse che la sottende, financo alla relativa cancellazione.

Ai fini della lecta a corretta utilizzazione dei dati è dunque anche in tal caso necessario che sussista una stretta correlazione temporale tra l’identificabilità del titolare dei dati e la finalità del relativo trattamento.

La finalità del trattamento condiziona la persistente identificabilità del soggetto titolare dei dati ma è a sua volta normativamente astretta dai rigorosi limiti temporali per i quali è giustificata ("per un periodo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati": d.lgs. n.196/2003, art.11, comma 1, lett.e).

Al riguardo, con riferimento alla rete Internet non si pone allora - diversamente da quanto affermato nell’impugnata sentenza - un problema di pubblicazione o di ripubblicazione dell’informazione, quanto bensì di permanenza della medesima nella memoria della rete Internet e, a monte, nell’archivio del titolare del sito sorgente.

Se il passaggio dei dati all’archivio storico è senz’altro ammissibile, ai fini della liceità e correttezza del relativo trattamento e della relativa diffusione a mezzo della rete Internet è indefettibilmente necessario che l’informazione e il dato trattato risultino debitamente integrati e aggiornati.

Anche in tal caso i dati debbono risultare "esatti" e "aggiornati", in relazione alla finalità del loro trattamento. A fortiori in caso di relativo inserimento in un archivio storico che come nella specie venga memorizzato pure nella rete di Internet la notizia non può continuare a risultare isolatamente trattata e non contestualizzata in relazione ai successivi sviluppi della medesima.

Ciò al fine di tutelare e rispettare la proiezione sociale dell’identità personale del soggetto, che come nel caso [...] costituisce invero proprio o essenzialmente lo scopo che fonda l’interesse pubblico, a sua volta a base della finalità del trattamento, alla persistente conoscenza della notizia.

Se pertanto come nella specie l’interesse pubblico alla persistente conoscenza di un fatto avvenuto in epoca (di molto) anteriore trova giustificazione nell’attività (nel caso, politica) svolta dal soggetto titolare dei dati, e tale vicenda ha registrato una successiva evoluzione, dalla notizia in ordine a quest’ultima non può invero prescindersi, giacché altrimenti la notizia, originariamente completa e vera, diviene non aggiornata, risultando quindi parziale e non esatta, e pertanto sostanzialmente non vera.

Se vera, esatta ed aggiornata essa era al momento del relativo trattamento quale notizia di cronaca, e come tale ha costituito oggetto di trattamento, il suo successivo spostamento in altro archivio di diverso scopo (nel caso, archivio storico) con memorizzazione anche nella rete Internet deve essere allora realizzato con modalità tali da consentire alla medesima di continuare a mantenere i suindici caratteri di verità ed esattezza, e conseguentemente di liceità e correttezza, mediante il relativo aggiornamento e contestualizzazione.
Solo in tal modo essa risulta infatti non violativa sia del diritto all'identità personale o morale del titolare, nella sua proiezione sociale, del dato oggetto di informazione e di trattamento, sia dello stesso diritto del cittadino utente a ricevere una completa e corretta informazione.

Anche laddove come nella specie non si ponga una questione di tutela contro la diffamazione o di protezione dell'immagine o dell'onore, sussiste allora in ogni caso l'esigenza di salvaguardare il diritto del soggetto al riconoscimento e godimento della propria attuale identità personale o morale.

Orbene, è il titolare del sito (nel caso, la controricorrente società Rcs Quotidiani s.p.a.), e non già il motore di ricerca (nel caso, Google), a dover provvedere al raggiungimento del suindicato obiettivo.

Senz'altro infondati sono allora l'assunto della società Rcs Quotidiani s.p.a. secondo cui la domanda "rivolta ai convenuti in tal senso è... palesemente mal indirizzata" e l'affermazione contenuta nell'impugnata sentenza che "la domanda non pare correttamente posta sotto il profilo soggettivo, non avendo parte ricorrente provveduto a citare quale legittimato passivo la società di gestione del motore di ricerca", e pertanto nella specie Google il giudice del merito ha al riguardo poi concluso che "peraltro, l'infondatezza nel merito di tale argomentazione (oltre che l'assenza di qualsivoglia richiesta in tal senso ad opera dei contraddittori) induceva il giudicante a ritenere il profilo processuale evidenziato assorbito".


Così come la rettifica è finalizzata a restaurare l'ordine del sistema informativo alterato dalla notizia non vera (che non produce nessuna nuova informazione), del pari l'integrazione e l'aggiornamento sono invero volti a ripristinare l'ordine del sistema alterato dalla notizia (storicamente o altrimenti) parziale.

L'aggiornamento ha in particolare riguardo all'inserimento di notizie successive o nuove rispetto a quelle esistenti al momento iniziale del trattamento, ed è volto a ripristinare la completezza e pertanto la verità della notizia, non più tale in ragione dell'evoluzione nel tempo della vicenda.

Orbene, atteso che non ricorrendo un'ipotesi di diffamazione o lesione dell'onore e della reputazione non viene nel caso in rilievo il rimedio della rettifica; e considerato per altro verso che, stante la sussistenza di persistente interesse pubblico alla conoscenza della ormai "storica" notizia in argomento ravvisata (diversamente da quanto sostenuto dall'odierno ricorrente) dal giudice di merito in considerazione della circostanza dell'essere l'odierno ricorrente "un possibile candidato politico in una delle ultime tornate elettorali" nonché "unico dei candidati in pectore per cariche, seppur non politiche, di rilievo pubblico", se non appare ammissibile farsi luogo al prospettato spostamento del la notizia di cronaca di cui trattasi in area non indicizzabile dai motori di ricerca, all'odierno ricorrente (che ha rinunziato all'originaria pretesa di blocco dei dati personali che lo riguardano) deve per converso senz'altro riconoscersi il diritto, a tutela della sua attuale identità personale o morale, al pure domandato (tempestivamente ed idoneamente in sede di ricorso introduttivo del giudizio avanti al Tribunale di Milano, non risultando d'altro canto dagli odierni controricorrenti nemmeno proposto ricorso incidentale con denunzia di errar in procedendo ex art.112 c.p.c., in riferimento all'art.360 c.p.c., comma 1, n.4) aggiornamento della notizia di cronaca de qua (pacificamente superato essendo d'altro canto rimasto l'originario improprio riferimento operato dal ricorrente ai "dati giudiziari").

Appare al riguardo invero necessaria una misura che consenta l'effettiva fruizione della notizia aggiornata, non potendo (diversamente da quanto affermato dal Garante nella memoria) considerarsi in proposito sufficiente la mera generica possibilità di rinvenire all'interno del "mare di Internet" ulteriori notizie concernenti il caso di specie, ma richiedendosi la predisposizione di sistema idoneo a segnalare (nel corpo o a margine) la sussistenza nel caso di un seguito e di uno sviluppo della notizia, e quale esso sia, consentendone il rapido ed agevole accesso ai fini del relativo adeguato approfondimento.

In caso di disaccordo tra le parti, spetta allora al giudice del merito individuare ed indicare le modalità da adottarsi in concreto per il conseguimento delle indicati finalità da parte del titolare dell'archivio e del sito web, salvo ed impregiudicata l'eventuale necessità per il medesimo di rivolgersi al gestore del motore di ricerca al fine di porre in essere le procedure tecnico-amministrative per la relativa attuazione su quest'ultimo.
Orbene, i suindicati principi risultano invero non osservati nell'impugnata sentenza.
In particolare là dove il giudice di merito afferma che "l'articolo di stampa in oggetto è pacificamente privo di carattere diffamatorio; le notizie potenzialmente lesive pubblicate risultano infatti scriminate, poiché costituiscono concreto esercizio del diritto di cronaca giudiziaria e di critica politica" sicché "ne discende quale ineludibile corollario che l'inserimento del detto articolo storico del [...] è del tutto lecito", non potendo "essere correttamente vantato il diritto all'oblio da parte del ricorrente" in quanto "nel caso di specie non si tratta di una nuova ed ulteriore veicolazione della vecchia notizia, ma del medesimo articolo, esaminabile, non già perché nuovamente ripubblicato ovvero citato in un diverso articolo di stampa pubblicato su un numero corrente del [...] ma solo attraverso l'accesso all'archivio del giornale, quale componente dell'archivio stesso".
Ancora, allorquando esso rileva "l'intrinseca contraddittorietà logica sussistente tra la richiesta applicazione del diritto ad essere dimenticato e l'ineludibile funzione - espressione della stessa ragione d'essere di una eremoteca - di offrire memoria storica delle vicende salienti di un'epoca, attraverso documenti redatti esercitando il diritto di cronaca giornalistica, non comprimibile, se non nei limiti di legge". Ritiene non sostenibile "che ad ogni accesso ad un articolo storico corrisponda una nuova pubblicazione a mezzo stampa della notizia ... non potendosi far discendere dalle concrete modalità di accesso alla fonte storica una differente autonoma valenza della stessa". Sottolinea che la "medesima difesa sti-
centa ragione d'essere di una eremoteca - di offrire memoria storica delle vicende salienti di un'epoca, attraverso documenti redatti esercitando il diritto di cronaca giornalistica, non comprimibile, se non nei limiti di legge". Ritiene non sostenibile "che ad ogni accesso ad un articolo storico corrisponda una nuova pubblicazione a mezzo stampa della notizia ... non potendosi far discendere dalle concrete modalità di accesso alla fonte storica una differente autonoma valenza della stessa". Sottolinea che la "medesima difesa sti-

- Anche in caso di memorizzazione nella rete Internet, mero deposito di archivi dei singoli utenti che accedono alla rete e cioè dei titolari dei siti costituenti la fonte dell'informazione (c.d. siti sorgente), deve riconoscersi al soggetto cui pertengono i dati personali oggetto di trattamento ivi contenuti il diritto all'oblio, e cioè al relativo controllo a tutela della propria immagine sociale, che anche quando trattasi di notizia vera, e a fortiori se di cronaca, può tradursi nella pretesa alla contestualizzazione e aggiornamento dei medesimi, e se del caso, avuto riguardo alla finalità della conservazione nell'archivio e all'interesse che la sottende, financo alla relativa cancellazione.

- In ipotesi, come nella specie, di trasferimento, ex art.11, comma 1, lett.b), del d.lgs. n.196/2003, di notizia già di cronaca (nel caso, relativa a vicenda giudiziaria di personaggio politico) nel proprio archivio storico, il titolare dell'organo di informazione (nel caso, la società Rcs Quotidiani s.p.a.) che avvalendosi di un motore di ricerca (nel caso, Google) memorizza la medesima anche nella rete Internet è tenuto ad osservare i criteri di proporzionalità, necessità, pertinenza e non eccedenza dell'informazione, avuto riguardo alla finalità che ne consente illecito trattamento, nonché a garantire la contestualizzazione e l'aggiornamento della notizia già di cronaca oggetto di informazione e di trattamento, a tutela del diritto del soggetto cui i dati pertengono alla propria identità personale o morale nella sua proiezione sociale, nonché a salvaguardia del diritto del cittadino utente di ricevere una completa e corretta informazione, non essendo al riguardo sufficiente la mera generica possibilità di rinvenire all'interno del "mare di Internet" ulteriori notizie concernenti il caso di specie, ma richiedendosi, atteso il raviviso istantaneo interesse pubblico alla conoscenza della notizia in argomento, la predisposizione di sistema idoneo a segnalare (nel corpo o a margine) la sussistenza di un seguito e di uno sviluppo della notizia, e quale esso sia stato (nel caso, dei termini della intervenuta relativa definizione in via giudiziaria), consentendone il rapido ed agevole accesso da parte degli utenti ai fini del relativamente adeguato approfondimento, giusta modalità operative stabilite, in mancanza di accordo tra le parti, dal giudice di merito.

[…] P.Q.M.

La Corte accoglie il ricorso. Cassa l'impugnata sentenza e rinvia, anche per le spese del giudizio di cassazione al Tribunale di Milano, in diversa composizione.

*****

DISCUSSIONE

1. Quali sono i criteri utilizzabili per bilanciare diritto alla riservatezza da un lato e libertà di espressione e diritto all’informazione dall’altro?

2. In cosa consiste la distinzione, proposta nella sentenza in esame, tra archivio da un lato e memoria di Internet dall’altro? Siete d’accordo con tale distinzione? In cosa consiste la memoria di Internet e quali sono le sue caratteristiche?

3. Come viene definito Google, in qualità di motore di ricerca? Siete d’accordo?

4. Nel caso in esame si può parlare di diritto all’oblio?

5. Cosa intende la Corte di Cassazione per contestualizzazione e aggiornamento?


*****

NORME

- art.21, Cost.
- art.8, Carta dei diritti fondamentali dell’Unione Europea
- artt.2, 7, 11, d.lgs. n.196/2003
10.2. Testata giornalistica telematica e sequestro preventivo

Corte di Cassazione, sez.un. penali, 29 gennaio 2015, n.31022

Ritenuto in fatto


Il Giudice del riesame, dopo avere, in via preliminare, risolto positivamente la sollevata questione della competenza per territorio, facendo leva sulla regola suppletiva di cui all'art.9, comma 3, c.p.p. (prima iscrizione della notizia di reato), riteneva sussistenti sia il fumus commissi delicti, insito nella dettagliata ed eloquente contestazione in fatto elevata dal p.m. sulla base delle univoche insinuazioni diffamatorie contenute nell'articolo incriminato, sia il periculum in mora, desumibile dalla libera disponibilità in rete della corrispondente pagina telematica, che avrebbe potuto «concretamente aggravare le conseguenze dannose del reato».

3. Avverso la pronuncia di riesame hanno proposto ricorso per cassazione, tramite i loro difensori, gli indagati, sviluppando due articolati e analitici motivi.


Stigmatizzano l'omessa considerazione dei motivi di riesame, con i quali si era specificamente contestata la legittimità del provvedimento di sequestro, per lesione del diritto costituzionale di libera manifestazione del pensiero e della libertà di stampa.

Aggiungono che non poteva essere condiviso l'arresto della giurisprudenza di legittimità (sez.V, n.10594 del 5 novembre 2013, [...], Montanari) circa l'ammissibilità del sequestro preventivo di articoli giornalistici on line, misura che sarebbe legittimata dalla considerazione che gli spazi comunicativi sul web non godono della stessa protezione accordata alla stampa. Tale orientamento non considerava che la testata telematica regolarmente registrata è «un giornale a tutti gli effetti»; il mezzo elettronico e la rete costituiscono soltanto una «modalità di diffusione aggiuntiva rispetto a quella tradizionale cartacea», con l'effetto che doveva privilegiarsi una interpretazione costituzionalmente orientata della disciplina sulla stampa.

5. Quest'ultima Sezione, con ordinanza 3 ottobre 2014 [...] osserva che il sollecitato scrutinio di legittimità della pronuncia del Tribunale del riesame impone la soluzione preliminare di due
questioni di diritto, strettamente connesse tra loro: a) la prima, di carattere generale, concerne la stessa possibilità giuridica di disporre il sequestro preventivo di risorse telematiche, posto che la cautela si risolverebbe non nella materiale apprensione della cosa pertinente al reato, bensì nell'imposizione all'indagato o all'imputato o a terzi di un facere, consistente nel compimento delle operazioni tecniche necessarie per "oscurare" e rendere, quindi, inaccessibile agli utenti, ove ne ricorrano i presupposti, un intero sito o una pagina web; b) una volta risolta positivamente tale prima questione, residua quella ulteriore dell'ammisibilità del sequestro preventivo della pagina web di una testata giornalistica telematica debitamente registrata.

In relazione al primo tema, la Sezione rimettente, dopo avere dato atto che la giurisprudenza di legittimità era pacificamente orientata, pur senza particolari approfondimenti, nel senso dell'ammisibilità del sequestro preventivo mediante oscuramento di interi siti internet o di singole pagine web, manifesta perplessità sulla possibilità di imporre, a scopo preventivo, all'indagato, all'imputato o a terzi privati il compimento di attività tecniche necessarie per impedire l'accesso al sito o alla pagina web, oggetto di sequestro, e ciò perché la normativa sulla cautela reale, tipizzata e disciplinata dagli artt.321 c.p.p. e 104 disp. att. c.p.p., implica l'adprehensio, in senso materiale o giuridico, della res con il connesso vincolo d'indisponibilità della stessa e non già l'imposizione esclusiva di un facere.

Aggiunge che il legislatore, con la norma di cui all'art.254-bis c.p.p., disciplina il sequestro probatorio di dati informatici presso fornitori di servizi informatici, telematici e di telecomunicazioni, ma analoga previsione non è rinvenibile in materia di sequestro preventivo.

Con riferimento al secondo tema, contesta l'orientamento interpretativo espresso da sez.V, n.10594 del 5 novembre 2013, [...], Montanari, che aveva escluso la possibilità di applicare, in via estensiva o analogica, la normativa sulle guarentigie per la stampa ai giornali telematici.

Osserva che il principio costituzionale della libertà di manifestazione del pensiero con ogni mezzo di diffusione deve indurre, invece, ad equiparare il giornale on line a quello tradizionale e a ravvisare, sul piano logico-giuridico, la eadem ratio ai fini dell'applicazione delle relative guarentigie, con l'effetto che deve ritenersi inibito, salvo le eccezioni espressamente previste, il sequestro preventivo del prodotto editoriale telematico, destinatario peraltro, al pari della stampa tradizionale, delle provvidenze di cui alla l. n.62 del 2001.

Poiché entrambi i temi dibattuti potevano dare luogo a contrasto giurisprudenziale rispetto agli orientamenti già espressi in sede di legittimità, la Prima Sezione ha rimesso d'ufficio, ai sensi dell'art.618 c.p.p., i ricorsi alle Sezioni Unite.

[...] Considerato in diritto

1. Le questioni di diritto delle quali sono investite le Sezioni Unite sono le seguenti:
   - «Se sia ammissibile il sequestro preventivo, anche parziale, di un sito web»;
   - «Se sia ammissibile, al di fuori dei casi espressamente previsti dalla legge, il sequestro preventivo della pagina web di una testata giornalistica telematica debitamente registrata».

2. La prima questione, di carattere generale, concerne la possibilità giuridica di disporre, per contrastare reati commessi nella rete internet, il sequestro preventivo delle risorse informatiche o telematiche d'interesse.

La tematica, pur non espressamente dedotta dai ricorrenti, deve comunque essere esaminata, in quanto strettamente connessa alla specifica questione che viene qui in rilievo e che presuppone - al di là degli ulteriori problemi ermeneutici coinvolti e di cui si dirà in seguito - la positiva soluzione della prima.

2.1. La Sezione rimettente manifesta perplessità al riguardo, evidenziando che in questo caso la misura cautelare, contrariamente a quanto tipizzato e disciplinato dagli artt.321 c.p.p. e 104 disp. att. c.p.p., si concretizzerebbe non nella materiale apprensione della cosa pertinente al reato o nella indisponibilità giuridica della stessa, bensì nell'imposizione all'indagato, all'imputato ovvero a terzi di un facere, consistente nel compimento delle operazioni tecniche necessarie per oscurare e rendere, quindi, inaccessibile agli utenti la visione del sito o della pagina web incriminati. Ciò tradirebbe la natura reale della cautela, che si trasformerebbe in una inibitoria atipica con effetti obbligatori, il che violerebbe il principio di legalità processuale.

2.2. Non mancano, in verità, decisioni di questa Corte che, sia pure analizzando casi differenti (in materia di sequestro di documenti) da quello in esame, escludono la possibilità di perseguire, attraverso l'adozione del sequestro preventivo, la finalità di inibire l'esercizio di determinate attività.
Si è affermato, infatti, che il sequestro preventivo può avere ad oggetto solo il risultato di un'attività e non l'attività in sé, perché è estranea ad esso la funzione di inibizione di comportamenti, sicché è illegittimo, risolvendosi peraltro nell'indebita invasione della sfera di attribuzioni della giurisdizione civile, se il sequestro di un fascicolo processuale relativo all'esecuzione immobiliare in corso nei confronti di un soggetto vittima difatti estorsivi, finalizzato ad impedire che il reato sia portato ad ulteriori conseguenze (sez.II, n.10437 del 9 marzo 2006, Sindona, [...]). Con il sequestro preventivo non è possibile imporre al destinatario un facere, atteso che tale misura cautelare reale mira esclusivamente al congelamento della situazione pericolosa (sez.III, n.11275 del 17 gennaio 2002, Palmieri, [...]) e non è destinata a svolgere una atipica funzione inibitoria di comportamenti rilevanti sul piano penale, essendo predisposti, a tal fine, istituti di natura diversa, quali l'arresto o il ferro (sez.VI, n.4016 del 14 dicembre 1998, dep. 1999, Bottani, [...]).


Difettano, però, in tali decisioni, a giustificazione della tesi sostenuta, che pur si ritiene corretta, il necessario grado di approfondimento del tema specifico e una completa ricostruzione del quadro normativo di riferimento.

S'impone, pertanto, un esame analitico delle ragioni che giustificano il sequestro preventivo di risorse informatiche o telematiche pertinenti al reato, quando la libera disponibilità delle stesse possa aggravare o protrarre le conseguenze di esso ovvero agevolare la commissione di altri reati.

3. L'art.321 c.p.p. disciplina il sequestro preventivo, stabilendo testualmente, al comma 1, che «Quando vi è pericolo che la libera disponibilità di una cosa pertinente al reato possa aggravare o protrarre le conseguenze di esso ovvero agevolare la commissione di altri reati, a richiesta del pubblico ministero il giudice competente a pronunciarsi nel merito ne dispone il sequestro con decreto motivato. Prima dell'esercizio dell'azione penale provvede il giudice per le indagini preliminari». Ai sensi del successivo comma 3-bis, nel corso delle indagini preliminari, di fronte a una situazione di urgenza, il sequestro è disposto dal pubblico ministero; prima dell'intervento di costui e nella stessa situazione di urgenza, al sequestro procedono ufficiali di polizia giudiziaria; in questi due casi, devono fare seguito la convalida e l'emissione del decreto di cui al comma 1 da parte del giudice. È previsto anche (comma 2) il sequestro preventivo della cosa pericolosa in sé, essendone consentita o imposta la confisca.

Analizzando i presupposti di questa figura di sequestro, appare evidente che essa sia caratterizzata da un immediato fine di prevenzione. Trattasi di sequestro designato come "impeditivo" e tendenzialmente orientato ad operare, pur non perdendo la sua connotazione "reale", come inibitoria, in quanto caratterizzato - come si è precisato in dottrina - da finalità di difesa sociale perché «il vincolo diretto a rendere indisponibile la cosa è imposto per le generali esigenze di giustizia, quali sono quelle di tutela della collettività».

[...]

4. Ciò posto, deve rilevarsi che il caso sottoposto all'attenzione delle Sezioni Unite si connota per la particolarità dell'oggetto della coercizione reale.

Tale oggetto, almeno in apparenza, non si apprezza come una entità del mondo fisico, suscettibile di apprezzamento, possesso e custodia (id quod tangi potest), trattandosi di un prodotto del pensiero umano che circola liberamente nella rete telematica in forma dematerializzata.

Il sequestro preventivo di risorse telematiche o informatiche diffuse sul web implica un intervento sul prestatore di servizio (Internet Service Provider), perché impedisca l'accesso al sito o alla singola pagina ovvero disponga il blocco o la cancellazione del file incriminato; tanto comporta inevitabilmente l'inibitoria di una determinata attività.

[...]

4.2. Il codice di procedura penale vigente ha previsto e disciplinato l'istituto del sequestro preventivo, che, di fronte ad illeciti penali commessi nell'ambito dello spazio riservato ai nuovi
modelli comunicativi e alle innovative modalità di fruizione dei beni immateriali, è destinato ad operare anche con effetti inibitori.

La misura cautelare, in questa nuova realtà, non può limitarsi a porre un vincolo d'indisponibilità su di una cosa, tenuto conto che tale vincolo è comunque implicato nell'agire contra legem della persona, alla quale, per garantire l'effettività della cautela, devono necessariamente essere inibite le corrispondenti attività pericolose realizzabili mediante la disponibilità del bene. E ciò a superamento del riferimento riduttivo e anacronistico alla sola cosa materiale, per dare il necessario risalto al prodotto intellettuale in essa incorporato, che costituisce l'oggetto primario del vincolo d'indisponibilità.

Devesi quindi stabilire se tutto ciò sia compatibile col principio di legalità processuale, considerato che il sequestro di cui all'art.321 c.p.p. ha una evidente natura reale e comporta, pertanto, la materiale apprensione della cosa pertinente al reato. In altri termini, è necessario chiarire se il dato informatico in quanto tale abbia una sua fiscilità, rientri nel concetto di "cosa" e possa essere oggetto di coercizione reale.

5. Internet non è un luogo, né uno spazio, ma una metodologia di comunicazione ipertestuale che consente l'accesso a qualsiasi contenuto digitale posto su sistemi informatici connessi alla rete.

La dimensione fisica delle informazioni reperibili attraverso la rete telematica consiste nella struttura di ciascun file e si radica spazialmente nel computer, al cui interno il documento è materialmente memorizzato.

I documenti reperibili in rete non sono altro che files (registrazioni magnetiche o ottiche di bytes) registrati all'interno dei server degli Internet Service Providers ovvero sui computers degli utenti, utilizzando un sia pure intesimale spazio fisico. Il dato informatico, quindi, è incorporato sempre in un supporto fisico, anche se la sua fruizione attraverso la rete fa perdere di vista la sua "fiscilità". Al supporto fisico di memorizzazione si fa specifico riferimento nel Codice dell'amministrazione digitale (d.lgs. 7 marzo 2005, n.82) nella parte in cui disciplina la conservazione sicura dei dati e ne garantisce, quindi, la protezione e l'immutabilità (artt.1, 43, 44).

La visualizzazione dei suddetti documenti non avviene "da remoto", ma nel computer di ciascun utente, attraverso il programma browser, che, una volta individuato il documento, lo preleva, lo copia e lo rende così visibile.

6. Devesi, inoltre, sottolineare che, a seguito dell'entrata in vigore della l. 18 marzo 2008, n.48, di ratifica della Convenzione del Consiglio d'Europa, fatta a Budapest il 23 novembre 2001, sulla criminalità informatica (cybercrime) e di adeguamento del nostro ordinamento agli impegni assunti con la medesima Convenzione, il dato informatico è esplicitamente equiparato al concetto di "cosa", che, se pertinente al reato, può essere oggetto di sequestro.

La Convenzione, infatti, dopo avere definito all'art.1 il concetto di "dato informatico", disciplina nel successivo art.19 «Perquisizione e sequestro di dati informatici immagazzinati», stabilendo che «Ogni Parte deve adottare le misure legislative e di altra natura che dovessero essere necessarie per consentire alle proprie autorità competenti di sequestrare o acquisire in modo simile i dati informatici per i quali si è proceduto all'accesso [...]. Tali misure devono includere il potere di: a) sequestrare o acquisire in modo simile un sistema informatico o parte di esso o un supporto per la conservazione di dati informatici; b) fare e trattenere una copia di quei dati informatici; c) mantenere l'integrità dei relativi dati informatici immagazzinati; d) rendere inaccessibile o rimuovere quei dati dal sistema informatico analizzato». Al termine "sequestrare" è affiancata l'espressione "acquisire in modo simile", indicativa, come si legge nella relazione esplicativa del Comitato dei ministri del Consiglio d'Europa, degli altri modi con i quali i dati intangibili possono essere resi indisponibili (renderli cioè inaccessibili o rimuoverli dal sistema).

Le modifiche apportate, in esecuzione di tale Convenzione, dalla l. n.48 del 2008 al codice penale e a quello di procedura penale confermano l'assimilazione del dato informatico alle "cose".

[...]

Anche le innovazioni introdotte nel codice di rito, con riferimento alle norme relative ai mezzi di ricerca della prova e all'attività a iniziativa della giudiziaria, evidenziano chiaramente che il dato informatico è normativamente equiparato a un oggetto "fisico".

La l. n.48 del 2008 (cfr. artt.8 e 9) ha rimodulato disposizioni già vigenti, come il sequestro di oggetti di corrispondenza «anche se inoltrati per via telematica» (art.254, comma 1, c.p.p.); ha introdotto nuove disposizioni, come il sequestro di dati informatici presso fornitori di servizi informatici, telematici e di telecomunicazioni (art.254-bis c.p.p.); ha sottoposto, inoltre, ad
un'operazione di "chirurgia lessicale" numerose altre disposizioni processuali, ampliandone l'oggetto attraverso l'inserimento di espressioni che rimandano ad attività connesse a «dati, informazioni e programmi informatici»: il riferimento è alla materia di ispezioni e rilievi tecnici (art.244, comma 2, c.p.p.), all'esame di atti, documenti e corrispondenza presso banche (art.248, comma 2, c.p.p.), ai doveri di esibizione e consegna (art.256, comma 1, c.p.p.), agli obblighi e alle modalità di custodia (art.259, comma 2, c.p.p.), ai sigilli e ai vincoli delle cose sequestrate (art.260, commi 1 e 2, c.p.p.), all'acquisizione di plichi e corrispondenza ad iniziativa della polizia giudiziaria (art.353, comma 3, c.p.p.) e, infine, agli accertamenti urgenti e al sequestro ad opera sempre della polizia giudiziaria (art.354, comma 2, c.p.p.).

6.1. Al di là della discutibile scelta sul metodo emendativo seguito, deve ritenersi ormai per definitivamente acquisito che il dato informatico in sé, in quanto normativamente equiparato a una "cosa", può essere oggetto di sequestro, da eseguirsi, avuto riguardo al caso concreto, secondo quanto in esse previsto, dal legislatore e nel rispetto del principio di proporzionalità.

[...] 6.3. A questo punto, però, devono individuarsi, nel rispetto del principio di legalità processuale, le concrete modalità esecutive della cautela reale che ha ad oggetto risorse telematiche o informatiche, non essendo rinvenibile nel codice di rito alcuna norma analoga a quella prevista per il sequestro probatorio (art.254-bis c.p.p.).

Nel contesto della realtà digitale della rete, devesi stabilire, in sostanza, se il sequestro preventivo debba essere limitato alla sola adprehensio in senso fisico della "cosa" o piuttosto debba concretizzarsi, tenuto conto della peculiare realtà nella quale va ad incidere, in una vera e propria inibitoria rivolta al fornitore di connettività, che deve impedire agli utenti l'accesso al sito o alla singola pagina web incriminati ovvero rimuovere il file che viene in rilievo, con l'effetto di arrestare l'attività criminosa in atto o scongiurare la commissione di ulteriori condotte illecite.

7. Ritiene il Collegio che il sequestro preventivo di risorse telematiche o informatiche sia conforme con la detta inibitoria, la sola in grado di assicurare "effettività" alla cautela.

Soccorre al riguardo, sul piano normativo, il d.lgs. 9 aprile 2003, n.70, che, in attuazione della Direttiva n.2000/31/CE, ha regolamentato taluni aspetti giuridici dei servizi della società dell'informazione nel mercato interno, con particolare riferimento al commercio elettronico.

L'intera gamma dei servizi di rete è disciplinata nel citato decreto legislativo. Questo si occupa, all'art.14, dell'attività di semplice trasporto, vale a dire della diffusione in rete delle informazioni fornite da un destinatario del servizio (mere conduit); all'art.15, dell'attività di memorizzazione automatica, intermedia e temporanea (caching) delle informazioni fornite dall'utente e trasmesse in rete al solo scopo di rendere più efficace il successivo inoltro a destinatari che ne fanno richiesta; all'art.16, dell'attività di memorizzazione, con caratteri di tendenziale stabilità, delle informazioni (hosting).

L'ultimo comma delle tre norme richiamate, riproducendo pedissequamente il contenuto della Direttiva comunitaria (artt.12, 13 e 14), prevede che l'autorità giudiziaria o quella amministrativa con funzioni di vigilanza può esigere, anche in via di urgenza, che il prestatore di un servizio della società dell'informazione (ossia l'Internet Service Provider) «impedisca o ponga fine alle violazioni».

Il successivo art.17, comma 3, inoltre, contempla che l'autorità giudiziaria può richiedere al detto prestatore di inibire l'accesso al contenuto illecito del servizio offerto.

Come correttamente rilevato da sez.III, n.49437 del 29 settembre 2009, Sunde Kolmisoppi (decisione di ampio respiro in tema di copyright), la lettura congiunta e coordinata di tutte le citate disposizioni consente di affermare che quanto in esse previsto, imponendo, per effetto della richiesta dell'autorità giudiziaria, un obbligo di attivazione da parte del prestatore dei servizi telematici, delinea una vera e propria inibitoria.

Ed invero, il meccanismo processuale, attraverso il quale si consegue l'obiettivo di paralizzare la protrazione delle conseguenze dannose del reato o il rischio di reiterazione dell'attività criminosa, implica un duplice intervento: 1) il sequestro preventivo con cui s'impone al fornitore dei servizi telematici di bloccare l'accesso agli utenti alle risorse elettroniche incriminate; 2) l'intervento tecnico di tale fornitore, che deve rendere, operando in modo consequenziale, concretamente indisponibili tali risorse.

Gli artt.14, 15, 16 e 17 del d.lgs. n.70 del 2003 integrano, con riferimento alla specifica materia disciplinata, il contenuto dell'art.321 c.p.p. e consentono di superare qualunque riserva.
corta la possibilità di sottoporre a sequestro preventivo dati informatici che circolano in rete in forma dematerializzata. Tale misura cautelare, per conseguire lo scopo che le è proprio, deve implicare necessariamente l'inibitoria dell'attività criminosa in atto.

[...] Conclusivamente, nell'ambito del mondo digitale, il sequestro preventivo, ove ne ricorrano i presupposti, investe direttamente la disponibilità delle risorse telematiche o informatiche d'interesse, equiparate normativamente a "cose", e ridonda, solo come conseguenza, anche in inibizione di attività, per garantire concreta incisività alla misura. Questa, quindi, non tradisce la sua connotazione di cautela reale e non si pone comunque, anche in relazione al suo risvolto inibitorio, al di fuori della legalità, tenuto conto delle specifiche previsioni normative di cui al d.lgs. n.70 del 2003.

Né va sottaciuto che la normativa comunitaria è costantemente orientata nel senso di riconoscere espressamente che l'oscuramento di interi siti web o di singole pagine telematiche con contenuti illeciti è un efficace strumento di contrasto alla criminalità informatica: non è superfluo ricordare l'art.25 della Direttiva 2011/93/UE sulla pedopornografia, alla quale si è data attuazione nell'ordinamento interno con il d.lgs. 4 marzo 2014, n.39.

8. Alla luce delle argomentazioni sin qui sviluppate, deve enunciarsi il seguente principio di diritto:

- "Ove ricorrano i presupposti del fumus commissi delicti e del periculum in mora, è ammissibile, nel rispetto del principio di proporzionalità, il sequestro preventivo ex art.321 c.p.p. di un sito web o di una singola pagina telematica, anche imponendo al fornitore dei relativi servizi di attivarsi per rendere inaccessibile il sito o la specifica risorsa telematica incriminata".

9. Risolto positivamente tale problema di carattere generale, deve ora essere esaminata l'ulteriore questione dell'ammissibilità o meno del sequestro preventivo di una testata giornalistica on line regolarmente registrata o di una determinata pagina web di detta testata.

È questo il tema di specifico interesse per la soluzione del caso portato all'attenzione delle Sezioni Unite.

10. La libertà di stampa è un principio cardine su cui si fonda lo Stato democratico.

L'art.21 della Costituzione, dopo avere riconosciuto nel primo comma il diritto di libera manifestazione del pensiero con ogni mezzo di diffusione, riserva le previsioni dei commi successivi specificamente alla stampa.

[...]

13. La Costituzione repubblicana, entrata in vigore il 1° gennaio 1948, proclama testualmente all'art.21:

«Tutti hanno diritto di manifestare liberamente il proprio pensiero con la parola, lo scritto e ogni altro mezzo di diffusione. La stampa non può essere soggetta ad autorizzazioni o censure. Si può procedere a sequestro soltanto per atto motivato dell'autorità giudiziaria nel caso di delitti, per i quali la legge sulla stampa espressamente lo autorizzi, o nel caso di violazione delle norme che la legge stessa prescriva per l'indicazione dei responsabili. In tali casi, quando vi sia assoluta urgenza e non sia possibile il tempestivo intervento dell'autorità giudiziaria, il sequestro della stampa periodica può essere eseguito da ufficiali di polizia giudiziaria, che devono immediatamente, e non mai oltre ventiquattro ore, fare denunzia all'autorità giudiziaria. Se questa non lo convalida nelle ventiquattro ore successive, il sequestro s'intende revocato e privo d'ogni effetto. La legge può stabilire, con norme di carattere generale, che siano resi noti i mezzi di finanziamento della stampa periodica. Sono vietate le pubblicazioni a stampa, gli spettacoli e tutte le altre manifestazioni contrarie al buon costume. La legge stabilisce provvedimenti adeguati a prevenire e a reprimere le violazioni».

L'Assemblea costituente, in attuazione della XVII disposizione transitoria della Carta fondamentale, varò anche la l. 8 febbraio 1948, n.47, intitolata "Disposizioni sulla stampa".

I due eventi sono da raccordare e si integrano tra loro.

L'art.21, secondo comma, Cost. sancisce che la stampa non può essere soggetta ad autorizzazioni o censure. Il termine "stampa" compare per la prima volta nel dettato costituzionale e l'art.1 della l. n.47 del 1948 precisa che sono da considerarsi stampe o stampati «tutte le riproduzioni tipografiche o comunque ottenute con mezzi meccanici o fisico-chimici, in qualsiasi modo destinate alla pubblicazione».

L'art.2 della stessa legge disciplina le indicazioni obbligatorie sugli stampati, finalizzate a individuare i responsabili di eventuali illeciti. La previsione del successivo art.5 circa l'obbligo di
registrazione della stampa periodica presso la cancelleria del competente Tribunale non è in contrasto con il dettato costituzionale della non assoggettabilità della stampa ad autorizzazioni, considerato che non v'è alcun margine di discrezionalità dell'organo competente a ordinare l'iscrizione del giornale nell'apposito registro, ove la documentazione presentata sia regolare (Corte cost., sentt. n.31 del 1957).

L'art.21, terzo comma, Cost., disciplina l'istituto del sequestro, sottoponendolo alla duplice garanzia della riserva di legge e di giurisdizione.

Il sequestro della stampa può essere disposto, con atto motivato dell'autorità giudiziaria, soltanto nel caso di delitti per i quali la legge sulla stampa espressamente lo autorizzi o nel caso di stampa clandestina. Il riferimento alla legge sulla stampa non introduce una riserva qualificata di legge, ma è indicativo del complesso delle norme riguardanti la materia (Corte cost., sentt. n.4 del 1972 e n.60 del 1976).

I casi nei quali le leggi vigenti consentono il sequestro preventivo sono: a) violazione delle norme sulla registrazione delle pubblicazioni periodiche e sull'indicazione dei responsabili (artt.3 e 16 l. n.47 del 1948); b) stampati osceni o offensivi della pubblica decenza ovvero divulganti mezzi atti a procurare l'aborto (art.2 r.d.lgs. n.561 del 1946); c) stampa periodica che faccia apologia del fascismo (art.8 l. 20 giugno 1952, n.645); d) violazione delle norme a protezione del diritto d'autore (art.161 l. 22 aprile 1941, n.633).

La disciplina costituzionale differenzia la stampa periodica da quella comune e ulteriori differenze sono rinvenibili nella l. n.47 del 1948, che rende gli adempimenti relativi alla stampa periodica (indicazioni obbligatorie, obbligo di registrazione) più gravosi rispetto a quelli previsti per la stampa comune.

L'art.8 della l. n.47 del 1948 introduce il nuovo istituto della rettifica, estraneo alla precedente normativa.

La legge sulla stampa, inoltre, non ha modificato la disciplina codicistica dei reati che possono essere commessi attraverso l'esercizio dell'attività giornalistica, ma si è limitata a introdurre nell'ordinamento la categoria dei "reati di stampa" (art.16 sulla stampa clandestina) e a integrare le previsioni concernenti i reati a mezzo stampa (artt.13, 14, 15).

Per i reati commessi a mezzo della stampa periodica, la responsabilità penale grava non solo sull'autore dell'articolo incriminato ma anche sul direttore o vice-direttore responsabile, il quale risponde per fatto proprio a titolo di culpa in vigilando (art.57 c.p., come sostituito dall'art.1 della l. 4 marzo 1958, n.127), escludendosi qualsiasi forma di responsabilità di tipo oggettivo o - per così dire - "di posizione", come accadeva in epoca fascista.

Numerosi interventi normativi susseguitisi nel tempo prevedono, infine, in attuazione dell'art.21, comma quinto, Cost., finanziamenti pubblici in favore dell'editoria giornalistica, nella prospettiva di garantire il massimo pluralismo dell'informazione e arginare fenomeni concentrzionistici.

14. La disciplina costituzionale della libertà di informazione (art.21) - già arricchita nella sua interpretazione dall'art.19 della Dichiarazione Universale dei Diritti dell'Uomo, approvata dall'Assemblea generale delle Nazioni Unite nel 1948 - è oggi completata dalle disposizioni della Convenzione Europea dei Diritti dell'Uomo (CEDU), che, all'art.10, riconosce espressa tutela ai profili attivi e passivi della libertà di manifestazione del pensiero.


15. All'esito di tale excursus storico sulla normativa d'interesse, può affermarsi che l'Italia democratica - a differenza di quanto accaduto per lo Statuto Albertino e l'Editto sulla stampa, che rappresentarono una elargizione del Sovrano ai sudditi - ha guadagnato da sé la Costituzione e la legge sulla stampa, reagendo al ventennio fascista, in cui ogni forma di libertà era stata sospesa in attuazione di un preciso disegno politico volto a controllare, in particolare, il settore dell'informazione, per assicurarsi il consenso dell'opinione pubblica.

La Carta Fondamentale, in antitesi con l'impostazione dirigistica e repressiva propria del regime fascista, garantisce il principio della libera manifestazione del pensiero e non consente che
la stampa possa essere soggetta ad autorizzazioni o censure. La libertà di stampa è condizione imprescindibile per il libero confronto di idee, nel quale la democrazia affonda le sue radici, e per la formazione di un'opinione pubblica avvertita e consapevole.

Sulla base di tali principi, il Costituente - come innanzi si è precisato - ha accordato alla "stampa" una specifica e rafforzata tutela (art.21, terzo comma), inibendo, nel caso di delitti commessi con tale mezzo, il ricorso all'istituto del sequestro preventivo se non nelle ipotesi tassativamente previste, come eccezioni, dalla legge.

Esemplicando, l'offensività della condotta diffamatoria a mezzo stampa, proprio perché considerata normativamente repressiva, nel bilanciamento di valori, rispetto alla salvaguardia della libertà d'informazione, non può legittimare l'adozione della misura cautelare reale; ad opposta conclusione deve pervenirsi in ipotesi di pubblicazioni a contenuto osceno ovvero contrario alla pubblica decenza o al buon costume, considerato che la tutela del corrispondente bene giuridico protetto prevala, per espressa previsione del legislatore (art.2 r.d.lgs. n.561 del 1946; art.21, sesto comma, Cost.), su quella della libertà di stampa.

16. L'operatività della disciplina costituzionale, così come compatibilmente integrata dalla legislazione ordinaria, in materia di sequestro preventivo della stampa risulta per lo più condizionata dalla definizione che di questa si rinviene nella l. n.47 del 1948, la quale, senza occuparsì in alcun modo della materia cautelare, regola i presupposti di realizzazione e diffusione della stampa, chiarendo che per tale si considerano le riproduzioni tipografiche o comunque ottenute con mezzi meccanici o fisico-chimici in qualsiasi modo destinate alla pubblicazione (art.1).

I più recenti arresti giurisprudenziali di questa Corte Suprema (sez.V, n.10594 del 5 novembre 2013, [...], Montanari) e voci autorevoli della dottrina ritengono che le garanzie costituzionali in tema di sequestro preventivo della stampa non siano estensibili alle manifestazioni del pensiero destinate ad essere trasmesse in via telematica, ivi comprese quelle oggetto di articoli giornalistici pubblicati sul web, e ciò perché il termine "stampa" sarebbe stato assunto dalla norma costituzionale nella accezione tecnica innanzi precisata, vale a dire con riferimento alla sola "carta stampata".

A conforto di tale opzione ermeneutica, si è evidenziato che nessun esito ebbe la proposta di revisione costituzionale, contenuta nella relazione finale che la Commissione bicamerale "Bozzi" (istituita il 14 aprile 1983) presentò, in data 29 gennaio 1985, al Parlamento. In particolare, con le ipotesi di riscrittura dell'art.21 e di introduzione - nella Parte I, Titolo I - dell'art.21-ter, si mirava ad omologare le manifestazioni del pensiero espresse con altri mezzi di diffusione dell'informazione a quelle a mezzo stampa, anche ai fini della eseguibilità del sequestro. La mancata realizzazione dell'auspicata revisione costituzionale non consentirebbe all'interprete - secondo tale indirizzo interpretativo - di estendere automaticamente la specifica garanzia negativa apprestata dall'art.21, terzo comma, Cost. all'informazione giornalistica diffusa per via telematica.

17. Tale conclusione, però, pur di fronte alla colpevole inerzia del legislatore, rimasto insensibile a ogni sollecitazione di fare chiarezza sullo specifico punto controverso, non può essere condivisa.

Si verrebbe a determinare - come consapevolmente avvertono gli stessi sostenitori della tesi che si contrasta - un'evidente situazione di tensione con il principio di uguaglianza di cui all'art.3 Cost. Si legittimerebbe, infatti, un irragionevole trattamento differenziato dell'informazione giornalistica veicolata su carta rispetto a quella diffusa in rete, con la conseguenza paradossale che la seconda, anche se mera riproduzione della prima, sarebbe assoggettabile, diversamente da quest'ultima, a sequestro preventivo.

È necessario, pertanto, discostarsi dall'esegesi letterale del dettato normativo e privilegiare una interpretazione estensiva dello stesso, si da attribuire al termine "stampa" un significato evolutivo, che sia coerente col progresso tecnologico e, nel contempo, non risulti comunque estraneo all'ordinamento positivo, considerato nel suo complesso e nell'assetto progressivamente raggiunto nel tempo.

L'interpretazione estensiva, se coerente con la mens legis - nel senso che ne rispetta lo scopo oggettivamente inteso, senza porsi in conflitto con il sistema giuridico che regola il settore d'interesse - consente di discostarsi dalle definizioni legali, le quali sono semplici generalizzazioni destinate ad agevolare l'applicazione della legge in un determinato momento storico, e di accreditare al dato normativo un senso e una portata corrispondenti alla coscienza giuridica e alle necessità sociali del momento attuale.
18. Prima, però, di esporre le ragioni che inducono a legittimare, nel rispetto del principio di legalità, una interpretazione evolutiva e costituzionalmente orientata del termine "stampa", è necessario chiarire che l'esito di tale operazione ermeneutica non può riguardare tutti in blocco i nuovi mezzi, informatici e telematici, di manifestazione del pensiero (forum, blog, newsletter, newsgroup, mailing list, pagine Facebook), a prescindere dalle caratteristiche specifiche di ciascuno di essi, ma deve rimanere circoscritto a quelli soli casi che, per i profili strutturale e finalistico che li connotano, sono riconducibili, come meglio si preciserà in seguito, nel concetto di "stampa" inteso in senso più ampio.

Ed invero, deve tenersi ben distinta, ai fini che qui interessano, l'area dell'informazione di tipo professionale, veicolata per il tramite di una testata giornalistica on line, dal vasto ed eterogeneo ambito della diffusione di notizie ed informazioni da parte di singoli soggetti in modo spontaneo.

18.1. Il forum è una bacheca telematica, un'area di discussione, in cui qualsiasi utente o i soli utenti registrati (forum chiuso) sono liberi di esprimere il proprio pensiero, rendendolo visionabile agli altri soggetti autorizzati ad accedervi, attivando così un confronto libero di idee in una piazza virtuale. Il forum, per struttura e finalità, non è assimilabile ad una testata giornalistica e non è soggetto, pertanto, alle tutele e agli obblighi previsti dalla legge sulla stampa.

18.2. Non diversa deve essere la conclusione per il blog (contrazione di web log, ovvero "diario in rete"), che è una sorta di agenda personale aperta e presente in rete, contenente diversi argomenti ordinati cronologicamente. Il blogger pubblica un proprio post, vale a dire un messaggio testuale espressivo della propria opinione, e lo apre all'intervento e al commento dei lettori; oppure ospita i post di altri soggetti che vogliono esprimere la loro opinione in merito a un determinato fatto.

18.3. Anche il social-network più diffuso, denominato Facebook, non è inquadrabile nel concetto di "stampa", ma è un servizio di rete sociale, lanciato nel 2004 e basato su una piattaforma software scritta in vari linguaggi di programmazione; offre servizi di messaggistica privata ed instaura una trama di relazioni tra più persone all'interno dello stesso sistema.

18.4. Altrettanto dicasi, infine, per la newsletter, che è un messaggio scritto o per immagini, diffuso periodicamente per posta elettronica e utilizzato frequentemente a scopi pubblicitari; per i newsgroup, che sono spazi virtuali in cui gruppi di utenti si trovano a discutere di argomenti di interesse comune; per la mailing list, che è un metodo di comunicazione, gestito per lo più da aziende o associazioni, che inviano, tramite posta elettronica, a una lista di destinatari interessati e iscritti informazioni utili, in ordine alle quali si esprime condivisione o si attivano discussioni e commenti.

18.5. Conclusivamente, le forme di comunicazione telematica testé citate sono certamente espressione del diritto di manifestare liberamente il proprio pensiero (art.21, primo comma, Cost.), ma non possono godere delle garanzie costituzionali in tema di sequestro della stampa. Rientrano, infatti, nei generici siti internet che non sono soggetti alle tutele e agli obblighi previsti dalla normativa sulla stampa.

19. La riflessione, quindi, deve essere concentrata sul fenomeno, sempre più diffuso, dei giornali telematici che affollano l'ambiente virtuale e che sono disponibili, in alcuni casi, nella sola versione on line e, in altri, si affiancano alle edizioni diffuse su supporto cartaceo.

È di intuitiva evidenza che un quotidiano o un periodico telematico, strutturato come un vero e proprio giornale tradizionale, con una sua organizzazione redazionale e un direttore responsabile (spesso coincidenti con quelli della pubblicazione cartacea), non può certo paragonarsi a uno qualunque dei siti web innanzi citati, in cui chiunque può inserire dei contenuti, ma assume una sua peculiare connotazione, funzionalmente coincidente con quella del giornale tradizionale, sicché appare incongruente, sul piano della ragionevolezza, ritenere che non soggiaccia alla stessa disciplina prevista per quest'ultimo.

È questo specifico aspetto che merita di essere approfondito.

20. Osserva il Collegio che l'art.1 della l. n.47 del 1948 si limita a definire esplicitamente il concetto di stampa nella sua accezione tecnica di riproduzione tipografica o comunque ottenuta con mezzi meccanici o fisico-chimici.

Il termine "stampa", però, ha anche un significato figurato e, in tal senso, indica i giornali, che sono strumento elettivo dell'informazione e lo erano soprattutto all'epoca in cui entrarono in vigore la Carta Fondamentale e la richiamata l. n.47 del 1948, quando cioè gli altri mass media, in particolare la televisione e i siti di informazione on line, non erano operativi.
Questo concetto di stampa in senso figurato definisce il prodotto editoriale che presenta i requisiti ontologico (struttura) e teleologic (scopi della pubblicazione) propri di un giornale. La struttura di questo è costituita dalla "testata", che è l'elemento che lo identifica, e dalla periodicità regolare delle pubblicazioni (quotidiano, settimanale, mensile); la finalità si concretizza nella raccolta, nel commento e nell'analisi critica di notizie legate all'attualità (cronaca, economia, costume, politica) e dirette al pubblico, perché ne abbia conoscenza e ne assuma consapevolezza nella libera formazione della propria opinione.

A ben vedere, il concetto di stampa così rilevato, anche se non esplicitato, non è estraneo alla l. n.47 del 1948, che, all'art.1, al di là della definizione in senso tecnico enunciata, evoca il requisito della destinazione alla pubblicazione (quindi alla diffusione dell'informazione) e, agli artt.2 e ss., detta la disciplina per i giornali e i periodici di ogni altro genere, con riferimento alle indicazioni obbligatorie che in essi devono comparire, ai requisiti richiesti per rivestire il ruolo di direttore responsabile, all'obbligo di registrazione, all'obbligo di rettifica.

Anche il r.d.lgs. n.561 del 1946, tuttora in vigore, fa generico riferimento ai «giornali» o ad «altre pubblicazioni», nel disciplinare le ipotesi di sequestro degli stessi.

L'art.21, primo comma, Cost., proclama solennemente la libertà di manifestare il proprio pensiero «con la parola, lo scritto e ogni altro mezzo di diffusione». La norma, di carattere generale e precettivo, ha una portata molto ampia, nel senso che riconosce a tutti i consociati, in quanto individui, tale diritto di libertà ed incide inevitabilmente sulle specifiche previsioni che i successivi commi dello stesso art.21 riservano alla "stampa", che è la più importante espressione della libera manifestazione del pensiero. Certamente lungimirante è l'espressione utilizzata dal Costituente «con [...] ogni altro mezzo di diffusione» che oggi abbraccia anche internet, frontiera moderna per la diffusione dell'informazione professionale, ancorata ai valori della responsabilità e della correttezza.

È evidente che l'area riduttiva del significato attribuito al termine "stampa" dall'art.1 della l. n.47 del 1948 è strettamente legata alle tecnologie dell'epoca, il che non impedisce - oggi - di accreditare, tenuto conto dei notevoli progressi verificatisi nel settore, una interpretazione estensiva del detto termine, la quale non esorbita dal campo di significanza del segno linguistico utilizzato ed è coerente col dettato costituzionale.

Lo scopo informativo è il vero elemento caratterizzante l'attività giornalistica e un giornale può ritenersi tale se ha i requisiti, strutturale e finalistico, di cui si è detto sopra, anche se la tecnica di diffusione al pubblico sia diversa dalla riproduzione tipografica o ottenuta con mezzi meccanici o fisico-chimici.

Ma anche a prescindere da tali considerazioni, è il caso di aggiungere che non è certamente dirimente la tesi, secondo cui il giornale telematico non rispecchierebbe le due condizioni ritenute essenziali ai fini della sussistenza del prodotto stampa come definito dalla l. n.47 del 1948, vale a dire un'attività di riproduzione e la destinazione alla pubblicazione.

È possibile, invero, un differente approccio al significato del termine "riproduzione". La riproduzione può ben essere intesa come potenziale accessibilità di tutti al contenuto dello stampato; la produzione di un testo su internet è funzionale alla possibilità di riprodurne e leggerne il contenuto sul proprio computer. L'immissione dell'informazione giornalistica in rete, inoltre, lascia presumere la diffusione della stessa, che diventa fruibile da parte di un numero indeterminato di utenti, il che integra la nozione di "pubblicazione".

L'informazione professionale, pertanto, può essere espressa non solo attraverso lo scritto (giornale cartaceo), ma anche attraverso la parola unita eventualmente all'immagine (telegiornale, giornale radio) o altro mezzo di diffusione, qual è internet (giornale telematico); e tutte queste forme espressive, ove dotate dei requisiti richiesti, non possono essere sottratte alle garanzie e alle responsabilità previste dalla normativa sulla stampa.

Tale conclusione è il frutto di una mera deduzione interpretativa di carattere evolutivo, non analogica, la quale fa leva - nel cogliere fino in fondo, in sintonia con l'evoluzione socio-culturale e tecnologica, il senso autentico dell'art.1 della l. n.47 del 1948 - sull'applicazione di un criterio storico-sistematico in coerenza col dettato costituzionale di cui all'art.21 Cost.

21. Il superamento del concetto di stampa di "gutenberghiana" memoria - d'altra parte - non è affidato esclusivamente alle argomentazioni sviluppate, ma trova riscontro in altri significativi dati positivi.

Il legislatore, pur pigro nell'intervenire organicamente sul tema specifico della stampa on line, non ha mancato, nel corso degli anni, di approvare una serie di leggi, che segnano chiaramente il
superamento dello stretto legame tra informazione professionale e giornale cartaceo, pongono in secondo piano il requisito della necessaria “fisicità” del giornale e polarizzano l’attenzione sulla finalità informativa dell’attività giornalistica, che deve essere contraddistinta da attendibilità, pertinenza, continenza e imparzialità rispetto a qualsiasi altro tipo di informazione.

21.1. In materia di sistema radiotelevisivo - oggetto notoriamente di un continuo “dialogo” tra legislatore e Corte Costituzionale - la legge di riforma della RAI 14 aprile 1975, n.103, la l. 6 agosto 1990, n.223 (nota come legge Mammì), ed il d.lgs. 31 luglio 2005, n.177, offrono una definizione e una disciplina della testata giornalistica televisiva o radiofonica, ricalcando in gran parte, al di là di alcuni specifici aspetti, la regolamentazione della stampa cartacea.

L’art.10 della l. n.223 del 1990 (attualmente art.32-quinquies d.lgs. n.177 del 2005) ha esteso, infatti, alle emittenti televisive e radiofoniche l'obbligo di registrazione delle rispettive testate giornalistiche, che devono avere un direttore responsabile, e quello della rettifica (art.5, 6 e 8 della l. n.47 del 1948). La detta legge ha posto una netta linea di demarcazione tra telegiornali e giornali radio, da una parte, e trasmissioni di diverso genere effettuate dalle reti delle singole emittenti, dall'altra.

È innegabile che la nozione di testata giornalistica radiotelevisione accredita il concetto contenutistico di stampa e rappresenta un modello per i giornali della rete.

21.2. La l. 31 luglio 1997, n.249 (nota come legge Maccanico), nell'istituire l'Autorità per le garanzie nelle comunicazioni (AGCom), ha previsto anche l'istituzione del Registro degli operatori della comunicazione (ROC), in sostituzione dei preesistenti registri nazionali della stampa e delle imprese radiotelevisive. In tale unico registro sono tenuti ad iscriversi, superando le suddivisioni che avevano caratterizzato in precedenza i singoli settori, tutti gli operatori della comunicazione, ivi comprese le imprese editoriali di giornali quotidiani, periodici o riviste, le agenzie di stampa di carattere nazionale, i soggetti esercenti l'editoria elettronica e digitale, le imprese fornitrici di servizi telematici.

21.3. La l. 23 dicembre 2000, n.388 (Finanziaria per il 2001), per la prima volta, equipara in modo esplicito, ai fini dei finanziamenti previsti per le imprese editoriali, la stampa tradizionale a quella telematica e consacra il principio dell'obbligo di registrazione presso il Tribunale anche delle testate online. L'art.153, commi 2 e 3, della legge fa riferimento, in particolare, ai quotidiani e ai periodici telematici espressione di partiti e dei movimenti politici.

21.4. La l. 7 marzo 2001, n.62, intitolata «Nuove norme sull'editoria e sui prodotti editoriali», offre una nuova definizione di "prodotto editoriale". Per tale s'intende, ai sensi dell'art.1, comma 1, «il prodotto realizzato su supporto cartaceo o su supporto informatico, destinato alla pubblicazione o, comunque, alla diffusione di informazioni presso il pubblico con ogni mezzo, anche elettronico». Questa nuova definizione di prodotto editoriale comporta l'estensione anche all'editoria on line delle norme relative alle indicazioni obbligatorie sugli stampati e all'obbligo di registrazione delle testate giornalistiche e dei periodici.

L'art.1, comma 3, infatti, testualmente statuisce: «Al prodotto editoriale si applicano le disposizioni di cui all'art.2 della legge 8 febbraio 1948, n.47. Il prodotto editoriale diffuso al pubblico con periodicità regolare e contraddistinto da una testata, costituente elemento identificativo del prodotto, è sottoposto, altresì, agli obblighi previsti dall'art.5 della medesima legge n.47 del 1948».

Si distinguono, quindi, analogamente a quanto previsto dalla legge sulla stampa, due tipi di prodotto editoriale: senza o con periodicità regolare. La prima parte della disposizione testé richiamata prescrive che ogni prodotto editoriale deve contenere le indicazioni di cui all'art.2 della l. n.47 del 1948; la seconda parte prevede che devono essere iscritte nell'apposito registro tenuto dalla cancelleria del competente Tribunale le testate telematiche che abbiano le stesse caratteristiche di quelle cartacee.

Poiché la legge in esame aveva sollevato non pochi interrogativi circa la riferibilità delle disposizioni in essa contenute anche all'informazione di natura non professionale, sebbene a carattere periodico, il d.lgs. n.70 del 2003 ha precisato (art.7, comma 3) che la registrazione della testata editoriale telematica è obbligatoria esclusivamente per le attività per le quali i prestatori del servizio intendano avvalersi delle provvidenze economiche previste dalla l. n.62 del 2001.

21.5. Anche il d.l. 18 maggio 2012, n.63, convertito dalla l. 16 luglio 2012, n.103, intervenendo in maniera urgente sul riordino dei contributi alle imprese editoriali, si muove lungo la linea di omologazione della testata giornalistica in edizione digitale a quella in edizione cartacea, stabilendo che, in caso di pubblicazione di entrambe con lo stesso marchio editoriale, l'impresa non
è obbligata alla duplice iscrizione, ma soltanto a dare apposita comunicazione al registro degli operatori di comunicazione (art.3, comma 2, ultimo periodo). La medesima legge contiene disposizioni (art.3-bis) volte a favorire l'editoria digitale, esentando dall'obbligo di registrazione presso il Tribunale e di iscrizione al ROC i periodici di piccole dimensioni (ricavi annui non superiori a 100.000 euro) diffusi esclusivamente via web. Di norma, quindi, i giornali telematici sono soggetti agli obblighi di cui alle leggi n.47 del 1948 e n.62 del 2001.

22. Tutto quanto esposto legittima, pertanto, una interpretazione costituzionalmente orientata del concetto di "stampa", idoneo ab origine ad adeguarsi alla prevedibile evoluzione dei tempi e a ricomprendere la nuova realtà dei quotidiani o periodici on line regolarmente registrati e destinatari, al pari della stampa tradizionale, delle provvidenze pubbliche previste per l'editoria.

I successivi e numerosi interventi - sia pure disorganici e farraginosi - del legislatore, ai quali si è fatto cenno, non costituiscono una fonte di rilettura della l. n.47 del 1948, bensì sopravvenienze coerenti con questa, della quale viene colta e assorbita la reale portata, per estenderne la relativa disciplina anche alle testate giornalistiche telematiche.

La previsione dell'obbligo di registrazione della testata on line, che deve contenere le indicazioni prescritte e deve essere guidata da un direttore responsabile, giornalista professionista o pubblicista, non è un mero adempimento amministrativo fine a sé stesso, ma è funzionale a individuare le responsabilità (civili, penali, amministrative) collegate alle pubblicazioni e a rendere operative le corrispondenti garanzie costituzionali, aspetti questi che, in quanto strettamente connessi e consequenziali alla detta previsione, sono ineludibili.

Conclusivamente, il giornale telematico, sia se riproduzione di quello cartaceo, sia se unica e autonoma fonte di informazione professionale, soggiace alla normativa sulla stampa, perché ontologicamente e funzionalmente è assimilabile alla pubblicazione cartacea. E, infatti, un prodotto editoriale, con una propria testata identificativa, diffuso con regolarità in rete; ha la finalità di raccogliere, commentare e criticare notizie di attualità dirette al pubblico; ha un direttore responsabile, giornalista professionista; ha una propria testata identificativa, diffuso con regolarità in rete; ha la finalità di raccogliere, commentare e criticare notizie di attualità dirette al pubblico; ha un direttore responsabile, iscritto all'Albo dei giornalisti; è registrato presso il Tribunale del luogo in cui ha sede la redazione; ha un hosting provider, che funge da stampatore, e un editore registrato presso il ROC.

Ovviamente - è il caso di sottolinearlo - le garanzie e le responsabilità previste, per la stampa, dalle disposizioni sia di rango costituzionale, sia di livello ordinario, devono essere riferite ai soli contenuti redazionali e non anche ad eventuali commenti inseriti dagli utenti (soggetti estranei alla redazione), che attivano un forum, vale a dire una discussione su uno o più articoli pubblicati.

Il percorso ermeneutico privilegiato, per pervenire alla ritenuta equiparazione tra i due prodotti editoriali, è il solo che scongiura tensione con il principio di uguaglianza di cui all'art.3 della Carta fondamentale, evitando il rischio di riservare, al di là di qualsiasi ragionevolezza, trattamenti differenziati a due fattispecie praticamente identiche sotto il profilo della loro funzionalità (diffusione dell'informazione professionale).

Conseguentemente, la "stampa telematica", al pari di quella tradizionale, in quanto emancipata da qualsiasi forma di censura, non può essere sottoposta a sequestro preventivo, se non nei casi eccezionali espressamente previsti dalla legge, e soggiace alle norme che disciplinano la responsabilità per gli illeciti commessi.

A margine, è opportuno ricordare che le Corti sovranazionali, in numerose pronunce, hanno data per scontata, ritenendola realtà acquisita, l'equiparazione tra giornale cartaceo e giornale on line (Corte EDU, 16 luglio 2013, Wegrzynowski e Smolczewsky c. Polonia; Corte Giustizia, 25 ottobre 2011, Martinez c. Società MGN Limited; Corte Giustizia, 25 ottobre 2011, Date Advertising c. X).

23. All'esito dell'iter argomentativo sin qui seguito sul tema specifico, vanno enunciati i seguenti principi di diritto:

- "La testata giornalistica telematica, in quanto assimilabile funzionalmente a quella tradizionale, rientra nel concetto ampio di 'stampa' e soggiace alla normativa, di rango costituzione e di livello ordinario, che disciplina l'attività d'informazione professionale diretta al pubblico";

- "Il giornale on line, al pari di quello cartaceo, non può essere oggetto di sequestro preventivo, eccettuati i casi tassativamente previsti dalla legge, tra i quali non è compreso il reato di diffamazione a mezzo stampa".

24. Passando ad analizzare la vicenda che coinvolge i due indagati, deve osservarsi quanto segue.
L'atto di ricorso proposto nell'interesse dei predetti, con particolare riferimento al primo motivo di censura, che è decisivo e assorbente rispetto alle altre doglianze, è fondato.

L'ordinanza impugnata, invero, non si fa carico della delicata problematica implicata nel caso esaminato, nonostante il Giudice del riesame ne fosse stato espressamente investito dalla difesa, con specifici motivi scritti in data 25 marzo 2014.

Il provvedimento in verifica, in ogni caso, in palese disarmonia con i principi di diritto innanzi enunciati, ha confermato il decreto di sequestro preventivo della pagina web della testata telematica "Il Giornale.it", regolarmente registrata, limitandosi a ritenere la sussistenza del fumus dell'ipotizzato reato di diffamazione e del pericolo di aggravamento delle conseguenze dannose di tale illecito.

Nel caso specifico, avuto riguardo al titolo di reato per cui si procede, la detta misura cautelare reale, per tutte le considerazioni più sopra svolte, non poteva essere adottata e si risolve in una indiretta e non consentita forma di censura.

Palese è, pertanto, la violazione di legge che contraddistingue sia il provvedimento genetico sia quello di riesame.

Sarebbe stato possibile adottare, ai fini dell'accertamento dell'ipotizzato reato, soltanto il sequestro probatorio, secondo le modalità di cui all'art.254-bis c.p.p.

Conseguentemente, deve disporsi l'annullamento senza rinvio dell'ordinanza impugnata e del decreto di sequestro preventivo emesso in data 7 marzo 2014 dal G.i.p. del Tribunale di Monza.

[...]

P.Q.M.

Annulla senza rinvio l'ordinanza impugnata, nonché il decreto di sequestro preventivo del 7 marzo 2014 del G.i.p. del Tribunale di Monza.

*****

**DISCUSSIONE**

1. **Come può avvenire, materialmente, il sequestro preventivo di un sito o di una pagina web?**
2. **È ammissibile il sequestro preventivo, anche parziale, di un sito web?**
3. **È ammissibile, al di fuori dei casi espressamente previsti dalla legge, il sequestro preventivo della pagina web di una testata giornalistica telematica registrata? In cosa, e perché, la disciplina è distinta da quella relativa ad altri siti web?**
4. **Come viene definito Internet nella sentenza?**
5. **I dati informatici presenti in Rete sono considerati equiparabili a “cose”?**
6. **La sentenza distingue diversi mezzi informatici o telematici di manifestazione del pensiero (forum, blog, social network, newsletter, newsgroup, masiling list). A che fini? I citati mezzi godono di protezione costituzionale? Di che tipo?**
7. **Il giornale telematico soggiace alla disciplina sulla stampa? A che condizioni?**

*****

**NORME**

- **art.21 Cost.**
10.3. Giornale telematico e tutela costituzionale

Corte di Cassazione, sez.un. civili, 25 ottobre 2016, n.23469

Fatto e diritto
A.- La richiesta del Procuratore Generale.

1. Il Procuratore Generale ha chiesto a questa Corte, [...] l'enunciazione del principio di diritto al quale il giudice del merito avrebbe dovuto attenersi nelle controversie civili, decise in sede cautelare in senso opposto dai giudici del tribunale di Napoli, vertenti tra il presidente di una università telematica, nella qualità ed anche in proprio, resa oggetto di reiterati articoli apparsi sia in forma cartacea che sul sito internet di un noto settimanale e poi di un quotidiano, prospettati come aventi contenuto diffamatorio perché incentrati su notizie e informazioni o collegamenti con altre notizie e informazioni quanto a presunte eccessive facilitazioni nei corsi di studio, soprattutto in favore di alcune forze politiche.

2. La prima delle due controversie (relativa ad articoli apparsi sia sul numero del 20 ottobre 2014 del settimanale «L'Espresso» che sul relativo sito internet il 17 novembre 2014) era stata definita con ordinanza 18 febbraio 2015 di accoglimento del reclamo avverso la declaratoria di inammissibilità del ricorso cautelare del diffamato e contestuale ordine, peraltro non seguito dall'instaurazione del giudizio di merito, al gruppo editoriale di rimuovere l'articolo dalla pagina web e di deindicizzarlo presso i più comuni motori di ricerca, nonché di non rendere più visibile, sul sito web della testata, il blog collegato al medesimo articolo; la seconda delle dette controversie (relativa ad articoli apparsi sul sito web del quotidiano «La Repubblica» nei giorni 28 gennaio 2015 e 23 marzo 2015) era stata invece definita con valutazione, in sede di reclamo e con ordinanza del giorno 8 luglio 2015, di inammissibilità del provvedimento cautelare in materia.

B.- Il procedimento: le parti del procedimento presupposto.

6. È formulata dal Procuratore Generale richiesta di enunciazione di un principio di diritto nell'interesse della legge ai sensi del primo comma dell'art.363 c.p.c. [...] norma in virtù della quale «quando le parti non hanno proposto ricorso nei termini di legge o vi hanno rinunciato, ovvero quando il provvedimento non è ricorribile in cassazione e non è altrimenti impugnabile, il Procuratore generale presso la Corte di Cassazione può chiedere che la Corte enunci, nell'interesse della legge, il principio di diritto al quale il giudice di merito avrebbe dovuto attenersi».

25. L'opportunità di intervenire con l'enunciazione di un principio di diritto è poi positivamente ed effettivamente riscontrata nella fattispecie in esame, sia pure non certo per dirimere una discrepanza - quand'anche rilevante - interna però ad un unico tribunale, benché tra i maggiori italiani per dimensioni, visto che non è compito istituzionale di questa Corte Suprema comporre simili divergenze ermeneutiche locali.

26. L'opportunità si riscontra piuttosto:
- perché le Sezioni Unite penali di questa stessa Corte sono di recente intervenute a disciplinare la materia, con un importante arresto di ampio portata anche ricostruttiva della materia (Cass. Sez. Un. pen., 29 gennaio 2015, dep. 17 luglio 2015, n.31022, imp. Fazzo e a.), statuendo, come da massima ufficiale, che «in tema di sequestro di giornali e di altre pubblicazioni, la testata giornalistica telematica, funzionalmente assimilabile a quella tradizionale in formato cartaceo, rientra nella nozione di "stampa" di cui all'art.1 della legge 8 febbraio 1948, n.47 e, pertanto, non può essere oggetto di sequestro preventivo in caso di commissione del reato di diffamazione a mezzo stampa, in quanto si tratta di prodotto editoriale sottoposto alla normativa di rango costituzionale e di livello ordinario, che disciplina l'attività di informazione professionale diretta al pubblico»;
- in ogni caso, per la rilevante importanza che la stampa telematica ha conquistato - per nozioni di comune esperienza, quando non di cronaca - nella vita quotidiana per la pervasività delle telecomunicazioni via internet e l'assenza di prese di posizione da parte della giurisprudenza civile sul regime di tutela dell'informazione diffusa con quei mezzi, quale ulteriore forma di espressione della libertà di manifestazione del pensiero, in rapporto alle peculiari potenzialità
offensive soprattutto di diritti altrettanto fondamentali, quali la dignità o il rispetto della riservatezza e della vita privata o lo stesso onore in una moderna accezione.

D.- Il merito della questione.
27. Può quindi procedersi alla disamina della questione, con la precisazione che al riguardo questa Corte non è vincolata dalla concreta articolazione delle richieste formulate dal Procuratore Generale, poiché il presente procedimento postula certo il suo atto di impulso, ma non è retto da un principio di corrispondenza tra chiesto e pronunciato.

E.- Il quadro normativo di riferimento.
30. Quale punto di arrivo di una più che secolare elaborazione giuridica nazionale, della quale Cass. Sez. Un. pen. n.31022 del 2015 si è fatta carico ai punti da 10 a 12 della motivazione e quale principio cardine della restaurata democrazia, la libertà di pensiero e di stampa - significativamente accostati i due oggetti - fu proclamata solennemente dalla Costituzione della Repubblica al suo art.21, [...].

31. Com'è evidente, l'art.21, comma 3, Cost., disciplina l'istituto del sequestro in stretta correlazione col divieto di autorizzazione o censura, preventiva o successiva, sottoponendolo alla duplice garanzia della riserva di legge e di giurisdizione: il sequestro della stampa generalmente intesa - cioè, senza specificazioni, sia essa periodica o comune - può essere disposto, con atto motivato dell'autorità giudiziaria, soltanto nel caso di delitti per i quali la legge sulla stampa espressamente lo autorizzi o nel caso di stampa clandestina; quello della stampa periodica è soggetto ad ulteriori garanzie procedurali; in ogni caso, il riferimento alla legge sulla stampa non introduce una riserva qualificata di legge, ma è indicativo del complesso delle norme riguardanti la materia (Corte cost., sentn. 19 gennaio 1972, n.4 e 25 marzo 1976, n.60).

32. L'Assemblea Costituente, in attuazione della XVII disposizione transitoria della Carta fondamentale, varò anche la legge 8 febbraio 1948, n.47, intitolata «Disposizioni sulla stampa» e ritenuta integrante il disposto dell'art.21 Cost., il cui art.1 precisa che sono da considerarsi stampe o stampati «tutte le riproduzioni tipografiche o comunque ottenute con mezzi meccanici o fisico-chimici, in qualsiasi modo destinate alla pubblicazione».

33. Per quel che in questa sede rileva, i casi nei quali le leggi vigenti consentono il sequestro preventivo sono:
   a) violazione delle norme sulla registrazione delle pubblicazioni periodiche e sull'indicazione dei responsabili (artt.3 e 16 legge n.47 del 1948);
   b) stampati osceni o offensivi della pubblica decenza ovvero divulganti mezzi atti a procurare l'aborto (art.2 r.d.lgs. n.561 del 1946: dichiarato incostituzionale con sent. Corte cost. n.49 del 1971);
   c) stampa periodica che faccia apologia del fascismo (art.8 legge 20 giugno 1952, n.645);
   d) violazione delle norme a protezione del diritto d'autore (art.161 legge 22 aprile 1941, n.633).

34. La Carta dei Diritti Fondamentali dell'Unione Europea, dal canto suo, consacra, al suo art.11, la libertà di espressione e d'informazione [...].

35. Non alla stampa in particolare, ma alla libertà di espressione in generale nei suoi profili attivi e passivi, dedica poi il suo art.10 la Convenzione europea per la salvaguardia dei diritti dell'Uomo e delle libertà fondamentali [...]).

36. Ancora, per l'art.19 della Dichiarazione universale dei diritti dell'Uomo, approvata dall'Assemblea generale dell'Organizzazione delle Nazioni Unite il 10 dicembre 1948, «ogni individuo ha il diritto alla libertà di opinione e di espressione, incluso il diritto di non essere molestato per la propria opinione e quello di cercare, ricevere e diffondere informazioni e idee attraverso ogni mezzo e senza riguardo a frontiere».

37. La disciplina costituzionale differenzia la stampa periodica da quella comune e ulteriori differenze sono rinvenibili nella legge n.47 del 1948, che rende gli adempimenti relativi alla stampa periodica (indicazioni obbligatori, obbligo di registrazione) più gravosi rispetto a quelli previsti per la stampa comune; e numerosi ulteriori interventi normativi - anch'essi presi in considerazione dalla già richiamata Cass. Sez. Un. pen. n.31022 del 2015 - prevedono, poi, in attuazione dell'art.21, comma 5, Cost., finanziamenti pubblici in favore dell'editoria giornalistica, nella prospettiva di favorire il pluralismo nell'informazione e contrastare fenomeni di concentrazionismo, con interventi cui gli interpreti in genere rimproverano una scarsa sistematicità, rimarcandone la finalità di accesso indifferenziato a risorse pubbliche.
38. In particolare, la legge 7 marzo 2001, n.62 (intitolata "Nuove norme sull'editoria e sui prodotti editoriali"), ha, in un minimale tentativo di organicità (contestato in quanto tale però dalla prevalente dottrina, che sottolinea la settorialità dell'intervento), definito unitariamente come «prodotto editoriale» quello «realizzato su supporto cartaceo (...) o su supporto informatico, destinato alla pubblicazione o, comunque, alla diffusione di informazioni presso il pubblico con ogni mezzo, anche elettronico», distinguendo, all'interno del genus, due species:
- quella dei prodotti editoriali senza periodicità regolare e quella dei prodotti editoriali con periodicità regolare - e comunque estendendo diverse normative previste per la stampa tradizionale ad ogni prodotto editoriale caratterizzato dalla periodicità regolare.
39. Anche gli interventi successivi, tra i quali quello del 2012 (d.l. 18 maggio 2012, n.63, conv. con mod. in l. 16 luglio 2012, n.103) ed altro in via di pubblicazione proprio in questi giorni sulla Gazzetta Ufficiale dopo l'approvazione da parte dei due rami del Parlamento, privilegiano comunque una disciplina orientata alla gestione di provvidenze pubbliche, orientate a sostenere il pluralismo e la professionalità nell'erogazione dell'informazione.

F.- La nozione rilevante di «stampa».
40. Appartiene alla comune esperienza come, da qualche decennio, l'avvento di tecnologie prima impensabili abbia rivoluzionato il modo di vivere e soprattutto di interagire quotidiano non solo della maggior parte degli scambi economici mondiali, ma anche di una gran parte della vita e delle relative abitudini dei singoli individui; ma è certamente la possibilità di una interconnessione costante - da taluno paragonata a quella neuronale, capace di esaltare esponenzialmente le capacità dei singoli componenti - con una moltitudine virtualmente illimitata di corrispondenti in uno spazio teoricamente privo di barriere, in uno all'immediatezza intesa sia sotto il profilo temporale che dell'assenza di controlli o filtri intermedi a caratterizzare l'aspetto principale della «comunicazione», nel recuperato etimo originario di «messa in comune» di una mole di informazioni e di dati, assai spesso personali ed anzi personalissimi, che neutralizza ed abbatte la distanza fisica tra gli individui, rendendo teoricamente e spesso praticamente possibile la materializzazione sul singolo dispositivo - a questo punto, ben definibile quale terminale della Rete - personale di un contatto con ogni altro analogo punto nel mondo e il collegamento interattivo con questo, sol che sia da esso consentito.
41. Non solo ogni aspetto della vita quotidiana, ma anche ogni suo istituto tradizionale ed ogni sua trasposizione nel mondo del diritto, sono investiti da questa rivoluzione: e lo è a maggior ragione il settore della comunicazione di notizie e informazioni in senso tradizionale; ma, in attesa che la società prima e, coi suoi consueti tempi, il legislatore poi disciplinino ed irreggimentino in norme più o meno specificamente ad essi destinate le singole mutazioni in atto della società prima e, coi suoi consueti tempi, il legislatore poi disciplinino ed irreggimentino in norme più o meno specificamente ad essi destinate le singole mutazioni in atto degli istituti tradizionali, è compito del giurista quello di interpretare il sistema giuridico esistente per verificarne l'ampiezza ed indeterminatezza delle ipotesi da affrontare (ché adducere inconveniens non est vere argumentum), quanto piuttosto per tanto equivarrebbe alla pretesa di regolare la tutela cautelare della singola mutazione con una multitudine virtualmente illimitata di corrispondenti in uno spazio teoricamente privo di barriere, in uno all'immediatezza intesa sia sotto il profilo temporale che dell'assenza di controlli o filtri intermedi a caratterizzare l'aspetto principale della «comunicazione», nel recuperato etimo originario di «messa in comune» di una mole di informazioni e di dati, assai spesso personali ed anzi personalissimi, che neutralizza ed abbatte la distanza fisica tra gli individui, rendendo teoricamente e spesso praticamente possibile la materializzazione sul singolo dispositivo - a questo punto, ben definibile quale terminale della Rete - personale di un contatto con ogni altro analogo punto nel mondo e il collegamento interattivo con questo, sol che sia da esso consentito.
42. Per questo è indispensabile rinunciare a passare in rassegna, per differenziarle dal giornale telematico, le forme di manifestazione e comunicazione del pensiero su internet ai fini dell'individuazione della rispettiva tutela cautelare - anche preventiva - in sede civile, non tanto per l'ampiezza ed indeterminatezza delle ipotesi da affrontare (ché adducere inconveniens non est vere argumentum), quanto piuttosto perché tanto equivocarebbe alla pretesa di regolare la trasposizione nel mondo della Rete di ogni possibile, eventualmente anche ipotetica e futura o non ancora sperimentata, forma con la quale il proprio pensiero o la propria personalità sia messa in comune con tutti i potenziali fruitori del world wide web, vale a dire con ogni individuo che possa ad essa connettesi e, quindi, in teoria, con chiunque: ciò che, se non appare francamente velleitario, esula ad ogni modo dalla fattispecie concreta da cui il potere nomofilatico trae il suo presupposto, per quanto argomentato più sopra al p.to 29.
43. Ai fini che qui interessano, occorre stabilire soltanto se e a quali condizioni quella forma particolare di comunicazione, che va comunemente sotto il nome di giornale telematico, goda o meno delle garanzie che la Costituzione accorda alla stampa e, quindi, se in tale ultimo concetto quel giornale possa essere condotto; ed a tale domanda queste Sezioni Unite ritengono possibile dare risposta positiva per due vie, tra loro concorrenti, se non alternative: una prima, fondata sull'applicazione diretta, non cioè analogica, né estensiva, del lemma della norma costituzionale; una seconda, fondata sull'interpretazione del concetto funzionale di stampa finalizzata alla divulgazione professionale dell'informazione.
44. In entrambi i casi, può bene prescindersi - siccome non conferente ai fini dell'enunciazione del principio di diritto e quindi estraneo all'ambito della decisione - da qualsiasi sforzo di ricostruzione sistematica della disciplina di settore, solo apparendo indispensabile individuare i tratti caratterizzanti comuni al giornale telematico e a quello tradizionale, al quale ultimo sicuramente la tutela, prevista dalle norme di rango costituzionale ed ordinario su richiamate, è già accordata.

45. Se la Carta costituzionale non definisce il termine «stampa», si è visto che a tanto si induce la legge sulla stampa pubblicata pochi mesi dopo l'entrata in vigore della Costituzione, che riconduce a tale nozione «tutte le riproduzioni tipografiche o comunque ottenute con mezzi meccanici o fisico-chimici, in qualsiasi modo destinate alla pubblicazione», escludendo espressamente, in un contesto in cui la tecnologia già conosceva la radiodiffusione e non ignorava la diffusione televisiva, tali mezzi dalla relativa nozione.

46. Solamente con la legislazione di settore in campo radiotelevisivo a partire dal 1975 (legge 14 aprile 1975, n.103; legge 6 agosto 1990, n.223; legge 31 luglio 1997, n.249; d.lgs. 31 luglio 2005, n.177) fu poi accettata una equiparazione, prevalentemente a fini di garanzia del do la sua stessa

47. Alla riproduzione tipografica (o mediante pressione di caratteri originariamente mobili, con metodi analoghi a quelli messi a punto da Gutenberg a partire dal 1455), cioè di caratteri propri della scrittura o di immagini immediatamente percepibili col senso della vista (o, in alcuni casi eccezionali come la scrittura Braille, con quello del tatto), avvenuta su di un supporto durevole (inteso peraltro nel senso che possa perdurare il tempo necessario alla lettura) - quale la carta - ed ottenuta con qualsiasi mezzo «chimico-fisico», a ben guardare può però bene essere equiparata la diffusione a mezzo internet.

48. Con la premessa di rinunciare a qualsiasi velleità di precisione tecnica e soltanto con la pretesa di valutare la tenuta dell'interpretazione giuridica di un lemma secondo la sua stessa definizione originaria, ripudiando le tesi dell'esclusività dell'interpretazione secondo il senso inteso dal legislatore al tempo in cui la norma fu redatta, può infatti qui rilevarsi, sia pure in via eminentemente descrittiva o con le necessarie approssimazioni ed a rischio di qualche anche grossolana semplificazione o banalizzazione, ma al fine di verificare l'applicabilità della regola di diritto eadem ratio eadem dispositio, come anche la diffusione via internet comporta una riproducibilità di un originale, solo che questo può dirsi quello integrato dai dati fisicamente immagazzinati - ospitati - presso il server dell'internet service provider, per esservi stato immesso dal suo autore, sicché la riproduzione avviene previo trasferimento («scarico») dei dati da quel server al dispositivo dell'utente finale e riscomposizione e riorganizzazione dei dati stessi presso quest'ultimo dispositivo fino ad essere riprodotto, con meccanismi indubbiamente fisico-chimici, sul video dell'apparecchio terminale o «client» (ed eventualmente, ma non necessariamente, anche stampato mediante un dispositivo ad esso collegato). Ed ancora più semplice è l'equiparazione tra riproduzione radiotelevisiva e riproduzione telematica, una volta scaricato il file audio o video, che viene riprodotto, con le viste modalità, sul dispositivo dell'utente.

49. In sostanza, mentre con la stampa tradizionale alla moltiplicazione dell'originale provvede direttamente in via per così dire accentrata lo stampatore e la distribuzione avviene in tempo successivo, con quella telematica si ha la messa a disposizione dell'originale (o di una molteplicità di originali tra loro generalmente conformi) di una moltitudine indifferenziata di utenti finali, lasciando a questi il processo tecnico finale della visualizzazione, con mezzi indubbiamente fisico-chimici, dei segni grafici o degli altri mezzi di comunicazione impiegati dall'autore di questa: si ha - in termini sempre meramente descrittivi e volutamente atecnici - quindi una sorta di scomparsa del procedimento di riproduzione, mediante una delocalizzazione, presso il singolo utente o client, della fase concernente l'attività materiale di riproduzione dell'originale, che resta in remoto sul server ove l'autore ha collocato il file in cui quello consiste, anche se la riproduzione può limitarsi alla visualizzazione (che, a stretto rigore, è anch'essa una riproduzione per il tempo necessario alla fruizione con uno dei sensi fisici, vista e/o udito).

G.- L'equiparazione funzionale tra giornale telematico e giornale tradizionale

50. Una simile ricostruzione elide la necessità di interpretazioni evolutive, storiche, estensive o tanto meno analogiche del concetto di «stampa», bastando semplicemente applicare in via diretta la relativa definizione alla fattispecie della trasmissione a distanza con mezzo telematico ed alle sue peculiarità, per sussumerla nella previsione costituzionale dell'art.21, comma terzo (e
seguinte, per quel che potrebbe rilevare), della Costituzione il giornale telematico; ma alla stessa conclusione si perviene anche per altra via.

51. Infatti, le Sezioni Unite penali di questa Corte (con la più volte richiamata sentenza n.31022 del 2015) hanno già ricordato come alla nozione di «stampa» siano pacificamente ricondotti i giornali tradizionali ed alla stessa hanno concluso di potere condurre quelli telematici: gli uni e gli altri, secondo la specifica rielaborazione offerta (v. p.ti 21.4 e ss., nonché 22), sono qualificabili come prodotti editoriali, caratterizzati da una testata, dalla diffusione regolare, dall'organizzazione in una struttura con un direttore responsabile che sia giornalista professionista o pubblicita, una redazione ed un editore registrato presso il registro degli operatori della comunicazione, dalla finalizzazione all'attività professionale di informazione diretta al pubblico, per tale intendendosi quella di raccolta e commento di notizie di attualità e di informazioni da parte di soggetti professionalmente qualificati.

52. In estrema sintesi, è dal riscontro di identici requisiti, elaborati per le due tipologie, che è fatta discendere l'equiparazione dei giornali - in tutto o in parte - telematici a quelli tradizionali: evidentemente, vi è qui da dire, sulla base del riscontro dell'esercizio, da parte di entrambi in forme simili, di un'attività professionale di divulgazione e commento di notizie ed informazione, esercitata secondo regole preliminarmente elaborate di responsabilità o doveri o rispetto di limiti - ed in prevalenza autoamministrate per l'organizzazione in albi di natura pubblicistica - da parte di soggetti particolarmente qualificati, in regime di trasparenza anche quanto a fonti di finanziamento e sostanzialmente di riferimento.

53. La piena libertà di comunicazione di informazioni e di idee su tutte le questioni di interesse pubblico, riconosciuta alla stampa in una società democratica anche in un contesto sovranazionale (Corte eur. dir. Uomo, Gr. Ch., 16 giugno 2015, Delfi as c/ Estonia, ric. n.64569/09, p.to 132, con richiamo ai risalenti precedenti Jersild c/ Danimarca, 23 settembre 1994, §37, […], e Bladet Tromso e Stensaaas c/ Norvegia [GC], n.21980/93, §58, […]), trova infatti limitazioni in doveri e responsabilità a garanzia anche dei diritti fondamentali altrui: doveri e responsabilità che possono essere adeguatamente rispettati, a tutela dei diritti fondamentali altrui, evidentemente con una organizzazione strutturata come sopra, sicché solo ad un tale statuto può collegarsi la - così ben più pregnante rispetto a quella generale, in ogni caso spettante, prevista dal primo comma del medesimo art.21 Cost. - tutela costituzionale ed ordinaria del divieto di cautele preventive dal contenuto corrispondente al sequestro.

54. Né rileva che tale elaborazione si poggi, come criticamente rilevato in dottrina, in prevalenza sulla normativa di settore finalizzata al sovvenzionamento dell'editoria per favorirne la diffusione pluralistica e professionale; potendo, al contrario, osservarsi:

- che quest’ultimo obiettivo è idoneamente in grado di orientare, quale mezzo di intervento indiretto dei pubblici poteri, la disciplina di una stampa moderna ed appunto responsabile (nel senso indicato al punto precedente), quale valore da privilegiare od incentivare nell’ambito della più generale e per altro verso comunque garantita libertà di espressione: nel senso che soltanto la stampa che presenti quelle caratteristiche, in teoria idonee ad offrire una divulgazione di informazione responsabile e professionale, possono meritare anche, da un lato, un sovvenzionamento pubblico e, dall’altro, la tutela preventiva dal sequestro.

55. In altri termini, che si tratta di connotazioni obiettivamente funzionali alle esigenze di tutela dalle attività di controllo preventivo previste dall’art.21 della Costituzione: invero, tali forme di tutela bene possono predicarsi riservate a quelle specifiche forme di manifestazioni di pensiero, come appunto la diffusione ed il commento professionali di notizie od informazioni, indispensabili per la formazione della pubblica opinione in una moderna società democratica, quali giustificazione stessa o contrappeso della particolare responsabilità loro richiesta ed imposta.

56. Ove questi connotati strutturali e funzionali siano posseduti dal giornale pubblicato, non importa se in tutto o in parte, col mezzo telematico, a prescindere anche dall'equipollenza dei metodi impiegati descritta ai precedenti p.ti 51 e 52 si giustifica allora la riconduzione di tale giornale nel concetto di «stampa» rilevante ai fini dell’art.21, comma terzo, della Costituzione e quindi ai fini dell’esclusione del sequestro od altra forma di controllo preventivo.

57. Va solo precisato che la periodicità, talvolta richiesta dalla normativa in esame ed in ogni caso imposta per la qualificazione di una pubblicazione come giornale o periodico, sta nella non occasionalità o nella non episodicità o nella non unicità dell’edizione o pubblicazione: cosa che può riscontrarsi in una regolarità di pubblicazione di nuove edizioni (o numeri), unificate dall'identità o perlomeno dalla costanza degli altri elementi sopra descritti; e che, nella stampa telematica
periodica, strutturalmente articolata su di un sito tendenzialmente permanente, può risolversi - ai fini che qui interessano e sempre con la vista premessa di grande approssimazione, funzionale all’applicazione di concetti originariamente modellati su realtà fattuali non ancora evolute - anche nel consueto «aggiornamento» delle relative pagine: ciò che, per mantenere un parallelismo meramente descrittivo con la stampa tradizionale, può equivarsi alla lontana ad una «edizione» di un certo giorno o di una certa ora.


60. Il mezzo di comunicazione è sicuramente più pervasivo e diffusivo, idoneo a causare danno in modo maggiore, rispetto alla carta stampata ed in genere alla stampa tradizionale, ma - evidentemente - in modo appena più capillare della diffusione via radio o via televisione: sicché correttamente - secondo quanto già prospettato dai giudici del merito che ditanto si sono occupati - ogni problematica connessa a tali modalità tecniche o strutturali del mezzo va riservata al momento successivo della pronuncia a cognizione piena, quando, accertata definitivamente la prevalenza sul diritto di libertà di manifestazione del pensiero e di stampa di quello all’onore ed alla dignità del soggetto diffamatore, occorrerà risarcire il danno, in via prioritaria in forma specifica e solo sussidiariamente per equivalente.

61. D’altra parte, la maggiore ed anzi immediata diffusività - che, per la sua illimitatezza, potrebbe quasi definirsi diffusività globale - è il **proprium** di tale rivoluzionario mezzo di comunicazione: limitare il quale in via cautelare equivarrebbe a sterilizzarlo o a svuotarne di contenuto le potenzialità; sicché le stesse valutazioni di bilanciamento tra diritti altrettanto fondamentali (la libertà di stampa ed il diritto all’onore o all’immagine, prevalente senz’altro la prima, benché soltanto nella fase cautelare preventiva civilistica), operate dalla Corte Costituzionale italiana con sobria lungimiranza quantasei anni fa, vanno ribadite per la persistente attualità della necessità di garantire quella libertà di manifestazione del pensiero, se intesa con le cautele già riconosciute ed elaborate per la stampa tradizionale.

62. In sostanza, davvero non si può trattare in via interpretativa in modo deteriore rispetto al passato la libertà di stampa solo perché è diventato tecnicamente più facile avvalersene.

63. Per quanto argentato in premessa, peraltro, non può in questa sede farsi luogo ad alcun altro approfondimento: i contenuti del giornale telematico - nel relativo concetto compreso anche il settimanale o periodico - in quanto tale sono equiparati ai corrispondenti contenuti del giornale tradizionale, ovviamente a parità di presupposti applicativi e mutevoli esclusivamente le modalità tecniche di realizzazione (o «implementazione»); i contenuti propri ed esclusivi del giornale telematico (nel relativo concetto compreso anche il settimanale o periodico), cioè resi possibili esclusivamente da questo e non comuni anche alla stampa tradizionale, andranno valutati separatamente e ad essi non potrà allora immediatamente estendersi la conclusione di applicazione de plano della normativa di tutela, di rango tanto costituzionale che sovranazionale ed ordinario, ma dovrà essere ricercata di volta in volta in base ai parametri rilevanti propri della
singola fattispecie, eventualmente diversi, a tutto concedere riferiti al solo primo comma dell'art.21 Cost. ed al più intenso bilanciamento con gli altri diritti fondamentali della prima parte della Carta fondamentale.

H.- La tutela prevista dall'art.21 Cost., terzo comma

64. A questo punto, la disamina di queste Sezioni Unite si fa più semplice, perché i principi tradizionali e le conclusioni già raggiunte in materia conservano, nonostante il lungo tempo trascorso dall'ultimo esplicito arresto in materia, la loro actualità.

65. Al riguardo, Corte cost. 24 giugno 1970, n.122, dichiarando non fondata la questione di legittimità costituzionale dell'art.10 del codice civile, degli artt.96 e 97 della legge 22 aprile 1941, n.633 (contenente disposizioni sulla «protezione del diritto d'autore e di altri diritti connessi al suo esercizio»), e - nei sensi di cui in motivazione - dell'art.700 c.p.c., in riferimento all'art.21, comma terzo, della Costituzione, statuì solennemente che il sequestro della stampa era vietato, tranne i soli casi previsti dalla legge sulla stampa stessa, per la prevalenza della libertà di stampa - a causa dell'importanza del suo ruolo in una società democratica - su ogni altro interesse meramente individuale, così reputando preclusa altresì la concessione di qualsiasi misura atipica, soprattutto ai sensi dell'art.700 c.p.c., di contenuto corrispondente a quelle espressamente vietate da altre norme dell'ordinamento, a maggior ragione quando si tratti di norme di rango costituzionale.

66. E, di lì a pochi anni, Cass. 7 febbraio 1975, n.2129, sancì espressamente che «l'art.700 c.p.c., se può consentire l'emanazione di provvedimenti cautelari atipici intesi a far cessare temporaneamente o a contenere il pregiudizio che deriva a terzi da una pubblicazione a stampa, non può, tuttavia, costituire la fonte del potere di concedere un provvedimento di sequestro della stampa vietato da altra norma dell'ordinamento giuridico e, in particolare, dall'art.21 Cost.», che lo consentiva solo con l'osservanza di limiti rigorosi: sicché il giudice, nel disporre la cessazione dell'abuso dell'immagine altrui a norma dell'art.10 c.c. avrebbe potuto ordinare con provvedimento d'urgenza il sequestro del materiale lesivo solo quando si trattasse di materiale che, pur essendo destinato alla pubblicazione, non fosse stato ancora stampato, poiché, diversamente, il provvedimento cautelare avrebbe inciso su una riproduzione a stampa che costituisce già una manifestazione attuale e concreta dell'esercizio del diritto di libertà tutelato dall'art.21 Cost., che lo consente solo nei rigorosi limiti ivi indicati (ovverosia, pubblicazioni contrarie al buon costume e delitti per i quali la legge sulla stampa espressamente lo autorizzi ex artt.1 e 2 del r.d.l. n.561 del 1946).

67. Non è questa la sede per apprezzare il bilanciamento tra i diritti coinvolti, attesa la chiarezza della previsione costituzionale e quindi dell'opzione operata direttamente dai Costituenti, rispondente tuttora ad un ragionevole componimento tra le esigenze contrapposte.

68. Tali principi vanno riaffermati in relazione al giornale telematico, quando il conflitto sia con il diritto all'onore o alla reputazione e, quindi, allorché il contenuto di quello sia prospettato come diffamatorio: ciò che costituisce l'oggetto delle fattispecie all'esame dei provvedimenti dei giudici di merito, concluendo la manifestazione attuale e concreta dell'esercizio del diritto di libertà tutelato dall'art.21 Cost., lo consente solo nei rigorosi limiti ivi indicati (ovverosia, pubblicazioni contrarie al buon costume e delitti per i quali la legge sulla stampa espressamente lo autorizzi ex artt.1 e 2 del r.d.l. n.561 del 1946).

69. Infatti, il solo diritto alla reputazione e all'onore (cioè, a prescindere da altri diritti di pari od eventualmente poizore rango, tutelati da altre discipline, la cui applicazione - è bene ribadirlo - è lasciata impregiudicata), benché certamente anch'esso fondamentale in quanto inerente in modo diretto alla personalità od alla dignità dell'individuo, deve intendersi recessivo dinanzi alla tutela della libertà di stampa, sia pure nella fase a cognizione sommaria di un giudizio civile quale quella cautelare finalizzata all'adozione di misure urgenti (v. Corte cost. 122/70, cit.), di qualunque contenuto, ripristinatorio o inibitorio o analogo.

70. A loro volta, le misure cautelari proibite dalla lettera del comma terzo dell'art.21 Cost. sono tutte quelle che impedirebbero la diffusione del materiale già pronto alla circolazione (in tal senso interpretando la norma Cass. 2129/75): sicché, considerate le caratteristiche tecniche del mezzo con cui l'offesa è arrecata, devono qualificarsi precluse, e quindi non ammissibili quale oggetto di qualsiasi provvedimento cautelare equiparato al giudicato. Tutte le misure, comunque denominate, che tendano ad impedire la persistenza nella Rete o l'ulteriore circolazione o diffusione dell'articolo - o equipollente - di giornale telematico ritenuto diffamatorio o, se da esse inscindibile, dell'intera pagina o dell'edizione o, in casi estremi, della testata; misure tra cui devono comprendersi anche quelle indicate come deindicizzazione o ad esse analoghe o di contenuto o soprattutto effetto corrispondente.
71. La tutela piena, con il risarcimento in forma specifica o per equivalente e soprattutto con strumenti che spetterà al giudice che avrà conosciuto in modo non sommario della vicenda e dei suoi effetti individuare anche in ordine alle conseguenze della particolare diffusività degli strumenti adoperati, andrà riservata al momento, necessariamente successivo, del riconoscimento - con pronuncia almeno esecutiva - se non definitiva ed irretrattabile - dell'effettiva violazione del diritto individuale all'onore od alla reputazione, il quale solo potrà eventualmente ribaltare la valutazione di prevalenza tra i due diritti fondamentali.

72. Giova ribadire ancora una volta che tale conclusione è limitata al caso in cui si invochi una tutela civilistica cautelare preventiva contro il giornale (in tale espressione ricondotto anche il settimanale) telematico con cui sia commessa una lesione all'onore o alla reputazione, cioè che si prospetti come connotato da un contenuto diffamatorio, mentre non è estesa a diversi casi di conflitti con altri diritti assistiti da differenti e specifiche normative, come quella in materia di protezione dei dati personali, ogni questione relativa all'interazione con le quali essendo lasciata esplicitamente impregiudicata.

I.- Conclusioni.

73. In conclusione, sulla richiesta del Procuratore Generale ai sensi del primo comma dell’art.363 c.p.c. queste Sezioni Unite deliberano di enunciare il seguente principio di diritto: «La tutela costituzionale assicurata dal terzo comma dell’art.21 Cost. alla stampa si applica al giornale o al periodico pubblicato, in via esclusiva o meno, con mezzo telematico, quando possieda i medesimi tratti caratterizzanti del giornale o periodico tradizionale su supporto cartaceo e quindi sia caratterizzato da una testata, diffuso o aggiornato con regolarità, organizzato in una struttura con un direttore responsabile, una redazione ed un editore registrato presso il registro degli operatori della comunicazione, finalizzata all’attività professionale di informazione diretta al pubblico, cioè di raccolta, commento e divulgazione di notizie di attualità e di informazioni da parte di soggetti professionalmente qualificati. Pertanto, nel caso in cui sia dedotto il contenuto diffamatorio di notizie ivi pubblicate, il giornale pubblicato, in via esclusiva o meno, con mezzo telematico non può essere oggetto, in tutto o in parte, di provvedimento cautelare preventivo o inibitorio, di contenuto equivalente al sequestro o che ne impedisca o limiti la diffusione, ferma restando la tutela eventualmente concomitante prevista in tema di protezione dei dati personali».

P.Q.M.

La Corte, pronunciando a sezioni unite e decidendo sulla richiesta del Procuratore Generale ai sensi del primo comma dell’art.363 c.p.c. […] enuncia il principio di diritto di cui al p.to 73 della motivazione.

[...] *****

DISCUSSIONE

1. Cosa si intende per “prodotto editoriale”, ai sensi della legge n.62/2001? Che distinzione è presente all’interno della norma?
2. I giornali telematici sono riconducibili alla nozione di stampa e di prodotto editoriale? Se sì, tale inquadramento cosa comporta?
3. Che tutela fornisce alla stampa l’art.21, comma 3, Cost.?
4. Quale tratti deve avere il giornale telematico per essere ricompreso nel concetto di stampa ai fini dell’applicazione dell’art. 21, comma 3, Cost.?

*****

NORME

- art.21, Cost.
11. DIRITTI ECONOMICI E SOCIETÀ DELL’INFORMAZIONE
11.1. Diritti d’autore e ruolo del provider

Corte di Giustizia dell’Unione Europea, 16 febbraio 2012 (causa C-360/10)

[...] 1. La domanda di pronuncia pregiudiziale verte sull’interpretazione delle seguenti direttive:
- 2000/31/CE […] dell’8 giugno 2000, relativa a taluni aspetti giuridici dei servizi della società dell’informazione, in particolare il commercio elettronico, nel mercato interno («Direttiva sul commercio elettronico») […]
- 2001/29/CE […] del 22 maggio 2001, sull’armonizzazione di taluni aspetti del diritto d’autore e dei diritti connessi nella società dell’informazione […]
- 2004/48/CE […] del 29 aprile 2004, sul rispetto dei diritti di proprietà intellettuale […]
- 95/46/CE […] del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati […]
- 2002/58/CE del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche) […]


Causa principale e questione pregiudiziale

15. La SABAM è una società di gestione che rappresenta gli autori, i compositori e gli editori di opere musicali. A tale titolo, essa ha, in particolare, il compito di autorizzare l’utilizzo delle loro opere protette da parte di terzi.

16. La Netlog gestisce una piattaforma di rete sociale in linea sulla quale ogni iscritto riceve uno spazio personale, denominato «profilo», che l’utente stesso può riempire e che è accessibile a livello mondiale.

17. La funzione principale di tale piattaforma, quotidianamente utilizzata da decine di milioni di persone, è quella di creare comunità virtuali che consentono a dette persone di comunicare tra loro e, in tal modo, di stringere amicizie. Sul proprio profilo gli utenti possono, in particolare, tenere un diario, indicare i propri passatempi e preferenze, mostrare i propri amici, visualizzare foto personali o pubblicare estratti di video.

18. La SABAM ha tuttavia ritenuto che la rete sociale della Netlog permetta altresì a tutti gli utenti di utilizzare, tramite il loro profilo, opere musicali ed audiovisive del repertorio della SABAM, mettendo dette opere a disposizione del pubblico in maniera tale che altri utenti della suddetta rete possano avervi accesso, e questo senza l’autorizzazione della SABAM e senza che la Netlog versi un compenso a tale titolo.

19. Nel corso del mese di febbraio 2009, la SABAM si è rivolta alla Netlog al fine di stipulare una convenzione relativa al versamento, da parte di quest’ultima, di un compenso per l’utilizzo del repertorio della SABAM.

20. Con lettera del 2 giugno 2009, la SABAM ha intimato alla Netlog di impegnarsi a cessare immediatamente e per il futuro la messa a disposizione del pubblico non autorizzata di opere musicali e audiovisive del repertorio della SABAM, mettendo dette opere a disposizione del pubblico in maniera tale che altri utenti della suddetta rete possano avervi accesso, e questo senza l’autorizzazione della SABAM e senza che la Netlog versi un compenso a tale titolo.

21. Il 23 giugno 2009 la SABAM ha fatto notificare alla Netlog un atto di citazione dinanzi al presidente del Rechtbank van eerste aanleg te Brussel, nell’ambito di un’azione inibitoria ai sensi dell’art.87, §1, della legge del 30 giugno 1994, sul diritto d’autore e sui diritti connessi, chiedendo, in particolare, che venga ordinato alla Netlog di cessare immediatamente qualsiasi messa a disposizione illecita delle opere musicali o audiovisive del repertorio della SABAM, sotto pena del pagamento di una sanzione pecuniaria di € 1.000 per ogni giorno di ritardo.

22. A tale riguardo, la Netlog ha sostenuto che l’accoglimento dell’azione della SABAM equivarrebbe ad imporre alla Netlog un obbligo generale di sorveglianza, vietato dall’art.21, §1,
della legge dell’11 marzo 2003, relativa a taluni aspetti giuridici dei servizi della società dell’informazione, che recepisce nel diritto nazionale l’art.15, §1, della direttiva 2000/31/CE.

23. Inoltre, la Netlog ha affermato, senza essere contraddetta dalla SABAM, che l’accoglimento di un’azione siffatta potrebbe avere l’effetto di costringerla a predisporre, nei confronti della sua intera clientela, in abstracto e a titolo preventivo, a sue spese e senza limiti nel tempo, un sistema di filtraggio della maggior parte delle informazioni memorizzate sui suoi server, al fine di individuare file elettronici contenenti opere musicali, cinematografiche o audiovisive sulle quali la SABAM affermi di vantare diritti e, successivamente, di bloccarne lo scambio.

24. Orbene, la predisposizione di un simile sistema di filtraggio farebbe, probabilmente, sorgere l’obbligo di sottoporre i dati personali ad un trattamento che deve essere conforme alle disposizioni del diritto dell’Unione sulla protezione dei dati personali e sul segreto delle comunicazioni.

25. Per questi motivi, il presidente del Rechtbank van eerste aanleg te Brussel ha deciso di sospendere il procedimento e di sottoporre alla Corte la seguente questione pregiudiziale:

«Se le direttive 2001/29/CE e 2004/48/CE, lette in combinato disposto con le direttive 95/46/CE, 2000/31/CE e 2002/58/CE, interpretate, in particolare, alla luce degli artt.8 e 10 della Convenzione europea per la salvaguardia dei diritti dell’uomo e delle libertà fondamentali, […] consentano agli Stati membri di autorizzare un giudice nazionale, adito nell’ambito di un procedimento nel merito e in base alla sola disposizione di legge che prevede che “[I giudici nazionali possono] altresì emettere un’ingiunzione recante un provvedimento inibitorio nei confronti di intermediari cui servizi siano utilizzati da un terzo per violare il diritto d’autore o un diritto connesso”, ad ordinare ad un fornitore di servizi di hosting di predisporre, nei confronti della sua intera clientela, in abstracto e a titolo preventivo, esclusivamente a sue spese e senza limitazioni nel tempo, un sistema di filtraggio della maggior parte delle informazioni che vengono memorizzate sui suoi server, al fine di individuare file elettronici contenenti opere musicali, cinematografiche o audiovisive sulle quali la SABAM affermi di vantare diritti e, successivamente, di bloccare lo scambio di questi file».

Sulla questione pregiudiziale


- delle informazioni memorizzate sui server di detto prestatore dagli utenti dei suoi servizi;
- che si applichi indistintamente nei confronti di tutti questi utenti;
- a titolo preventivo;
- a spese esclusive del prestatore, e
- senza limiti nel tempo,

idoneo ad identificare i file elettronici contenenti opere musicali, cinematografiche o audiovisive rispetto alle quali il richiedente il provvedimento di ingiunzione affermi di vantare diritti di proprietà intellettuale, onde bloccare la messa a disposizione del pubblico di dette opere, lesiva del diritto d’autore (in prosieguo: il «sistema di filtraggio controverso»).

27. A tale proposito, è anzitutto pacifico che il gestore di una piattaforma di rete sociale in linea, quale la Netlog, memorizza sui propri server informazioni fornite dagli utenti di tale piattaforma e relative al loro profilo e che, pertanto, questi è un prestatore di servizi di hosting ai sensi dell’art.14 della direttiva 2000/31/CE.

28. Occorre altresì rammentare che, secondo gli artt.8, §3, della direttiva 2001/29/CE e 11, terza frase, della direttiva 2004/48/CE, i titolari di diritti di proprietà intellettuale possono chiedere un provvedimento inibitorio nei confronti dei gestori di piattaforme di reti sociali in linea, come la Netlog, che agiscono in qualità di intermediari ai sensi delle suddette disposizioni, dato che i loro servizi possono essere utilizzati dagli utenti di simili piattaforme per violare i diritti di proprietà intellettuale.

29. Inoltre, dalla giurisprudenza della Corte emerge che la competenza attribuita, a norma di tali disposizioni, ai giudici nazionali deve consentire a questi ultimi di ingiungere a detti intermediari di adottare provvedimenti diretti non solo a porre fine alle violazioni già inferte ai diritti di proprietà intellettuale mediante i loro servizi della società dell’informazione, ma anche a prevenire nuove violazioni (v. sentenza del 24 novembre 2011, Scarlet Extended, C-70/10, […]).
30. Infine, dalla medesima giurisprudenza si evince che le modalità delle ingiunzioni che gli Stati membri devono prevedere ai sensi di detti artt.8, §3, e 11, terza frase, quali quelle relative alle condizioni che devono essere soddisfatte e alla procedura da seguire, devono essere stabilite dal diritto nazionale (v. sentenza Scarlet Extended, cit., p.to 32).


33. Di conseguenza, le medesime norme devono rispettare, segnatamente, l’art.15, §1, della direttiva 2000/31/CE, che vieta alle autorità nazionali di adottare misure che impongano ad un prestatore di servizi di hosting di procedere ad una sorveglianza generalizzata sulle informazioni che esso memorizza (v., per analogia, sentenza Scarlet Extended, cit., p.to 35).

34. A questo riguardo, la Corte ha già dichiarato che siffatto divieto abbraccia, in particolare, le misure nazionali che obblighino un prestatore intermedio, come un prestatore di servizi di hosting, a realizzare una sorveglianza attiva su tutti i dati di ciascuno dei suoi clienti per prevenire qualsiasi futura violazione di diritti di proprietà intellettuale. Peraltro, un siffatto obbligo di sorveglianza generale sarebbe incompatibile con l’art.3 della direttiva 2004/48/CE, il quale enuncia che le misure contemplate da detta direttiva devono essere eque, proporzionate e non eccessivamente costose (v. sentenza Scarlet Extended, cit., p.to 36).

35. Alla luce di tali premesse, occorre esaminare se l’ingiunzione di cui al procedimento principale, che imporrebbe al prestatore di servizi di hosting di predisporre il sistema di filtraggio controverso, lo obblighi a realizzare, in tale occasione, una sorveglianza attiva su tutti i dati di ciascuno degli utenti dei suoi servizi per prevenire qualsiasi futura violazione di diritti di proprietà intellettuale.

36. A tale riguardo, è pacifico che la predisposizione di tale sistema di filtraggio presupporrebbe che il prestatore di servizi di hosting:
- identifichi, anzitutto, all’interno dell’insieme dei file memorizzati sui suoi server da tutti gli utenti dei suoi servizi, quelli che possono contenere opere su cui i titolari di diritti di proprietà intellettuale affermano di vantare diritti;
- determini, successivamente, quali dei suddetti file siano memorizzati e messi a disposizione del pubblico in maniera illecita, e
- proceda, infine, al blocco della messa a disposizione dei file che ha considerato illeciti.

37. Pertanto, una siffatta sorveglianza preventiva richiederebbe un’osservazione attiva dei file memorizzati dagli utenti presso il prestatore di servizi di hosting e riguarderebbe sia la quasi totalità delle informazioni così memorizzate sia ciascuno degli utenti dei servizi di tale prestatore (v., per analogia, sentenza Scarlet Extended, cit., p.to 39).

38. Alla luce delle suesposte considerazioni, occorre dichiarare che l’ingiunzione rivolta al prestatore di servizi di hosting di predisporre il sistema di filtraggio controverso lo obbligherebbe a procedere ad una sorveglianza attiva della quasi totalità dei dati relativi a ciascuno degli utenti dei suoi servizi, onde prevenire qualsiasi futura violazione di diritti di proprietà intellettuale. Ne consegue che la suddetta ingiunzione imporrebbe al prestatore di servizi di hosting una sorveglianza generalizzata, vietata dall’art.15, §1, della direttiva 2000/31/CE (v., per analogia, sentenza Scarlet Extended, cit., p.to 40).

39. Per vagliare la conformità di tale ingiunzione al diritto dell’Unione, occorre inoltre tenere conto delle condizioni che discendono dalla tutela dei diritti fondamentali applicabili, come quelli menzionati dal giudice del rinvio.

40. In proposito va ricordato che l’ingiunzione oggetto del procedimento principale è volta a garantire la tutela dei diritti d’autore, che appartengono alla sfera del diritto di proprietà intellettuale e che possono essere lesi dalla natura e dal contenuto di talune informazioni memorizzate e messe a disposizione del pubblico attraverso il servizio fornito dal prestatore di servizi di hosting.

41. Sebbene la tutela del diritto di proprietà intellettuale sia sancita dall’art.17, §2, della Carta dei diritti fondamentali dell’Unione Europea (in prosieguo: la «Carta»), non può desumersi né da

235
tale disposizione né dalla giurisprudenza della Corte che tale diritto sia intangibile e che la sua tutela debba essere garantita in modo assoluto (sentenza Scarlet Extended, cit., p.to 43).


43. Più precisamente, dal p.to 68 di tale sentenza emerge che è compito delle autorità e dei giudici nazionali, nel contesto delle misure adottate per proteggere i titolari di diritti d’autore, garantire un giusto equilibrio tra la tutela di tali diritti e quella dei diritti fondamentali delle persone su cui incidono dette misure.

44. Pertanto, in circostanze come quelle del procedimento principale, le autorità ed i giudici nazionali devono, in particolare, garantire un giusto equilibrio tra la tutela del diritto di proprietà intellettuale, di cui godono i titolari di diritti d’autore, e quella della libertà d’impresa, di cui beneficiano operatori quali i prestatori di servizi di hosting in forza dell’art.16 della Carta (v. sentenza Scarlet Extended, cit., p.to 46).

45. Orbene, nel procedimento principale, l’ingiunzione di predisporre il sistema di filtraggio controverso implica una sorveglianza, nell’interesse di tali titolari, sulla totalità o sulla maggior parte delle informazioni memorizzate presso il prestatore di servizi di hosting coinvolto. Tale sorveglianza è inoltre illimitata nel tempo, riguarda qualsiasi futura violazione e postula che si debbano tutelare non solo opere esistenti, bensì anche opere che non sono state ancora create nel momento in cui viene predisposto detto sistema.

46. Un’ingiunzione di questo genere causerebbe, quindi, una grave violazione della libertà d’impresa del prestatore di servizi di hosting, poiché l’obbligherebbe a predisporre un sistema informatico complesso, costoso, permanente e unicamente a sue spese, il che risulterebbe peraltro contrario alle condizioni stabilite dall’art.3, §1, della direttiva 2004/48/CE, il quale richiede che le misure adottate per assicurare il rispetto dei diritti di proprietà intellettuale non siano inutilmente complesse o costose (v., per analogia, sentenza Scarlet Extended, cit., p.to 48).

47. Occorre pertanto dichiarare che l’ingiunzione di predisporre il sistema di filtraggio controverso non può considerarsi conforme all’esigenza di garantire un giusto equilibrio tra, da un lato, la tutela del diritto di proprietà intellettuale, di cui godono i titolari di diritti d’autore, e, dall’altro, quella della libertà d’impresa, di cui beneficiano operatori come i prestatori di servizi di hosting (v., per analogia, sentenza Scarlet Extended, cit., p.to 49).

48. Per di più, gli effetti di detta ingiunzione non si limiterebbero al prestatore di servizi di hosting, poiché il sistema di filtraggio controverso è idoneo a ledere anche i diritti fondamentali degli utenti dei servizi di tale prestatore, ossia il loro diritto alla tutela dei dati personali e la loro libertà di ricevere o di comunicare informazioni, diritti questi ultimi, tutelati dagli utenti dei servizi di tale prestatore.

49. Infatti, l’ingiunzione di predisporre il sistema di filtraggio controverso implicherebbe, da un lato, l’identificazione, l’analisi sistematica e l’elaborazione delle informazioni relative ai profili creati sulla rete sociale dagli utenti della medesima, informazioni, queste, che costituiscono dati personali protetti, in quanto consentono, in linea di principio, di identificare i suddetti utenti (v., per analogia, sentenza Scarlet Extended, cit., p.to 51).

50. Dall’altro, detta ingiunzione rischerebbe di ledere la libertà di informazione, poiché tale sistema potrebbe non essere in grado di distinguere adeguatamente tra un contenuto illegale e un contenuto legale, sicché il suo impiego potrebbe produrre il risultato di bloccare comunicazioni aventi un contenuto legito. Infatti, è indiscusso che la questione della liceità di una trasmissione dipende anche dall’applicazione di eccezioni di legge al diritto d’autore che variano da uno Stato membro all’altro. Inoltre, in determinati Stati membri talune opere possono rientrare nel pubblico dominio o possono essere state messe in linea a titolo gratuito da parte dei relativi autori (v., per analogia, sentenza Scarlet Extended cit., p.to 52).

51. Pertanto, occorre dichiarare che, adottando un’ingiunzione che costringa il prestatore di servizi di hosting a predisporre il sistema di filtraggio controverso, il giudice nazionale in questione non rispetterebbe l’obbligo di garantire un giusto equilibrio tra il diritto di proprietà intellettuale, da un lato, e la libertà di impresa, il diritto alla tutela dei dati personali e la libertà di ricevere o di comunicare informazioni, dall’altro (v., per analogia, sentenza Scarlet Extended, cit., p.to 53).

52. Alla luce di quanto precede, occorre rispondere alla questione sottoposta dichiarando che le direttive 2000/31/CE, 2001/29/CE e 2004/48/CE lette in combinato disposto e interpretate alla luce delle esigenze di tutela dei diritti fondamentali applicabili, devono essere interpretate nel
senso che ostano all'ingiunzione, rivolta ad un prestatore di servizi di hosting, di predisporre il sistema di filtraggio controverso.

[...]
Per questi motivi, la Corte (Terza Sezione) dichiara:

Le direttive:
- 2000/31/CE [...] dell'8 giugno 2000, relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno («Direttiva sul commercio elettronico»);
- 2001/29/CE [...] del 22 maggio 2001, sull'armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione, e
- 2004/48/CE [...] del 29 aprile 2004, sul rispetto dei diritti di proprietà intellettuale,
lette in combinato disposto e interpretate alla luce delle esigenze di tutela dei diritti fondamentali applicabili, devono essere interpretate nel senso che ostano all'ingiunzione, rivolta da un giudice nazionale ad un prestatore di servizi di hosting, di predisporre un sistema di filtraggio:
- delle informazioni memorizzate sui server di detto prestatore dagli utenti dei suoi servizi;
- che si applichi indistintamente nei confronti di tutti questi utenti;
- a titolo preventivo;
- a spese esclusive del prestatore, e
- senza limiti nel tempo,
idoneo ad identificare i file elettronici contenenti opere musicali, cinematografiche o audiovisive rispetto alle quali il richiedente il provvedimento di ingiunzione affermi di vantare diritti di proprietà intellettuale, onde bloccare la messa a disposizione del pubblico di dette opere, lesiva del diritto d’autore.

*****

DISCUSSIONE

1. Un intermediario Internet può essere obbligato ad adottare un sistema di filtraggio permanente per individuare la presenza di file contenenti opere soggette a diritto d’autore ed a bloccare lo scambio di questi file?
2. Quali sono i diritti e gli interessi coinvolti nel caso? A quali soggetti si riferiscono?
3. Cosa si intende per «giusto equilibrio»?

*****

NORME

- artt.8, 11, 16, 17, Carta dei diritti fondamentali dell’Unione Europea
- artt.12-15, direttiva 2000/31/CE
- art.8, direttiva 2001/29/CE
- artt.2, 3, 11, direttiva 2004/48/CE
11.2. Diritti d’autore e link

Corte di Giustizia dell’Unione Europea, 13 febbraio 2014 (causa C-466/12)

[…]
1. La domanda di pronuncia pregiudiziale verte sull’interpretazione dell’art.3, §1, della direttiva 2001/29/CE […], del 22 maggio 2001, sull’armonizzazione di taluni aspetti del diritto d’autore e dei diritti connessi nella società dell’informazione […].
2. Tale domanda è stata presentata nell’ambito di una controversia avviata dai sigg. Svensson e Sjögren, nonché dalle sig.re Sahlman e Gadd, nei confronti della società Retriever Sverige AB (in prosieguo: la «Retriever Sverige») ai fini del risarcimento del preteso danno da essi subito per effetto dell’inserimento sul sito Internet di tale società di collegamenti cliccabili («ipertestuali») che rinviano ad articoli di cui i medesimi sono titolari del relativo diritto d’autore.

Contesto normativo

[…]

Procedimento principale e questioni pregiudiziali

8. I ricorrenti nel procedimento principale, tutti giornalisti, sono i redattori di taluni articoli pubblicati, da un lato, sul giornale Göteborgs-Posten e, dall’altro lato, sul sito Internet del Göteborgs-Posten. La Retriever Sverige gestisce un sito Internet che fornisce ai suoi clienti, secondo le loro necessità, liste di collegamenti Internet cliccabili verso articoli pubblicati da altri siti Internet. È pacifico inter partes che gli articoli erano liberamente accessibili sul sito del giornale Göteborgs-Posten. Secondo i ricorrenti nel procedimento principale, se il cliente clicca su uno di questi collegamenti non si rende conto chiaramente di essere trasferito su un altro sito per accedere all’opera di suo interesse. Per contro, secondo la Retriever Sverige il cliente è consapevole del fatto che cliccando su uno di questi collegamenti viene trasferito su un altro sito.
9. I ricorrenti nella causa principale hanno citato la Retriever Sverige dinanzi allo Stockholms tingsrätt (Tribunale di Stoccolma) per ottenere il risarcimento del danno derivante dal fatto che tale società avrebbe sfruttato, senza la loro autorizzazione, taluni loro articoli, mettendoli a disposizione dei suoi clienti.
13. Alla luce di queste considerazioni, lo Svea hovrätt ha deciso di sospendere il procedimento e di sottoporre alla Corte le seguenti questioni pregiudiziali:
«1) Se il fatto che un soggetto diverso dal titolare del diritto d’autore su una determinata opera fornisca un collegamento cliccabile alla stessa sul proprio sito Internet si configuri come comunicazione al pubblico dell’opera ai sensi dell’art.3, §1, della direttiva 2001/29.
2) Se sia rilevante, ai fini della soluzione della prima questione, il fatto che l’opera alla quale rimanda il collegamento si trovi su un sito Internet accessibile a chiunque senza limitazioni oppure che l’accesso sia in qualche modo limitato.
3) Se, ai fini della soluzione della prima questione, si debba distinguere il caso in cui l’opera, dopo che l’utente abbia cliccato il collegamento, sia presentata su un altro sito Internet da quello in cui l’opera sia presentata con modalità tali da offrire al cliente l’impressione di restare nello stesso sito Internet.
4) Se uno Stato membro possa stabilire una maggiore tutela del diritto esclusivo dell’autore includendo nella nozione di comunicazione al pubblico più forme di messa a disposizione di quante stabilite all’art.3, §1, della direttiva 2001/29».

Sulle questioni pregiudiziali

Sulle tre questioni pregiudiziali

14. Con le sue prime tre questioni, che è opportuno esaminare congiuntamente, il giudice del rinvio chiede, in sostanza, se l’art.3, §1, della direttiva 2001/29 debba essere interpretato nel senso che costituisce un atto di comunicazione al pubblico, come previsto da tale disposizione, la fornitura su un sito Internet di collegamenti cliccabili verso opere protette disponibili su un altro sito.
Internet, fermo restando che le opere di cui trattasi sono liberamente accessibili su questo altro sito.


17. Per quanto riguarda il primo di tali elementi, ossia l’esistenza di un «atto di comunicazione», tale nozione deve essere intesa in senso ampio (v., in tal senso, sentenza del 4 ottobre 2011, Football Association Premier League e a., C-403/08 e C-429/08, […]), p.to 193) e ciò allo scopo di garantire, come risulta segnatamente dai considerando 4 e 9 della direttiva 2001/29, un elevato livello di protezione ai titolari del diritto d’autore.

18. Nel caso di specie, occorre rilevare che il fatto di mettere a disposizione su un sito Internet dei collegamenti cliccabili verso opere protette, pubblicate senza alcun limite di accesso su un altro sito, offre agli utilizzatori del primo sito un accesso diretto a tali opere.


20. Ne consegue che in circostanze come quelle di cui al procedimento principale, il fatto di fornire collegamenti cliccabili verso opere tutelate deve essere qualificato come «messa a disposizione» e, di conseguenza, come «atto di comunicazione», nel senso di detta disposizione.


22. Orbene, un atto di comunicazione, come quello compiuto dal gestore di un sito Internet tramite i collegamenti cliccabili, è diretto a tutti gli utilizzatori potenziali del sito gestito da tale soggetto, vale a dire un numero indeterminato e piuttosto considerevole di destinatari.

23. Pertanto, si deve ritenere che tale gestore effettui una comunicazione ad un pubblico.

24. Ciò premesso, come risulta da costante giurisprudenza, per ricadere nella nozione di «comunicazione al pubblico», ai sensi dell’art.3, §1, della direttiva 2001/29, occorre che una comunicazione, come quella di cui trattasi nel procedimento principale, riguardante le stesse opere della comunicazione iniziale ed effettuata in Internet come la comunicazione iniziale, quindi con le stesse modalità tecniche, sia rivolta ad un pubblico nuovo, cioè ad un pubblico che i titolari del diritto d’autore non abbiano considerato, al momento in cui abbiano autorizzato la comunicazione iniziale al pubblico (v., per analogia, sentenza SGAE, cit., p.ti 40 e 42; ordinanza del 18 marzo 2010, Organismos Sillogikis Diacheirisis Dimiourgon Theatrikon kai Optikoakoustikon Ergon, C-136/09, p.to 38, nonché sentenza ITV Broadcasting e a., cit., p.to 39).

25. Nel caso di specie si deve rilevare che la messa a disposizione delle opere di cui trattasi tramite un collegamento cliccabile, come quello esaminato nel procedimento principale, non porta a comunicare le opere di cui trattasi ad un pubblico nuovo.

26. Infatti, il pubblico cui la comunicazione iniziale era diretta era costituito dal complesso dei potenziali visitatori del sito considerato, poiché, essendo a conoscenza del fatto che l’accesso alle opere su tale sito non era assoggettato ad alcuna misura restrittiva, tutti gli internauti potevano avere liberamente accesso ad esse.

27. Si deve pertanto dichiarare che, qualora il complesso degli utilizzatori di un altro sito, ai quali siano state comunicate le opere di cui trattasi tramite un collegamento cliccabile, potesse direttamente accedere a tali opere sul sito sul quale siano state inizialmente comunicate, senza intervento del gestore dell’altro sito, gli utilizzatori del sito gestito da quest’ultimo devono essere considerati come potenziali destinatari della comunicazione iniziale e, quindi, ricompresi nel pubblico previsto dai titolari del diritto d’autore al momento in cui hanno autorizzato la comunicazione iniziale.
28. Di conseguenza, in mancanza di un pubblico nuovo, l’autorizzazione dei titolari del diritto d’autore non è necessaria per una comunicazione al pubblico come quella di cui al procedimento principale.

29. Tale constatazione non potrebbe essere rimessa in discussione nel caso in cui il giudice del rinvio dovesse rilevare – cosa che non risulta chiaramente dagli atti – che, quando gli internauti cliccano sul collegamento in esame, l’opera appare dando l’impressione di essere a disposizione sul sito in cui si trova tale collegamento, mentre in realtà proviene da un altro sito.

30. Infatti, tale circostanza aggiuntiva non modifica affatto la conclusione secondo cui la fornitura su un sito di un collegamento cliccabile verso un’opera protetta, pubblicata e liberamente accessibile su un altro sito, ha l’effetto di mettere a disposizione degli utilizzatori del primo sito l’opera medesima e costituisce, quindi, una comunicazione al pubblico. Tuttavia, dal momento che non vi è un pubblico nuovo, per tale comunicazione al pubblico in ogni caso non è necessaria l’autorizzazione dei titolari del diritto d’autore.

31. Per contro, nell’ipotesi in cui un collegamento cliccabile consenta agli utilizzatori del sito in cui si trova tale collegamento di eludere misure restrittive adottate dal sito in cui l’opera protetta si trova per limitare l’accesso del pubblico ai soli abbonati e, in tal modo, costituisca un intervento senza il quale tali utilizzatori non potrebbero beneficiare delle opere diffuse, il complesso di tali utilizzatori dovrà essere considerato quale pubblico nuovo, che non è stato preso in considerazione dai titolari del diritto d’autore al momento in cui hanno autorizzato la comunicazione iniziale, ragion per cui per tale comunicazione al pubblico si impone l’autorizzazione dei titolari. Ciò avviene, in particolare, allorché l’opera non sia più a disposizione del pubblico sul sito in cui sia stata comunicata inizialmente o sia ormai disponibile su tale sito esclusivamente per un pubblico ristretto, mentre sia accessibile su un altro sito Internet senza autorizzazione degli aventi diritto.

32. Pertanto, occorre rispondere alle prime tre questioni proposte che l’art.3, §1, della direttiva 2001/29 deve essere interpretato nel senso che non costituisce un atto di comunicazione al pubblico, ai sensi di tale disposizione, la messa a disposizione su un sito Internet di collegamenti cliccabili verso opere liberamente disponibili su un altro sito Internet.

**Sulla quarta questione**

33. Con la sua quarta questione il giudice del rinvio chiede, in sostanza, se l’art.3, §1, della direttiva 2001/29 debba essere interpretato nel senso che osti a che uno Stato membro possa stabilire una tutela maggiore per i titolari del diritto d’autore, prevedendo che la nozione di comunicazione al pubblico comprenda più forme di messa a disposizione di quante stabilite in tale articolo.

34. A tale proposito, risulta segnatamente dai considerando 1, 6 e 7 della direttiva 2001/29 che quest’ultima è volta, in particolare, a rimediare all’incoerenza normativa e all’incertezza giuridica che accompagnano la protezione del diritto d’autore. Orbene, ammettere che uno Stato membro possa stabilire una tutela maggiore per i titolari del diritto d’autore prevedendo che la nozione di comunicazione al pubblico comprenda altrimenti operazioni diverse da quelle elencate all’art.3, §1, della direttiva 2001/29, avrebbe l’effetto di creare incoerenza normativa e, quindi, incertezza giuridica per i terzi.

35. Di conseguenza, l’obiettivo perseguito dalla direttiva 2001/29 risulterebbe inevitabilmente compromesso se la nozione di comunicazione al pubblico potesse essere intesa dai diversi Stati membri come comprendente più forme di messa a disposizione di quelle stabilite all’art.3, §1, di tale direttiva.

36. È pur vero che il considerando 7 della summenzionata direttiva non è finalizzato a sopprimere o a prevenire le disparità che non incidono negativamente sul funzionamento del mercato interno. Tuttavia, si deve rilevare che, se agli Stati membri dovesse essere riconosciuta la facoltà di stabilire che la nozione di comunicazione al pubblico comprende più forme di messa a disposizione rispetto a quelle previste all’art.3, §1, della direttiva stessa, il funzionamento del mercato interno ne risulterebbe necessariamente compromesso.

37. Ne consegue che l’art.3, §1, della direttiva 2001/29 non può essere inteso nel senso che consenta agli Stati membri di stabilire una tutela maggiore per i titolari del diritto d’autore, prevedendo che la nozione di comunicazione al pubblico comprenda più forme di messa a disposizione di quelle disposte da tale articolo.

38. Tale conclusione non è iniziata dalla circostanza, dedotta dai ricorrenti nel procedimento principale nelle loro osservazioni scritte, che l’art.20 della Convenzione di Berna prevede che i
Paesi firmatari possano concludere «accordi particolari» per conferire ai titolari di diritti d’autore diritti più ampi di quelli riconosciuti da tale Convenzione.


40. Poiché l’obiettivo della direttiva 2001/29 risulterebbe inevitabilmente compromesso se la nozione di comunicazione al pubblico fosse intesa come comprendente più forme di messa di disposizione di quante stabilite all’art.3, §1, di tale direttiva, uno Stato membro deve evitare di utilizzare la facoltà attribuitagli dall’art.20 della Convenzione di Berna.

41. Di conseguenza, occorre rispondere alla quarta questione dichiarando che l’art.3, §1, della direttiva 2001/29 deve essere interpretato nel senso che osta a che uno Stato membro possa stabilire una maggiore tutela dei titolari del diritto d’autore, includendo nella nozione di comunicazione al pubblico più forme di messa a disposizione di quelle disposte da tale articolo.

Per questi motivi, la Corte (Quarta Sezione) dichiara:

1) L’art.3, §1, della direttiva 2001/29/CE [...], del 22 maggio 2001, sull’armonizzazione di taluni aspetti del diritto d’autore e dei diritti connessi nella società dell’informazione, deve essere interpretato nel senso che non costituisce un atto di comunicazione al pubblico, ai sensi di tale disposizione, la messa a disposizione su un sito Internet di collegamenti cliccabili verso opere liberamente disponibili su un altro sito Internet.

2) L’art.3, §1, della direttiva 2001/29 deve essere interpretato nel senso che osta a che uno Stato membro possa stabilire una maggiore tutela dei titolari del diritto d’autore, includendo nella nozione di comunicazione al pubblico più forme di messa a disposizione di quelle disposte da tale articolo.

*****

DISCUSSIONE

1. Fornire link verso opere tutelate dal diritto d’autore è qualificabile come “messa a disposizione” e quindi come “atto di comunicazione”, ai sensi della normativa in materia?

2. Fornire link verso opere tutelate dal diritto d’autore viola la normativa in materia? Perché?

3. Cosa si intende per «pubblico» e per «pubblico nuovo»?

4. Gli Stati possono stabilire, in relazione alla fattispecie, una maggiore tutela per i titolari del diritto d’autore?

*****

NORME

- art.3 §1, direttiva 2001/29/CE
11.3. Diritti d’autore e cache

Corte di Giustizia dell’Unione Europea, 5 giugno 2014 (causa C-360/13)

[...] 1. La domanda di pronuncia pregiudiziale verte sull’interpretazione dell’art.5, §1, della direttiva 2001/29/CE [...] del 22 maggio 2001, sull’armonizzazione di taluni aspetti del diritto d’autore e dei diritti connessi nella società dell’informazione [...].

2. Tale domanda è stata presentata nell’ambito di una controversia tra la Public Relations Consultants Association Ltd (in prosieguo: la «PRCA») e la Newspaper Licensing Agency Ltd e a. (in prosieguo: la «NLA») in merito all’obbligo di ottenere un’autorizzazione dei titolari di diritti d’autore per la consultazione di siti Internet che comporta la realizzazione di copie di tali siti sullo schermo del computer dell’utente e nella «cache» Internet del disco fisso di tale computer.

Procedimento principale e questione pregiudiziale

7. La PRCA è un’organizzazione che raggruppa professionisti in relazioni pubbliche. Questi ultimi hanno usufruito del servizio di monitoraggio dei media proposto dal gruppo di società Meltwater (in prosieguo: la «Meltwater») che mette a loro disposizione online relazioni di monitoraggio di articoli di stampa pubblicati su Internet, realizzate in base a parole chiave fornite dai clienti.

8. La NLA è un organismo creato dagli editori di quotidiani del Regno Unito al fine di fornire licenze collettive riguardanti il contenuto dei quotidiani.

9. La NLA ha ritenuto che la Meltwater e i suoi clienti dovessero ottenere un’autorizzazione dei titolari di diritti d’autore per, rispettivamente, fornire e ricevere il servizio di monitoraggio dei media.

10. La Meltwater ha acconsentito a sottoscrivere una licenza di base di dati Internet. Tuttavia la PRCA ha continuato a sostenere che la ricezione online delle relazioni di monitoraggio da parte dei clienti della Meltwater non richiedeva alcuna licenza.

11. Adite della controversia, la High Court of Justice (England & Wales), Chancery Division, e la Court of Appeal (England & Wales) hanno stabilito che i membri della PRCA dovevano ottenere una licenza o un consenso della NLA per ricevere il servizio della Meltwater.

12. La PRCA ha impugnato tale decisione dinanzi alla Supreme Court of the United Kingdom, sostenendo in particolare che i suoi membri non avevano bisogno di alcuna autorizzazione dei titolari di diritti qualora si limitassero a consultare le relazioni di monitoraggio sul sito Internet della Meltwater.

13. La NLA ha sostenuto che per tale attività è necessaria dell’autorizzazione dei titolari di diritti d’autore, in quanto la consultazione del sito Internet comporta la realizzazione di copie sullo schermo del computer dell’utente (in prosieguo: le «copie sullo schermo») e di copie nella «cache» Internet del disco fisso di tale computer (in prosieguo: le «copie nella cache»). Orbene, tali copie costituirebbero «riproduzioni» ai sensi dell’art.2 della direttiva 2001/29 che non rientrerebbero nell’esenzione prevista all’art.5, §1, di tale direttiva.

14. Il giudice del rinvio rileva che il procedimento instaurato dinanzi ad esso verte sulla questione se gli utenti, che consultano siti Internet sui loro computer, senza scaricare o stampare i siti medesimi, violino il diritto d’autore mediante la realizzazione di copie sullo schermo e di copie nella cache, a meno che dispongano dell’autorizzazione dei titolari di diritti a realizzare tali copie.

15. A tale riguardo, il giudice del rinvio indica anzitutto che, qualora un utente consulti, senza scaricarlo, un sito Internet sul proprio computer, i procedimenti tecnologici in esame presuppongono necessariamente la realizzazione di dette copie. Tale realizzazione è la conseguenza automatica della navigazione in Internet e non richiede altro intervento umano oltre alla decisione di accedere al sito Internet in questione. Le copie sullo schermo e le copie nella cache sono conservate non oltre la durata dei normali processi relativi all’utilizzo di Internet. Inoltre la cancellazione di tali copie non richiede alcun intervento umano. Vero è che le copie create nella cache possono essere deliberatamente cancellate dall’utente in questione. Tuttavia, se ciò non avviene, tali copie sono di norma sovrascritte da altro materiale dopo un certo intervallo, che
dipende dalla capacità della cache, nonché dal volume e dalla frequenza dell’utilizzo di Internet da parte dell’utente medesimo.

16. Il giudice del rinvio precisa inoltre che la copia sullo schermo è una parte essenziale della tecnologia applicata, senza la quale il sito Internet non può essere visualizzato, e rimarrà sullo schermo fino a quando l’utente non esce dal medesimo. La cache Internet è una caratteristica universale dell’attuale tecnologia di navigazione in rete, senza la quale Internet non sarebbe in grado di far fronte agli attuali volumi di trasmissione di dati online e non funzionerebbe a dovere. La realizzazione di copie sullo schermo e di copie nella cache è quindi indispensabile per il funzionamento corretto ed efficiente dei procedimenti tecnologici che la navigazione in rete comporta.

17. Infine tale giudice sottolinea che, di norma, durante la navigazione, l’utente di Internet non ha l’intenzione di realizzare una copia dell’immagine, a meno che non scelga di scaricarla o di stamparla. Il suo obiettivo è quello di visualizzare il contenuto del sito Internet scelto. Le copie sullo schermo e le copie nella cache sono pertanto solo la conseguenza accessoria dell’utilizzo del suo computer per consultare un sito Internet.

18. Alla luce dei suesposti rilievi, il giudice del rinvio ha concluso che le copie sullo schermo e le copie nella cache soddisfano i requisiti previsti all’art. 5, §1, della direttiva 2001/29. Tuttavia, un rinvio pregiudiziale alla Corte sarebbe opportuno al fine di garantire l’applicazione uniforme del diritto dell’Unione in tutto il territorio dell’Unione Europea.

19. A tale riguardo, esso precisa di nutrire un dubbio relativo alla questione se dette copie siano temporanee, transitorie o accessorie e se costituiscono una parte integrante del procedimento tecnologico. Per contro, esso ritiene che siffatte copie soddisfino necessariamente gli altri requisiti previsti all’art. 5, §1, di tale direttiva.

20. Ciò considerato, la Supreme Court of the United Kingdom ha deciso di sospendere il procedimento e di sottoporre alla Corte la seguente questione pregiudiziale:

«Nell’ipotesi in cui:
– un utente finale visualizzi una pagina Internet senza scaricarla, stamparla o prefiggersi di farne altrimenti una copia;
– copie di tale pagina Internet siano automaticamente create sullo schermo e nella cache sul disco fisso [del computer] dell’utente finale;
– la creazione di tali copie sia indispensabile per i procedimenti tecnologici che consentono una corretta ed efficiente navigazione in rete;
– la copia sullo schermo rimanga sul medesimo fino a quando l’utente finale esce dalla pagina Internet di cui trattasi, momento in cui la copia è automaticamente cancellata dal normale funzionamento del computer;
– la copia nella cache vi rimanga fino a quando è sovrascritta da altro materiale, quando l’utente finale visualizza altre pagine Internet, momento in cui viene automaticamente cancellata dal normale funzionamento del computer; nonché
– le copie siano conservate solo per il tempo necessario ai regolari processi connessi all’utilizzo di Internet di cui ai precedenti [trattini quarto e quinto], se siffatte copie siano temporanee, transitorie o accessorie e costituiscono parte integrante ed essenziale del procedimento tecnologico, ai sensi dell’art. 5, §1, della direttiva 2001/29/CE».

Sulla questione pregiudiziale

21. Con la sua questione il giudice del rinvio chiede sostanzialmente se l’art. 5 della direttiva 2001/29 debba essere interpretato nel senso che le copie sullo schermo e le copie nella cache, realizzate da un utente finale durante la consultazione di un sito Internet, soddisfino i requisiti in base ai quali tali copie devono essere temporanee, transitorie o accessorie e costituire una parte integrante ed essenziale di un procedimento tecnologico, e quindi se tali copie possano essere realizzate senza l’autorizzazione dei titolari dei diritti d’autore.

Osservazioni preliminari

22. Ai sensi dell’art. 5, §1, della direttiva 2001/29, un atto di riproduzione è esentato dal diritto di riproduzione previsto all’art. 2 di tale direttiva a condizione:
– che sia temporaneo;
– che sia transitorio o accessorio;
– che costituisca parte integrante ed essenziale di un procedimento tecnologico;
– che sia eseguito all’unico scopo di consentire la trasmissione in rete tra terzi con l’intervento di un intermediario o un utilizzo legittimo di un’opera o di altri materiali, e
— che sia privo di rilievo economico proprio.

23. Dalla giurisprudenza della Corte emerge che i requisiti indicati supra devono essere oggetto di un’interpretazione restrittiva, in quanto l’art.5, §1, della direttiva 2001/29 costituisce una deroga alla regola generale sancita dalla medesima, che impone che sia il titolare dei diritti d’autore ad autorizzare qualsiasi riproduzione delle sue opere protette (sentenze Infopaq International, C-5/08, […], p.ti 56 e 57, nonché Football Association Premier League e a., C-403/08 e C-429/08, […], p.to 162).

24. Ciò premesso, dalla stessa giurisprudenza risulta che l’esenzione prevista dalla suddetta disposizione deve consentire e assicurare lo sviluppo ed il funzionamento di nuove tecnologie, nonché mantenere un giusto equilibrio tra i diritti e gli interessi dei titolari di diritti e degli utilizzatori delle opere protette che intendano beneficiare di tali tecnologie (v. sentenza Football Association Premier League e a., […], p.to 164).

Sul rispetto delle condizioni previste all’art.5, §1, della direttiva 2001/29

25. Il giudice del rinvio ha indicato che le copie sullo schermo e le copie nella cache soddisfano il quarto e il quinto requisito di cui all’art.5, §1, della direttiva 2001/29, di modo che solo il rispetto dei primi tre requisiti costituisce l’oggetto del rinvio medesimo.

26. Per quanto riguarda il primo requisito, in base al quale l’atto di riproduzione dev’essere temporaneo, dal fascicolo risulta, da un lato, che le copie sullo schermo sono cancellate quando l’utente esce dal sito Internet consultato. Dall’altro, le copie nella cache sono di norma sovrascritte da altro materiale dopo un certo intervallo, che dipende dalla capacità della cache, nonché dal volume e dalla frequenza dell’utilizzo di Internet da parte dell’utente medesimo. Ne risulta che tali copie hanno un carattere temporaneo.

27. Alla luce di ciò, si deve constatare che dette copie rispettano il primo requisito di cui all’art.5, §1, della direttiva 2001/29.


29. Per quanto riguarda, anzitutto, il primo di questi due elementi, occorre rilevare che, nel procedimento principale, le copie sullo schermo e le copie nella cache sono create ed eliminate dal procedimento tecnologico utilizzato per la consultazione dei siti Internet, di modo che esse sono realizzate interamente nell’ambito del procedimento medesimo.

30. A tale riguardo non rileva il fatto che il procedimento in questione sia avviato dall’utente di Internet e che sia concluso da un atto di riproduzione temporaneo quale la copia sullo schermo.

31. Dalla giurisprudenza della Corte risulta infatti che, dal momento che l’art.5, §1, della direttiva 2001/29 non precisa in quale fase del procedimento tecnologico debbano intervenire gli atti di riproduzione temporanea, non può escludersi che un simile atto dia avvio a tale procedimento oppure lo concluda (ordinanza Infopaq International, […], p.to 31).

32. Risulta inoltre dalla giurisprudenza che tale disposizione non ostena che il procedimento tecnologico implichi un intervento umano e, in particolare, che sia avviato o concluso manualmente (v., in tal senso, ordinanza Infopaq International, […], p.to 32).

33. Ne risulta che le copie sullo schermo e le copie nella cache devono essere considerate parte integrante del procedimento tecnologico di cui trattasi nel procedimento principale.

34. Per quanto concerne poi il secondo degli elementi di cui al p.to 28 della presente sentenza, dalla decisione di rinvio risulta che, anche se il procedimento di cui trattasi nel procedimento principale può essere avviato senza l’intervento degli atti di riproduzione di cui trattasi, tuttavia, in tal caso, detto procedimento non può funzionare correttamente ed efficacemente.

35. Infatti, secondo la decisione di rinvio, le copie nella cache agevolano notevolmente la navigazione in Internet, dal momento che quest’ultimo, senza tali copie, non sarebbe in grado di far fronte agli attuali volumi di trasmissione di dati online. Senza la realizzazione di siffatte copie, il procedimento utilizzato per la consultazione di siti Internet sarebbe decisamente meno efficace e non sarebbe in grado di funzionare correttamente.
36. Riguardo alle copie sullo schermo, non è stato contestato che, allo stato attuale, la tecnologia della visualizzazione di siti Internet sui computer presuppone la realizzazione di siffatte copie per poter funzionare in maniera corretta ed efficace.

37. Di conseguenza, le copie sullo schermo e le copie nella cache devono essere considerate una parte essenziale del procedimento tecnologico di cui trattasi nel procedimento principale.

38. Ne risulta che le due categorie di copie soddisfano il terzo requisito previsto all’art. 5, §1, della direttiva 2001/29.

39. Il secondo requisito, che occorre esaminare in terzo luogo, è un requisito alternativo. L’atto di riproduzione deve infatti essere o transitorio o accessorio.

40. Per quanto riguarda il primo dei due elementi, si deve ricordare che un atto può essere qualificato come «transitorio» esclusivamente qualora la sua durata sia limitata a quanto necessario per il buon funzionamento del procedimento tecnologico utilizzato, restando inteso che tale procedimento deve essere automatizzato in modo tale da cancellare detto atto in maniera automatica, senza intervento umano, nel momento in cui è esaurita la sua funzione tesa a consentire la realizzazione di un siffatto procedimento (v., in tal senso, sentenza Infopaq International, […], p.to 64).

41. Ciò premesso, il requisito di una cancellazione automatica non osta a che una siffatta cancellazione sia preceduta da un intervento umano diretto a porre fine all’utilizzo del procedimento tecnologico. Infatti, come rilevato al p.to 32 della presente sentenza, è consentito che il procedimento tecnologico di cui trattasi nel procedimento principale sia avviato e concluso manualmente.

42. Pertanto, contrariamente a quanto sostenuto dalla NLA, un atto di riproduzione non perde il suo carattere transitorio per il solo fatto che la cancellazione da parte del sistema della copia generata è preceduta dall’intervento dell’utente finale teso a porre fine al procedimento tecnologico di cui trattasi.

43. Per quanto concerne l’altro elemento di cui al p.to 39 della presente sentenza, un atto di riproduzione potrà essere qualificato come «accessorio» se non ha né un’esistenza né una finalità autonome rispetto al procedimento tecnologico di cui fa parte.

44. Nel procedimento principale, per quanto riguarda anzitutto le copie sullo schermo, occorre ricordare che esse sono cancellate automaticamente dal computer nel momento in cui l’utente esce dal sito Internet in questione e, quindi, nel momento in cui pone fine al procedimento tecnologico utilizzato per la consultazione di tale sito.

45. A tale riguardo è indifferente, contrariamente a quanto sostenuto dalla NLA, che la copia sullo schermo continui ad esistere fintantoché l’utente lasci acceso il computer e rimanga sul sito Internet in questione, dato che, durante tale periodo, il procedimento tecnologico utilizzato per la consultazione di tale sito rimane attivo.

46. Si deve pertanto constatare che la durata delle copie sullo schermo è limitata a quanto necessario per il buon funzionamento del procedimento tecnologico utilizzato per la consultazione del sito Internet in questione. Di conseguenza, tali copie devono essere qualificate come «transitorie».

47. Per quanto riguarda poi le copie nella cache, si deve certamente rilevare che, a differenza delle copie sullo schermo, esse non sono cancellate nel momento in cui l’utente pone fine al procedimento tecnologico utilizzato per la consultazione del sito Internet in questione, dal momento che esse sono conservate nella cache ai fini di un’eventuale ulteriore consultazione di tale sito.

48. Tuttavia non è necessario che siffatte copie siano qualificate come «transitorie», una volta stabilito che esse possiedono un carattere accessorio per quanto riguarda il procedimento tecnologico utilizzato.

49. A tale riguardo occorre rilevare, da un lato, che il procedimento tecnologico in questione determina interamente la finalità per cui tali copie sono realizzate e utilizzate, mentre tale procedimento, come risulta dal p.to 34, può funzionare, sebbene in modo meno efficace, senza che siano realizzate siffatte copie. Dall’altro, dal fascicolo risulta che gli utenti che utilizzano il procedimento tecnologico di cui trattasi nel procedimento principale non possono realizzare le copie nella cache al di fuori di tale procedimento.
50. Ne risulta che le copie nella *cache* non hanno né un’esistenza né una finalità autonoma rispetto al procedimento tecnologico di cui trattasi nel procedimento principale e devono pertanto essere qualificate come «accessorie».

51. In tale contesto, si deve constatare che le copie sullo schermo e le copie nella *cache* soddisfano il secondo requisito previsto all’art.5, §1, della direttiva 2001/29.

52. Alla luce dei susposti rilievi, occorre constatare che le copie di cui trattasi nel procedimento principale soddisfano i primi tre requisiti previsti da tale disposizione.

53. Ciò premesso, per poter sollevare l’eccezione prevista dalla menzionata disposizione, come interpretata al punto precedente della presente sentenza, occorre inoltre che tali copie soddisfino i requisiti stabiliti all’art.5, §5, della direttiva 2001/29 (v., in tal senso, sentenza Football Association Premier League e a., […] p.to 181).

**Sul rispetto delle condizioni previste all’art.5, §5, della direttiva 2001/29**

54. Conformemente all’art.5, §5, della direttiva 2001/29, la realizzazione di un atto di riproduzione transitorio è esentata dal diritto di riproduzione solo in determinati casi specifici, che non pregiudicano il normale sfruttamento dell’opera e non violano indebitamente gli interessi legittimi del titolare dei diritti.

55. A tale riguardo occorre ricordare anzitutto che le copie sullo schermo e le copie nella *cache*, dal momento che sono realizzate con l’unico scopo di consultare siti Internet, costituiscono a tale titolo un caso specifico.

56. Inoltre tali copie non pregiudicano in modo ingiustificato gli interessi legittimi dei titolari dei diritti d’autore, sebbene consentano agli utenti, in linea di principio, l’accesso, senza l’autorizzazione di detti titolari, alle opere presentate su siti Internet.

57. A tale riguardo occorre rilevare che le opere sono messe a disposizione degli utenti dagli editori dei siti Internet i quali si sono tenuti, conformemente all’art.3, §1, della direttiva 2001/29, ad ottenere un’autorizzazione dei titolari dei diritti d’autore interessati, poiché tale messa a disposizione costituisce una comunicazione al pubblico ai sensi del suddetto articolo.


59. In tale contesto, non è giustificato esigere dagli utenti di Internet che ottengano un’ulteriore autorizzazione che consenta loro di usufruire di questa stessa comunicazione già autorizzata dal titolare dei diritti d’autore in questione.

60. Occorre infine constatare che la realizzazione delle copie sullo schermo e delle copie nella *cache* non pregiudica il regolare sfruttamento delle opere.

61. A tale riguardo occorre rilevare che la consultazione dei siti Internet mediante il procedimento tecnologico in esame rappresenta un regolare sfruttamento delle opere che consenti agli utenti di Internet di usufruire della comunicazione al pubblico effettuata dall’editore del sito Internet in questione. Dato che la realizzazione delle copie in questione fa parte di detta consultazione, essa non può arrecare pregiudizio ad un siffatto sfruttamento delle opere.

62. Da quanto precede risulta che le copie sullo schermo e le copie nella *cache* soddisfano i requisiti previsti all’art.5, §5, della direttiva 2001/29.

63. In tale contesto, occorre rispondere alla questione sollevata dichiarando che l’art.5 della direttiva 2001/29 dev’essere interpretato nel senso che le copie sullo schermo e le copie nella *cache*, realizzate da un utente finale durante la consultazione di un sito Internet, soddisfano i requisiti in base ai quali tali copie devono essere temporanee, transitorie o accessorie e costituire una parte integrante ed essenziale di un procedimento tecnologico, nonché i requisiti stabiliti all’art.5, §5, di tale direttiva, e possono pertanto essere realizzate senza l’autorizzazione dei titolari di diritti d’autore.

[…]

Per questi motivi, la Corte (Quarta Sezione) dichiara:

L’art.5 della direttiva 2001/29/CE […] del 22 maggio 2001, sull’armonizzazione di taluni aspetti del diritto d’autore e dei diritti connessi nella società dell’informazione, dev’essere interpretato nel senso che le copie sullo schermo del computer dell’utente e le copie nella «cache» del disco fisso di tale computer, realizzate da un utente finale durante la consultazione di un sito Internet, soddisfano i requisiti in base ai quali tali copie devono essere temporanee, transitorie o accessorie e costituire una parte integrante ed essenziale di un procedimento tecnologico, nonché i requisiti stabiliti all’ art.5, §5, di tale direttiva, e possono pertanto essere realizzate senza l’autorizzazione dei titolari di diritti d’autore.
DISCUSSIONE

1. Cosa si intende per copie sullo schermo del computer e copie nella cache Internet del disco fisso? Quale è la loro funzione?
2. Tali copie sono create (e cancellate) automaticamente o è necessario l’intervento dell’utente finale?
3. Tali copie sono, ai sensi della normativa su diritto d’autore e società dell’informazione, da considerare riproduzioni e quindi soggette al pagamento dei relativi diritti? In base a quali criteri?

NORME

- art.5, direttiva 2001/29/CE
12. L'USO DI INTERNET SUL LUOGO DI LAVORO
12.1. Controlli in Rete sul lavoratore e privacy

European Court of Human Rights, Fourth Section, 3 April 2007 – appl. n.62617/00
(Copland v. United Kingdom)

Procedure
1. The case originated in an application (n.62617/00) against the United Kingdom of Great Britain and Northern Ireland lodged with the Court under Article 34 of the Convention for the Protection of Human Rights and Fundamental Freedoms ("the Convention") by Ms Lynette Copland.

[...] 3. The applicant complained about the monitoring of her telephone calls, e-mail correspondence and Internet usage under Articles 8 and 13.

[...] The facts
I. The circumstances of the case
[...]
7. In 1991 the applicant was employed by Carmarthenshire College ("the College").[...]

8. In 1995 the applicant became the personal assistant to the College Principal ("CP") and from the end of 1995 she was required to work closely with the newly appointed Deputy Principal ("DP").

9. In about July 1998, whilst on annual leave, the applicant visited another campus of the College with a male director. She subsequently became aware that the DP had contacted that campus to enquire about her visit and understood that he was suggesting an improper relationship between her and the director.

10. During her employment, the applicant's telephone, e-mail and Internet usage were subjected to monitoring at the DP's instigation. According to the Government, this monitoring took place in order to ascertain whether the applicant was making excessive use of College facilities for personal purposes. The Government stated that the monitoring of telephone usage consisted of analysis of the college telephone bills showing telephone numbers called, the dates and times of the calls and their length and cost. The applicant also believed that there had been detailed and comprehensive logging of the length of calls, the number of calls received and made and the telephone numbers of individuals calling her. She stated that on at least one occasion the DP became aware of the name of an individual with whom she had exchanged incoming and outgoing telephone calls. The Government submitted that the monitoring of telephone usage took place for a few months up to about 22 November 1999. The applicant contended that her telephone usage was monitored over a period of about 18 months until November 1999.

11. The applicant's Internet usage was also monitored by the DP. The Government accepted that this monitoring took the form of analysing the websites visited, the times and dates of the visits to the websites and their duration and that this monitoring took place from October to November 1999. The applicant did not comment on the manner in which her Internet usage was monitored but submitted that it took place over a much longer period of time than the Government admit.

12. In November 1999 the applicant became aware that enquiries were being made into her use of e-mail at work when her step-daughter was contacted by the College and asked to supply information about e-mails that she had sent to the College. The applicant wrote to the CP to ask whether there was a general investigation taking place or whether her e-mails only were being investigated. By an e-mail dated 24 November 1999 the CP advised the applicant that, whilst all e-mail activity was logged, the information department of the College was investigating only her e-mails, following a request by the DP.

13. The Government submitted that monitoring of e-mails took the form of analysis of e-mail addresses and dates and times at which e-mails were sent and that the monitoring occurred for a few months prior to 22 November 1999. According to the applicant the monitoring of e-mails occurred for at least six months from May 1999 to November 1999. She provided documentary evidence in the form of printouts detailing her e-mail usage from 14 May 1999 to 22 November 1999 which set out the date and time of e-mails sent from her e-mail account together with the
14. By a memorandum dated 29 November 1999 the CP wrote to the DP to confirm the contents of a conversation they had had in the following terms:

“To avoid ambiguity I felt it worthwhile to confirm my views expressed to you last week, regarding the investigation of [the applicant's] e-mail traffic.

Subsequent to the applicant becoming aware that someone from the College had been following up her e-mails, I spoke to ST who confirmed that this was true and had been instigated by yourself. Given the forthcoming legislation making it illegal for organisations to examine someone's e-mail without permission, I naturally felt concerned over recent events and instructed ST not to carry out any further analysis. Furthermore, I asked you to do likewise and asked that any information you have of concern regarding the applicant be forwarded to me as a matter of priority. You indicated that you would respond positively to both requests, whilst re-affirming your concerns regarding the applicant”.

15. There was no policy in force at the College at the material time regarding the monitoring of telephone, e-mail or Internet use by employees.

16. In about March or April 2000 the applicant was informed by other members of staff at the College that between 1996 and late 1999 several of her activities had been monitored by the DP or those acting on his behalf. The applicant also believed that people to whom she had made calls were in turn telephoned by the DP, or those acting on his behalf, to identify the callers and the purpose of the call. She further believed that the DP became aware of a legally privileged fax that was sent by herself to her solicitors and that her personal movements, both at work and when on annual or sick leave, were the subject of surveillance.

17. The applicant provided the Court with statements from other members of staff alleging inappropriate and intrusive monitoring of their movements. The applicant, who is still employed by the College, understands that the DP has been suspended.

[...]

I. Alleged violation of article 8 of the Convention

29. The applicant alleged that the monitoring activity that took place amounted to an interference with her right to respect for private life and correspondence under Article 8, which reads as follows:

“1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others”.

[...]

B. The Court’s assessment

[...]

1. Scope of private life

41. According to the Court's case-law, telephone calls from business premises are prima facie covered by the notions of “private life” and “correspondence” for the purposes of Article 8, §1 (see Halford, [...] §44 and Amann v. Switzerland -GC-, n.27798/95, §43, [...] ). It follows logically that e-mails sent from work should be similarly protected under Article 8, as should information derived from the monitoring of personal Internet usage.

42. The applicant in the present case had been given no warning that her calls would be liable to monitoring, therefore she had a reasonable expectation as to the privacy of calls made from her work telephone (see Halford, §45). The same expectation should apply in relation to the applicant's e-mail and Internet usage.

2. Whether there was any interference with the rights guaranteed under Article 8.

43. The Court recalls that the use of information relating to the date and length of telephone conversations and in particular the numbers dialled can give rise to an issue under Article 8 as such information constitutes an “integral element of the communications made by telephone” (see Malone v. the United Kingdom, judgment of 2 August 1984 [...] §84). The mere fact that these data may have been legitimately obtained by the College, in the form of telephone bills, is no bar to finding an interference with rights guaranteed under Article 8 [...] . Moreover, storing of personal
data relating to the private life of an individual also falls within the application of Article 8, §1 (see Amann […] §65). Thus, it is irrelevant that the data held by the college were not disclosed or used against the applicant in disciplinary or other proceedings.

44. Accordingly, the Court considers that the collection and storage of personal information relating to the applicant's telephone, as well as to her e-mail and Internet usage, without her knowledge, amounted to an interference with her right to respect for her private life and correspondence within the meaning of Article 8.

3. Whether the interference was “in accordance with the law”

45. The Court recalls that it is well established in the case-law that the term “in accordance with the law” implies - and this follows from the object and purpose of Article 8 - that there must be a measure of legal protection in domestic law against arbitrary interferences by public authorities with the rights safeguarded by Article 8, §1. This is all the more so in areas such as the monitoring in question, in view of the lack of public scrutiny and the risk of misuse of power (see Halford […] §49).

46. This expression not only requires compliance with domestic law, but also relates to the quality of that law, requiring it to be compatible with the rule of law (see, inter alia, Khan v. the United Kingdom, judgment of 12 May 2000 […] §26; P.G. and J.H. v. the United Kingdom […] §44). In order to fulfil the requirement of foreseeability, the law must be sufficiently clear in its terms to give individuals an adequate indication as to the circumstances in which and the conditions on which the authorities are empowered to resort to any such measures (see Halford […] §49 and Malone […] §67).

47. The Court is not convinced by the Government’s submission that the College was authorised under its statutory powers to do “anything necessary or expedient” for the purposes of providing higher and further education, and finds the argument unpersuasive. Moreover, the Government do not seek to argue that any provisions existed at the relevant time, either in general domestic law or in the governing instruments of the College, regulating the circumstances in which employers could monitor the use of telephone, e-mail and the Internet by employees. Furthermore, it is clear that the Telecommunications (Lawful Business Practice) Regulations 2000 […] which make such provision were not in force at the relevant time.

48. Accordingly, as there was no domestic law regulating monitoring at the relevant time, the interference in this case was not “in accordance with the law” as required by Article 8, §2, of the Convention. The Court would not exclude that the monitoring of an employee's use of a telephone, e-mail or Internet at the place of work may be considered “necessary in a democratic society” in certain situations in pursuit of a legitimate aim. However, having regard to its above conclusion, it is not necessary to pronounce on that matter in the instant case.

49. There has therefore been a violation of Article 8 in this regard.

[…]

For these reasons, the Court unanimously

1. Holds that there has been a violation of Article 8 of the Convention;

[…]

*****

DISCUSSIONE

1. La raccolta, da parte del datore di lavoro, dei dati relativi a telefonate, uso di Internet ed e-mail, costituisce un’interferenza con la vita privata del lavoratore?

2. Se sì, tale interferenza è da considerarsi giustificata dalla legge o è da considerarsi indebita? Perché?

*****

NORME

- artt.8,13, CEDU
12.2. Controllo della corrispondenza sul luogo di lavoro

European Court of Human Rights, Grand Chamber, 5 September 2017, appl. n.61496/08 (Bărbulescu v. Romania)

Procedure
1. The case originated in an application (no. 61496/08) against Romania lodged with the Court under Article 34 of the Convention for the Protection of Human Rights and Fundamental Freedoms ("the Convention") by a Romanian national, Mr Bogdan Mihai Bărbulescu ("the applicant"), on 15 December 2008.

[…] 3. The applicant complained, in particular, that his employer's decision to terminate his contract had been based on a breach of his right to respect for his private life and correspondence as enshrined in Article 8 of the Convention and that the domestic courts had failed to comply with their obligation to protect that right.

The facts
I. The circumstances of the case
10. The applicant was born in 1979 and lives in Bucharest.
11. From 1 August 2004 to 6 August 2007 he was employed in the Bucharest office of S., a Romanian private company ("the employer"), as a sales engineer. At his employer's request, for the purpose of responding to customers' enquiries, he created an instant messaging account using Yahoo Messenger, an online chat service offering real-time text transmission over the internet. He already had another personal Yahoo Messenger account.
12. The employer's internal regulations prohibited the use of company resources by employees in the following terms: Article 50 "Any disturbance of order and discipline on company premises shall be strictly forbidden, in particular: ... —... personal use of computers, photocopiers, telephones or telex or fax machines."
13. The regulations did not contain any reference to the possibility for the employer to monitor employees' communications.
14. It appears from documents submitted by the Government that the applicant had been informed of the employer's internal regulations and had signed a copy of them on 20 December 2006 after acquainting himself with their contents.
15. On 3 July 2007 the Bucharest office received and circulated among all its employees an information notice that had been drawn up and sent by the Cluj head office on 26 June 2007. The employer asked employees to acquaint themselves with the notice and to sign a copy of it. The relevant parts of the notice read as follows:
"1. ... Time spent in the company must be quality time for everyone! Come to work to deal with company and professional matters, and not your own personal problems! Don't spend your time using the internet, the phone or the fax machine for matters unconnected to work or your duties. This is what [elementary education], common sense and the law dictate! The employer has a duty to supervise and monitor employees' work and to take punitive measures against anyone at fault!
Your misconduct will be carefully monitored and punished!
2. Because of repeated [disciplinary] offences vis-à-vis her superior, [as well as] her private use of the internet, the telephone and the photocopier, her negligence and her failure to perform her duties, Ms B.A. was dismissed on disciplinary grounds! Take a lesson from her bad example! Don't make the same mistakes!
3. Have a careful read of the collective labour agreement, the company's internal regulations, your job description and the employment contract you have signed! These are the basis of our collaboration! Between employer and employee! ..."
16. It also appears from the documents submitted by the Government, including the employer's attendance register, that the applicant acquainted himself with the notice and signed it between 3 and 13 July 2007.
17. In addition, it transpires that from 5 to 13 July 2007 the employer recorded the applicant’s Yahoo Messenger communications in real time.
18. On 13 July 2007 at 4.30 p.m. the applicant was summoned by his employer to give an explanation. In the relevant notice he was informed that his Yahoo Messenger communications had been monitored and that there was evidence that he had used the internet for personal purposes, in breach of the internal regulations. Charts were attached indicating that his internet activity was greater than that of his colleagues. At that stage, he was not informed whether the monitoring of his communications had also concerned their content. The notice was worded as follows:

“Please explain why you are using company resources (Internet connection, Messenger) for personal purposes during working hours, as shown by the attached charts.”
19. On the same day, the applicant informed the employer in writing that he had used Yahoo Messenger for work-related purposes only.
20. At 5.20 p.m. the employer again summoned him to give an explanation in a notice worded as follows:

“Please explain why the entire correspondence you exchanged between 5 to 12 July 2007 using the S. Bucharest [internet] site ID had a private purpose, as shown by the attached forty-five pages.”
21. The forty-five pages mentioned in the notice consisted of a transcript of the messages which the applicant had exchanged with his brother and his fiancée during the period when he had been monitored; the messages related to personal matters and some were of an intimate nature. The transcript also included five messages that the applicant had exchanged with his fiancée using his personal Yahoo Messenger account; these messages did not contain any intimate information.
22. Also on 13 July, the applicant informed the employer in writing that in his view it had committed a criminal offence, namely breaching the secrecy of correspondence.
23. On 1 August 2007 the employer terminated the applicant's contract of employment.
24. The applicant challenged his dismissal in an application to the Bucharest County Court (“the County Court”).
[...]
28. In a judgment of 7 December 2007 the County Court rejected the applicant’s application and confirmed that his dismissal had been lawful.
[...]
29. The applicant appealed to the Bucharest Court of Appeal (“the Court of Appeal”).
[...]
30. The Court of Appeal dismissed the applicant’s appeal in a judgment of 17 June 2008.
[...]
31. In the meantime, on 18 September 2007 the applicant had lodged a criminal complaint against the statutory representatives of S., alleging a breach of the secrecy of correspondence. On 9 May 2012 the Directorate for Investigating Organised Crime and Terrorism (DIICOT) of the prosecutor’s office attached to the Supreme Court of Cassation and Justice ruled that there was no case to answer, on the grounds that the company was the owner of the computer system and the Internet connection and could therefore monitor its employees’ Internet activity and use the information stored on the server, and in view of the prohibition on personal use of the IT systems, as a result of which the monitoring had been foreseeable. [...]

The law
I. Alleged violation of article 8 of the Convention
55. The applicant submitted that his dismissal by his employer had been based on a breach of his right to respect for his private life and correspondence and that, by not revoking that measure, the domestic courts had failed to comply with their obligation to protect the right in question. He relied on Article 8 of the Convention, which provides:

“1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.”
C. Applicability of Article 8 of the Convention

2. The Court’s assessment

69. The Court notes that the question arising in the present case is whether the matters complained of by the applicant fall within the scope of Article 8 of the Convention.

70. At this stage of its examination it considers it useful to emphasise that “private life” is a broad term not susceptible to exhaustive definition (see Sidabras and Džiautas v. Lithuania, n.55480/00 and 59330/00, §43, […]). Article 8 of the Convention protects the right to personal development (see K.A. and A.D. v. Belgium, n.42758/98 and 45558/99, §83, 17 February 2005), whether in terms of personality (see Christine Goodwin v. the United Kingdom [GC], n.28957/95, §90, […] or of personal autonomy, which is an important principle underlying the interpretation of the Article 8 guarantees (see Pretty v. the United Kingdom, n.2346/02, §61[...]). The Court acknowledges that everyone has the right to live privately, away from unwanted attention (see Smirnova v. Russia, n.46133/99 and 48183/99, §95, […]). It also considers that it would be too restrictive to limit the notion of “private life” to an “inner circle” in which the individual may live his or her own personal life as he or she chooses, thus excluding entirely the outside world not encompassed within that circle (see Niemietz v. Germany, 16 December 1992, §29, […]). Article 8 thus guarantees a right to “private life” in the broad sense, including the right to lead a “private social life”, that is, the possibility for the individual to develop his or her social identity. In that respect, the right in question enshrines the possibility of approaching others in order to establish and develop relationships with them (see Bigaeva v. Greece, n.26713/05, §22, 28 May 2009, and Özpinar v. Turkey, n.20999/04, §45 […], 19 October 2010).

71. The Court considers that the notion of “private life” may include professional activities (see Fernández Martinez v. Spain [GC], n.56030/07, §110, […] and Oleksandr Volkov v. Ukraine, n.21722/11, §§165-66 […])), or activities taking place in a public context (see Von Hannover v. Germany (n.2) [GC], n.40660/08 and 60641/08, §95 […]). Restrictions on an individual’s professional life may fall within Article 8 where they have repercussions on the manner in which he or she constructs his or her social identity by developing relationships with others. It should be noted in this connection that it is in the course of their working lives that the majority of people have a significant, if not the greatest, opportunity to develop relationships with the outside world (see Niemietz, cited above, §29).

72. Furthermore, as regards the notion of “correspondence”, it should be noted that in the wording of Article 8 this word is not qualified by any adjective, unlike the term “life”. And indeed, the Court has already held that, in the context of correspondence by means of telephone calls, no such qualification is to be made. In a number of cases relating to correspondence with a lawyer, it has not even envisaged the possibility that Article 8 might be inapplicable on the ground that the correspondence was of a professional nature (see Niemietz, cited above, §32, with further references). Furthermore, it has held that telephone conversations are covered by the notions of “private life” and “correspondence” within the meaning of Article 8 (see Roman Zakharov v. Russia [GC], n.47143/06, §173, [...]). In principle, this is also true where telephone calls are made from or received on business premises (see Halford, cited above, § 44, and Amann v. Switzerland [GC], n.27798/95, §44 [...]). The same applies to emails sent from the workplace, which enjoy similar protection under Article 8, as does information derived from the monitoring of a person’s internet use (see Copland, cited above, §41 [...]).

73. It is clear from the Court’s case-law that communications from business premises as well as from the home may be covered by the notions of “private life” and “correspondence” within the meaning of Article 8 of the Convention (see Halford, cited above, §44; and Copland, cited above, §41). In order to ascertain whether the notions of “private life” and “correspondence” are applicable, the Court has on several occasions examined whether individuals had a reasonable expectation that their privacy would be respected and protected (ibid.; and as regards “private life”, see also Köpke v. Germany (dec.) , n.420/07, 5 October 2010). In that context, it has stated that a reasonable expectation of privacy is a significant though not necessarily conclusive factor (see Köpke, cited above).

74. Applying these principles in the present case, the Court first observes that the kind of internet instant messaging service at issue is just one of the forms of communication enabling individuals to lead a private social life. At the same time, the sending and receiving of
communications is covered by the notion of “correspondence”, even if they are sent from an employer’s computer. The Court notes, however, that the applicant’s employer instructed him and the other employees to refrain from any personal activities in the workplace. This requirement on the employer’s part was reflected in measures including a ban on using company resources for personal purposes […] 75. The Court further notes that with a view to ensuring that this requirement was met, the employer set up a system for monitoring its employees’ internet use (see paragraphs 17 and 18 above). The documents in the case file, in particular those relating to the disciplinary proceedings against the applicant, indicate that during the monitoring process, both the flow and the content of the applicants’ communications were recorded and stored (see paragraphs 18 and 20 above).

76. The Court observes in addition that despite this requirement on the employer’s part, the applicant exchanged messages of a personal nature with his fiancée and his brother […] Some of these messages were of an intimate nature […].

77. The Court considers that it is clear from the case file that the applicant had indeed been informed of the ban on personal internet use laid down in his employer’s internal regulations […]. However, it is not so clear that he had been informed prior to the monitoring of his communications that such a monitoring operation was to take place. Thus, the Government submitted that the applicant had acquainted himself with the employer’s information notice on an unspecified date between 3 and 13 July 2007 […]. Nevertheless, the domestic courts omitted to ascertain whether the applicant had been informed of the monitoring operation before the date on which it began, given that the employer recorded communications in real time from 5 to 13 July 2007 […].

78. In any event, it does not appear that the applicant was informed in advance of the extent and nature of his employer’s monitoring activities, or of the possibility that the employer might have access to the actual contents of his communications.

79. The Court also takes note of the applicant’s argument that he himself had created the Yahoo Messenger account in question and was the only person who knew the password […]. In addition, it observes that the material in the case file indicates that the employer also accessed the applicant’s personal Yahoo Messenger account […]. Be that as it may, the applicant had created the Yahoo Messenger account in issue on his employer’s instructions to answer customers’ enquiries […], and the employer had access to it.

80. It is open to question whether – and if so, to what extent – the employer’s restrictive regulations left the applicant with a reasonable expectation of privacy. Be that as it may, an employer’s instructions cannot reduce private social life in the workplace to zero. Respect for private life and for the privacy of correspondence continues to exist, even if these may be restricted in so far as necessary.

81. In the light of all the above considerations, the Court concludes that the applicant’s communications in the workplace were covered by the concepts of “private life” and “correspondence”. Accordingly, in the circumstances of the present case, Article 8 of the Convention is applicable.

D. Compliance with Article 8 of the Convention

2. The Court’s assessment
(a) Whether the case concerns a negative or a positive obligation

111. In the light of the particular circumstances of the case as described in paragraph 109 above, the Court considers, having regard to its conclusion concerning the applicability of Article 8 of the Convention […] and to the fact that the applicant’s enjoyment of his right to respect for his private life and correspondence was impaired by the actions of a private employer, that the complaint should be examined from the standpoint of the State’s positive obligations.

112. While the boundaries between the State’s positive and negative obligations under the Convention do not lend themselves to precise definition, the applicable principles are nonetheless similar. In both contexts regard must be had in particular to the fair balance that has to be struck between the competing interests of the individual and of the community as a whole, subject in any event to the margin of appreciation enjoyed by the State […].

(b) General principles applicable to the assessment of the State’s positive obligation to ensure respect for private life and correspondence in an employment context
113. The Court reiterates that the choice of the means calculated to secure compliance with Article 8 of the Convention in the sphere of the relations of individuals between themselves is in principle a matter that falls within the Contracting States’ margin of appreciation. There are different ways of ensuring respect for private life, and the nature of the State’s obligation will depend on the particular aspect of private life that is at issue […].

114. The Court’s task in the present case is therefore to clarify the nature and scope of the positive obligations that the respondent State was required to comply with in protecting the applicant’s right to respect for his private life and correspondence in the context of his employment.

121. The Court is aware of the rapid developments in this area. Nevertheless, it considers that proportionality and procedural guarantees against arbitrariness are essential. In this context, the domestic authorities should treat the following factors as relevant:

(i) whether the employee has been notified of the possibility that the employer might take measures to monitor correspondence and other communications, and of the implementation of such measures. While in practice employees may be notified in various ways depending on the particular factual circumstances of each case, the Court considers that for the measures to be deemed compatible with the requirements of Article 8 of the Convention, the notification should normally be clear about the nature of the monitoring and be given in advance;

(ii) the extent of the monitoring by the employer and the degree of intrusion into the employee’s privacy. In this regard, a distinction should be made between monitoring of the flow of communications and of their content. Whether all communications or only part of them have been monitored should also be taken into account, as should the question whether the monitoring was limited in time and the number of people who had access to the results (see Köpke, cited above). The same applies to the spatial limits to the monitoring;

(iii) whether the employer has provided legitimate reasons to justify monitoring the communications and accessing their actual content […]. Since monitoring of the content of communications is by nature a distinctly more invasive method, it requires weightier justification;

(iv) whether it would have been possible to establish a monitoring system based on less intrusive methods and measures than directly accessing the content of the employee’s communications. In this connection, there should be an assessment in the light of the particular circumstances of each case of whether the aim pursued by the employer could have been achieved without directly accessing the full contents of the employee’s communications;

(v) the consequences of the monitoring for the employee subjected to it (see, mutatis mutandis, the similar criterion applied in the assessment of the proportionality of an interference with the exercise of freedom of expression as protected by Article 10 of the Convention in Axel Springer AG v. Germany [GC], no. 39954/08, § 95, 7 February 2012, with further references); and the use made by the employer of the results of the monitoring operation, in particular whether the results were used to achieve the declared aim of the measure (see Köpke, cited above);

(vi) whether the employee had been provided with adequate safeguards, especially when the employer’s monitoring operations were of an intrusive nature. Such safeguards should in particular ensure that the employer cannot access the actual content of the communications concerned unless the employee has been notified in advance of that eventuality.

In this context, it is worth reiterating that in order to be fruitful, labour relations must be based on mutual trust.

(c) Application of the above general principles in the present case

124. The Court observes that the domestic courts held that the interests at stake in the present case were, on the one hand, the applicant’s right to respect for his private life, and on the other hand, the employer’s right to engage in monitoring, including the corresponding disciplinary powers, in order to ensure the smooth running of the company […]. It considers that, by virtue of the State’s positive obligations under Article 8 of the Convention, the national authorities were required to carry out a balancing exercise between these competing interests.

130. The evidence produced before the Court indicates that the applicant had been informed of his employer’s internal regulations, which prohibited the personal use of company resources […]. He had acknowledged the contents of the document in question and had signed a copy of it on 20 December 2006 […]. In addition, the employer had sent all employees an information notice
dated 26 June 2007 reminding them that personal use of company resources was prohibited and explaining that an employee had been dismissed for breaching this rule [...]. The applicant acquainted himself with the notice and signed a copy of it on an unspecified date between 3 and 13 July 2007 [...]. The Court notes lastly that on 13 July 2007 the applicant was twice summoned by his employer to provide explanations as to his personal use of the internet [...]. Initially, after being shown the charts indicating his internet activity and that of his colleagues, he argued that his use of his Yahoo Messenger account had been purely work-related [...]. Subsequently, on being presented fifty minutes later with a forty-five-page transcript of his communications with his brother and fiancée, he informed his employer that in his view it had committed the criminal offence of breaching the secrecy of correspondence [...].

131. The Court notes that the domestic courts correctly identified the interests at stake – by referring explicitly to the applicant’s right to respect for his private life – and also the applicable legal principles […]. In particular, the Court of Appeal made express reference to the principles of necessity, purpose specification, transparency, legitimacy, proportionality and security set forth in Directive 95/46/EC, and pointed out that the monitoring of internet use and of electronic communications in the workplace was governed by those principles […]. The domestic courts also examined whether the disciplinary proceedings had been conducted in an adversarial manner and whether the applicant had been given the opportunity to put forward his arguments.

132. It remains to be determined how the national authorities took the criteria set out above […] into account in their reasoning when weighing the applicant’s right to respect for his private life and correspondence against the employer’s right to engage in monitoring, including the corresponding disciplinary powers, in order to ensure the smooth running of the company.

133. As to whether the applicant had received prior notification from his employer, the Court observes that it has already concluded that he did not appear to have been informed in advance of the extent and nature of his employer’s monitoring activities, or of the possibility that the employer might have access to the actual content of his messages […]. With regard to the possibility of monitoring, it notes that the County Court simply observed that “the employees’ attention had been drawn to the fact that, shortly before the applicant’s disciplinary sanction, another employee had been dismissed” […] and that the Court of Appeal found that the applicant had been warned that he should not use company resources for personal purposes […]. Accordingly, the domestic courts omitted to determine whether the applicant had been notified in advance of the possibility that the employer might introduce monitoring measures, and of the scope and nature of such measures. The Court considers that to qualify as prior notice, the warning from the employer must be given before the monitoring activities are initiated, especially where they also entail accessing the contents of employees’ communications. International and European standards point in this direction, requiring the data subject to be informed before any monitoring activities are carried out […].

134. As regards the scope of the monitoring and the degree of intrusion into the applicant’s privacy, the Court observes that this question was not examined by either the County Court or the Court of Appeal […], even though it appears that the employer recorded all the applicant’s communications during the monitoring period in real time, accessed them and printed out their contents […].

135. Nor does it appear that the domestic courts carried out a sufficient assessment of whether there were legitimate reasons to justify monitoring the applicant’s communications. The Court is compelled to observe that the Court of Appeal did not identify what specific aim in the present case could have justified such strict monitoring. Admittedly, this question had been touched upon by the County Court, which had mentioned the need to avoid the company’s IT systems being damaged, liability being incurred by the company in the event of illegal activities in cyberspace, and the company’s trade secrets being disclosed […]. However, in the Court’s view, these examples can only be seen as theoretical, since there was no suggestion that the applicant had actually exposed the company to any of those risks. Furthermore, the Court of Appeal did not address this question at all.

136. In addition, neither the County Court nor the Court of Appeal sufficiently examined whether the aim pursued by the employer could have been achieved by less intrusive methods than accessing the actual contents of the applicant’s communications.
137. Moreover, neither court considered the seriousness of the consequences of the monitoring and the subsequent disciplinary proceedings. In this respect the Court notes that the applicant had received the most severe disciplinary sanction, namely dismissal.

138. Lastly, the Court observes that the domestic courts did not determine whether, when the employer summoned the applicant to give an explanation for his use of company resources, in particular the internet […], it had in fact already accessed the contents of the communications in issue. It notes that the national authorities did not establish at what point during the disciplinary proceedings the employer had accessed the relevant content. In the Court’s view, accepting that the content of communications may be accessed at any stage of the disciplinary proceedings runs counter to the principle of transparency […].

139. Having regard to the foregoing, the Court finds that the Court of Appeal’s conclusion that a fair balance was struck between the interests at stake […] is questionable. Such an assertion appears somewhat formal and theoretical. The Court of Appeal did not explain the specific reasons linked to the particular circumstances of the applicant and his employer that led it to reach that finding.

140. That being so, it appears that the domestic courts failed to determine, in particular, whether the applicant had received prior notice from his employer of the possibility that his communications on Yahoo Messenger might be monitored; nor did they have regard either to the fact that he had not been informed of the nature or the extent of the monitoring, or to the degree of intrusion into his private life and correspondence. In addition, they failed to determine, firstly, the specific reasons justifying the introduction of the monitoring measures; secondly, whether the employer could have used measures entailing less intrusion into the applicant’s private life and correspondence; and thirdly, whether the communications might have been accessed without his knowledge […].

141. Having regard to all the above considerations, and notwithstanding the respondent State’s margin of appreciation, the Court considers that the domestic authorities did not afford adequate protection of the applicant’s right to respect for his private life and correspondence and that they consequently failed to strike a fair balance between the interests at stake. There has therefore been a violation of Article 8 of the Convention.

II. Application of Article 41 of the Convention

A. Damage

1. Pecuniary damage

[…]

145. The Court observes that it has found a violation of Article 8 of the Convention in that the national courts failed to establish the relevant facts and to perform an adequate balancing exercise between the applicant’s right to respect for his private life and correspondence and the employer’s interests. It does not discern any causal link between the violation found and the pecuniary damage alleged, and therefore dismisses this claim.

2. Non-pecuniary damage

146. Before the Chamber, the applicant also claimed € 200,000 in respect of the non-pecuniary damage he had allegedly sustained as a result of his dismissal. He stated that because of the disciplinary nature of the dismissal, he had been unable to find another job, that his standard of living had consequently deteriorated, that he had lost his social standing and that as a result, his fiancée had decided in 2010 to end their relationship.

[…]

148. The Court considers that the finding of a violation constitutes sufficient just satisfaction for any non-pecuniary damage that may have been sustained by the applicant.

B. Costs and expenses

149. Before the Chamber, the applicant also claimed 3,310 Romanian lei (RON) (approximately € 750) in respect of the costs and expenses incurred in the domestic courts, and RON 500 (approximately € 115) for the fees of the lawyer who had represented him in the domestic proceedings. He claimed a further € 500 for the fees of the lawyers who had represented him before the Court.

[…]
151. According to the Court’s case-law, an applicant is entitled to the reimbursement of costs and expenses only in so far as it has been shown that these have been actually and necessarily incurred and are reasonable as to quantum [...]. In the present case, having regard to the documents in its possession and to its case-law, the Court considers it reasonable to award the applicant the sum of € 1,365 covering costs under all heads.

[...]

For these reasons, the Court
1. Holds, by eleven votes to six, that there has been a violation of Article 8 of the Convention;
2. Holds, by sixteen votes to one, that the finding of a violation constitutes in itself sufficient just satisfaction for the non-pecuniary damage sustained by the applicant;
3. Holds, by fourteen votes to three,
(a) that the respondent State is to pay the applicant, within three months, € 1,365 (one thousand three hundred and sixty-five euros) in respect of costs and expenses, to be converted into the currency of the respondent State at the rate applicable at the date of settlement, plus any tax that may be chargeable to the applicant;
[...]
4. Dismisses, unanimously, the remainder of the applicant’s claim for just satisfaction.
[...]

*****

DISCUSSIONE

1. Quale strumento di comunicazione era usato nel luogo di lavoro? Era un mezzo personale o aziendale?
2. Il lavoratore era stato avvisato del divieto di utilizzo degli strumenti aziendali di comunicazione per motivi personali?
3. Cosa contesta inoltre il lavoratore, come violazione ingiustificata della propria privacy?
4. Il comportamento del datore di lavoro è stato ritenuto ragionevole e proporzionato? Su quali basi?

*****

NORME

- art.8, CEDU
12.3. Uso di posta elettronica ed Internet sul luogo di lavoro

Garante per la protezione dei dati personali, delib. n.13 del 1 marzo 2007

**Lavoro: le linee guida del Garante per posta elettronica e Internet**

[...]

1. Utilizzo della posta elettronica e della rete Internet nel rapporto di lavoro

1.1. Premessa

Dall'esame di diversi reclami, segnalazioni e quesiti è emersa l'esigenza di prescrivere ai datori di lavoro alcune misure, necessarie o opportune, per conformare alle disposizioni vigenti il trattamento di dati personali effettuato per verificare il corretto utilizzo nel rapporto di lavoro della posta elettronica e della rete Internet.

Occorre muovere da alcune premesse:

a) compete ai datori di lavoro assicurare la funzionalità e il corretto impiego di tali mezzi da parte dei lavoratori, definendone le modalità d'uso nell'organizzazione dell'attività lavorativa, tenendo conto della disciplina in tema di diritti e relazioni sindacali;

b) spetta ad essi adottare idonee misure di sicurezza per assicurare la disponibilità e l'integrità di sistemi informativi e di dati, anche per prevenire utilizzi indebiti che possono essere fonte di responsabilità (artt.15, 31 ss., 167 e 169 del Codice);

c) emerge l'esigenza di tutelare i lavoratori interessati anche perché l'utilizzazione dei predetti mezzi, già ampiamente diffusi nel contesto lavorativo, è destinata ad un rapido incremento in numerose attività svolte anche fuori della sede lavorativa;

d) l'utilizzo di Internet da parte dei lavoratori può infatti formare oggetto di analisi, profilazione e integrale ricostruzione mediante elaborazione di log file della navigazione web ottenuti, ad esempio, da un proxy server o da un altro strumento di registrazione delle informazioni. I servizi di posta elettronica sono parimenti suscettibili (anche attraverso la tenuta di log file di traffico e-mail e l'archiviazione di messaggi) di controlli che possono giungere fino alla conoscenza da parte del datore di lavoro (titolare del trattamento) del contenuto della corrispondenza;

e) le informazioni così trattate contengono dati personali anche sensibili riguardanti lavoratori o terzi, identificati o identificabili.

1.2. Tutela del lavoratore.

Le informazioni di carattere personale trattate possono riguardare, oltre all'attività lavorativa, la sfera personale e la vita privata di lavoratori e di terzi. La linea di confine tra questi ambiti, come affermato dalla Corte europea dei diritti dell'uomo, può essere tracciata a volte solo con difficoltà.

Il luogo di lavoro è una formazione sociale nella quale va assicurata la tutela dei diritti, delle libertà fondamentali e della dignità degli interessati garantendo che, in una cornice di reciproci diritti e doveri, sia assicurata l'esplicazione della personalità del lavoratore e una ragionevole protezione della sua sfera di riservatezza nelle relazioni personali e professionali (artt.2 e 41, comma 2, Cost.; art.2087 c.c.; cfr. altresì l’art.2, comma 5, Codice dell'amministrazione digitale, d.lgs. 7 marzo 2005, n.82, riguardo al diritto ad ottenere che il trattamento dei dati effettuato mediante l'uso di tecnologie telematiche sia conformato al rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato).

Non a caso, nell'organizzare l'attività lavorativa e gli strumenti utilizzati, diversi datori di lavoro hanno prefigurato modalità d'uso che, tenendo conto del crescente lavoro in rete e di nuove tariffe di traffico forfettarie, assegnano aree di lavoro riservate per appunti strettamente personali, ovvero consentono usi moderati di strumenti per finalità private.

2. Codice in materia di protezione dei dati e discipline di settore

2.1. Principi generali.

Nell'impartire le seguenti prescrizioni il Garante tiene conto del diritto alla protezione dei dati personali, della necessità che il trattamento sia disciplinato assicurando un elevato livello di tutela delle persone, nonché dei principi di semplificazione, armonizzazione ed efficacia (artt.1 e 2 del Codice). Le prescrizioni potranno essere aggiornate alla luce dell'esperienza e dell'innovazione tecnologica.

2.2. Discipline di settore.
Alcune disposizioni di settore, fatte salve dal Codice, prevedono specifici divieti o limiti, come quelli posti dallo Statuto dei lavoratori sul controllo a distanza (artt.113, 114 e 184, comma 3, del Codice; artt.4 e 8 l. 20 maggio 1970, n.300).

La disciplina di protezione dei dati va coordinata con regole di settore riguardanti il rapporto di lavoro e il connesso utilizzo di tecnologie, nelle quali è fatta salva o richiamata espressamente (art.47, comma 3, lett.b) Codice dell'amministrazione digitale).

2.3. Principi del Codice.

I trattamenti devono rispettare le garanzie in materia di protezione dei dati e svolgersi nell'osservanza di alcuni cogenti principi:

a) il principio di necessità, secondo cui i sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi in relazione alle finalità perseguite (art.3 del Codice; §5.2);

b) il principio di correttezza, secondo cui le caratteristiche essenziali dei trattamenti devono essere rese note ai lavoratori (art.11, comma 1, lett.a, del Codice). Le tecnologie dell'informazione (in modo più marcato rispetto ad apparecchiature tradizionali) permettono di svolgere trattamenti ulteriori rispetto a quelli connessi ordinariamente all'attività lavorativa. Ciò, all'insaputa o senza la piena consapevolezza dei lavoratori, considerate anche le potenziali applicazioni di regola non adeguatamente conosciute dagli interessati (v. §3);

c) i trattamenti devono essere effettuati per finalità determinate, esplicite e legittime (art.11, comma 1, lett.b), del Codice; §§4 e 5), osservando il principio di pertinenza e non eccedenza (§6). Il datore di lavoro deve trattare i dati "nella misura meno invasiva possibile"; le attività di monitoraggio devono essere svolte solo da soggetti preposti (§§8) ed essere "mirate sull'area di rischio, tenendo conto della normativa sulla protezione dei dati e, se pertinente, del principio di segretezza della corrispondenza" (Parere n.8/2001, cit., p.ti 5 e 12).

3. Controlli e correttezza nel trattamento

3.1. Disciplina interna

In base al richiamato principio di correttezza, l'eventuale trattamento deve essere ispirato ad un canone di trasparenza, come prevede anche la disciplina di settore (art.4, comma 2, Statuto dei lavoratori; allegato VII, §3, d.lgs. 626/1994 e successive integrazioni e modificazioni in materia di "uso di attrezzature munite di videoterminali", il quale esclude la possibilità del controllo informatico "all'insaputa dei lavoratori").

Grava quindi sul datore di lavoro l'onere di indicare in ogni caso, chiaramente e in modo particolareggiato, quali siano le modalità di utilizzo degli strumenti messi a disposizione ritenute corrette e se, in che misura e con quali modalità vengano effettuati controlli. Ciò, tenendo conto della pertinente disciplina applicabile in tema di informazione, concertazione e consultazione delle organizzazioni sindacali.

Per la predetta indicazione il datore ha a disposizione vari mezzi, a seconda del genere e della complessità delle attività svolte, e informando il personale con modalità diverse anche a seconda delle dimensioni della struttura, tenendo conto, ad esempio, di piccole realtà dove vi è una continua condivisione interpersonale di risorse informative.

3.2. Linee guida

In questo quadro, può risultare opportuno adottare un disciplinare interno redatto in modo chiaro e senza formule generiche, da pubblicizzare adeguatamente (verso i singoli lavoratori, nella rete interna, mediante affissioni sui luoghi di lavoro con modalità analoghe a quelle previste dall'art.7 dello Statuto dei lavoratori, ecc.) e da sottoporre ad aggiornamento periodico.

A seconda dei casi andrebbe ad esempio specificato:

- se determinati comportamenti non sono tollerati rispetto alla "navigazione" in Internet (ad es., il download di software o di file musicali), oppure alla tenuta di file nella rete interna;

- in quale misura è consentito utilizzare anche per ragioni personali servizi di posta elettronica o di rete, anche solo da determinate postazioni di lavoro o caselle oppure ricorrendo a sistemi di webmail, indicandone le modalità e l'arco temporale di utilizzo (ad es., fuori dall'orario di lavoro o durante le pause, o consentendone un uso moderato anche nel tempo di lavoro);

- quali informazioni sono memorizzate temporaneamente (ad es., le componenti di file di log eventualmente registrati) e chi (anche all'esterno) vi può accedere legittimamente;

- se e quali informazioni sono eventualmente conservate per un periodo più lungo, in forma centralizzata o meno (anche per effetto di copie di back up, della gestione tecnica della rete o di file di log);
- se, e in quale misura, il datore di lavoro si riserva di effettuare controlli in conformità alla legge, anche saltuari o occasionali, indicando le ragioni legittime – specifiche e non generiche – per cui verrebbero effettuati (anche per verifiche sulla funzionalità e sicurezza del sistema) e le relative modalità (precisando se, in caso di abusi singoli o reiterati, vengono inoltrati preventivi avvisi collettivi o individuali ed effettuati controlli nominativi o su singoli dispositivi e postazioni);
- quali conseguenze, anche di tipo disciplinare, il datore di lavoro si riserva di trarre qualora constati che la posta elettronica e la rete Internet sono utilizzate indebitamente;
- le soluzioni prefigurate per garantire, con la cooperazione del lavoratore, la continuità dell'attività lavorativa in caso di assenza del lavoratore stesso (specie se programmata), con particolare riferimento all'attivazione di sistemi di risposta automatica ai messaggi di posta elettronica ricevuti;
- se sono utilizzabili modalità di uso personale di mezzi con pagamento o fatturazione a carico dell'interessato;
- quali misure sono adottate per particolari realtà lavorative nelle quali debba essere rispettato l'eventuale segreto professionale cui siano tenute specifiche figure professionali;
- le prescrizioni interne sulla sicurezza dei dati e dei sistemi (art.34 del Codice, nonché Allegato B), in particolare regole 4, 9, 10).

3.3. Informativa (art.13 del Codice)
All'onere del datore di lavoro di prefigurare e pubblicizzare una policy interna rispetto al corretto uso dei mezzi e agli eventuali controlli, si affianca il dovere di informare comunque gli interessati ai sensi dell'art.13 del Codice, anche unitamente agli elementi indicati ai p.ti 3.1. e 3.2..
Rispetto a eventuali controlli gli interessati hanno infatti il diritto di essere informati preventivamente, e in modo chiaro, sui trattamenti di dati che possono riguardarli.
Le finalità da indicare possono essere connesse a specifiche esigenze organizzative, produttive e di sicurezza del lavoro, quando comportano un trattamento lecito di dati (art.4, comma 1, legge 300/1970); possono anche riguardare l'esercizio di un diritto in sede giudiziaria.
Devono essere tra l'altre indicate le principali caratteristiche dei trattamenti, nonché il soggetto o l'unità organizzativa ai quali i lavoratori possono rivolgersi per esercitare i propri diritti.

4. Apparecchiature preordinate al controllo a distanza
Con riguardo al principio secondo cui occorre perseguire finalità determinate, esplicite e legittime (art.11, comma 1, lett.b), del Codice), il datore di lavoro può riservarsi di controllare (direttamente o attraverso la propria struttura) l'effettivo adempimento della prestazione lavorativa e, se necessario, il corretto utilizzo degli strumenti di lavoro (cfr. artt.2086, 2087 e 2104 c.c.).
Nell'esercizio di tale prerogativa occorre rispettare la libertà e la dignità dei lavoratori, in particolare per ciò che attiene al divieto di installare "apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori" (art.4, comma 1, legge 300/1970), tra cui sono certamente comprese le strumentazioni hardware e software mirate al controllo dell'utente di un sistema di comunicazione elettronica.
Il trattamento dei dati che ne consegue è illecito, a prescindere dall'illiceità dell'installazione stessa. Ciò, anche quando i singoli lavoratori ne siano consapevoli.
In particolare non può ritenersi consentito il trattamento effettuato mediante sistemi hardware e software preordinati al controllo a distanza, grazie ai quali sia possibile ricostruire – a volte anche minuziosamente – l'attività di lavoratori. È il caso, ad esempio:
- della lettura e della registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio e-mail;
- della riproduzione ed eventuale memorizzazione sistematica delle pagine web visualizzate dal lavoratore;
- della lettura e della registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo;
- dell'analisi occulta di computer portatili affidati in uso.
Il controllo a distanza vietato dalla legge riguarda l'attività lavorativa in senso stretto e altre condotte personali poste in essere nel luogo di lavoro. A parte eventuali responsabilità civili e penali, i dati trattati illecitamente non sono utilizzabili (art.11, comma 2, del Codice).

5. Programmi che consentono controlli "indiretti"
5.1. Il datore di lavoro, utilizzando sistemi informativi per esigenze produttive o organizzative (ad es., per rilevare anomalie o per manutenzioni) o, comunque, quando gli stessi si rivelano necessari per la sicurezza sul lavoro, può avvalersi legittimamente, nel rispetto dello Statuto dei
lavoratori (art.4, comma 2), di sistemi che consentono indirettamente un controllo a distanza (cd. controllo preterintenzionale) e determinano un trattamento di dati personali riferiti o riferibili ai lavoratori. Ciò, anche in presenza di attività di controllo discontinue.

Il trattamento di dati che ne consegue può risultare lecito. Resta ferma la necessità di rispettare le procedure di informazione e di consultazione di lavoratori e sindacati in relazione all’introduzione o alla modifica di sistemi automatizzati per la raccolta e l’utilizzazione dei dati, nonché in caso di introduzione o di modifica di procedimenti tecnici destinati a controllare i movimenti o la produttività dei lavoratori.

5.2. Principio di necessità

In applicazione del menzionato principio di necessità il datore di lavoro è chiamato a promuovere ogni opportuna misura, organizzativa e tecnologica volta a prevenire il rischio di utilizzo impropri (da preferire rispetto all’adozione di misure “repressive”) e, comunque, a “minimizzare” l’uso di dati riferibili ai lavoratori (artt.3, 11, comma 1, lett.d) e 22, commi 3 e 5, del Codice; aut. gen. al trattamento dei dati sensibili n.1/2005, p.to 4).

Dal punto di vista organizzativo è quindi opportuno che:
- si valuti attentamente l’impatto sui diritti dei lavoratori (prima dell’installazione di apparecchiature suscettibili di consentire il controllo a distanza e dell’eventuale trattamento);
- si individui preventivamente (anche per tipologie) a quali lavoratori è accordato l’utilizzo della posta elettronica e l’accesso a Internet;
- si determini quale ubicazione è riservata alle postazioni di lavoro per ridurre il rischio di un loro impiego abusivo.

Il datore di lavoro ha inoltre l’onere di adottare tutte le misure tecnologiche volte a minimizzare l’uso di dati identificativi (cd. privacy enhancing technologies – PETs). Le misure possono essere differenziate a seconda della tecnologia impiegata (ad es., posta elettronica o navigazione in Internet). 

a) Internet: la navigazione web

Il datore di lavoro, per ridurre il rischio di usi impropri della "navigazione" in Internet (consistenti in attività non correlate alla prestazione lavorativa quali la visione di siti non pertinenti, l’upload o il download di file, l’uso di servizi di rete con finalità ludiche o estranee all’attività), deve adottare opportune misure che possono, così, prevenire controlli successivi sul lavoratore. Tali controlli, leciti o meno a seconda dei casi, possono determinare il trattamento di informazioni personali, anche non pertinenti o idonei a rivelare convinzioni religiose, filosofiche o di altro genere, opinioni politiche, lo stato di salute o la vita sessuale (art.8 legge 300/1970; artt.26 e 113 del Codice; Prov. 2 febbraio 2006, cit.).

In particolare, il datore di lavoro può adottare una o più delle seguenti misure opportune, tenendo conto delle peculiarità proprie di ciascuna organizzazione produttiva e dei diversi profili professionali:
- individuazione di categorie di siti considerati correlati o meno con la prestazione lavorativa;
- configurazione di sistemi o utilizzo di filtri che prevengano determinate operazioni – reputate inconvenienti con l’attività lavorativa – quali l’upload o l’accesso a determinati siti (inseriti in una sorta di black-list) e/o il download di file o software aventi particolari caratteristiche (dimensionali o di tipologia di dato);
- trattamento di dati in forma anonima o tale da precludere l’immediata identificazione di utenti mediante loro opportune aggregazioni (ad es., con riguardo ai file di log riferiti al traffico web, su base collettiva o per gruppi sufficientemente ampi di lavoratori);
- eventuale conservazione nel tempo dei dati strettamente limitata al perseguimento di finalità organizzative, produttive e di sicurezza.

b) Posta elettronica


Tuttavia, con specifico riferimento all’impiego della posta elettronica nel contesto lavorativo e in ragione della veste esteriore attribuita all’indirizzo di posta elettronica nei singoli casi, può risultare dubbio se il lavoratore, in qualità di destinatario o mittente, utilizzi la posta elettronica.
operando quale espressione dell’organizzazione datoriale o ne faccia un uso personale pur operando in una struttura lavorativa.

La mancata esplicitazione di una policy al riguardo può determinare anche una legittima aspettativa del lavoratore, o di terzi, di confidenzialità rispetto ad alcune forme di comunicazione.

Tali incertezze si riverberano sulla qualificazione, in termini di liceità, del comportamento del datore di lavoro che intenda apprendere il contenuto di messaggi inviati all’indirizzo di posta elettronica usato dal lavoratore (posta “in entrata”) o di quelli inviati da quest’ultimo (posta “in uscita”).

É quindi particolarmente opportuno che si adottino accorgimenti anche per prevenire eventuali trattamenti in violazione dei principi di pertinenza e non eccedenza. Si tratta di soluzioni che possono risultare utili per contemperare le esigenze di ordinato svolgimento dell’attività lavorativa con la prevenzione di inutili intrusioni nella sfera personale dei lavoratori, nonché violazioni della disciplina sull’eventuale segretezza della corrispondenza.

In questo quadro è opportuno che:

- il datore di lavoro renda disponibili indirizzi di posta elettronica condivisi tra più lavoratori (ad esempio, info@ente.it, ufficiovendite@ente.it, ufficioreclami@società.com, urp@ente.it, etc.), eventualmente affiancandoli a quelli individuali (ad esempio, m.rossi@ente.it, rossi@società.com, mario.rossi@società.it);

- il datore di lavoro valuti la possibilità di attribuire al lavoratore un diverso indirizzo destinato ad uso privato del lavoratore;

- il datore di lavoro metta a disposizione di ciascun lavoratore apposite funzionalità di sistema, di agevole utilizzo, che consentano di inviare automaticamente, in caso di assenze (ad es., per ferie o attività di lavoro fuori sede), messaggi di risposta contenenti le “coordinate” (anche elettroniche o telefoniche) di un altro soggetto o altre utili modalità di contatto della struttura. É parimenti opportuno prescrivere ai lavoratori di avvalersi di tali modalità, prevenendo così l’apertura della posta elettronica. In caso di eventuali assenze non programmate (ad es., per malattia), qualora il lavoratore non possa attivare la procedura descritta (anche avvalendosi di servizi webmail), il titolare del trattamento, perdurando l’assenza oltre un determinato limite temporale, potrebbe disporre lecitamente, sempre che sia necessario e mediante personale appositamente incaricato (ad es., l’amministratore di sistema oppure, se presente, un incaricato aziendale per la protezione dei dati), l’attivazione di un analogo accorgimento, avvertendo gli interessati;

- i messaggi di posta elettronica contengono un avvertimento ai destinatari nel quale sia dichiarata l’eventuale natura non personale dei messaggi stessi, precisando se le risposte potranno essere conosciute nell’organizzazione di appartenenza del mittente e con eventuali rinvio alla predetta policy datoriale.

6. Pertinenza e non eccedenza

6.1. Graduazione dei controlli

Nell’effettuare controlli sull’uso degli strumenti elettronici deve essere evitata un’interferenza ingiustificata sui diritti e sulle libertà fondamentali di lavoratori, come pure di soggetti esterni che ricevono o inviano comunicazioni elettroniche di natura personale o privata. L’eventuale controllo è lecito solo se sono rispettati i principi di pertinenza e non eccedenza.

Nel caso in cui un evento dannoso o una situazione di pericolo non sia stato impedito con preventivi accorgimenti tecnici, il datore di lavoro può adottare eventuali misure che consentano la verifica di comportamenti anomali.

Deve essere per quanto possibile preferito un controllo preliminare su dati aggregati, riferiti all’intera struttura lavorativa o a sue aree.

Il controllo anonimo può concludersi con un avviso generalizzato relativo ad un rilevato utilizzo anomalo degli strumenti aziendali e con l’invito ad attenersi scrupolosamente a compiti assegnati e istruzioni impartite. L’avviso può essere circoscritto a dipendenti afferenti all’area o
settore in cui è stata rilevata l'anomalia. In assenza di successive anomalie non è di regola giustificato effettuare controlli su base individuale.

Va esclusa l'ammissibilità di controlli prolungati, costanti o indiscriminati.

6.2. Conservazione

I sistemi *software* devono essere programmati e configurati in modo da cancellare periodicamente ed automaticamente (attraverso procedure di sovraregistrazione come, ad esempio, la cd. rotazione dei *log files*) i dati personali relativi agli accessi ad Internet e al traffico telematico, la cui conservazione non sia necessaria.

In assenza di particolari esigenze tecniche o di sicurezza, la conservazione temporanea dei dati relativi all’uso degli strumenti elettronici deve essere giustificata da una finalità specifica e comprovata e limitata al tempo necessario – e predeterminato – a raggiungerla (v. *art.11, comma 1, lett.e, del Codice*).

Un eventuale prolungamento dei tempi di conservazione va valutato come eccezionale e può aver luogo solo in relazione:
- ad esigenze tecniche o di sicurezza del tutto particolari;
- all’indispensabilità del dato rispetto all’esercizio o alla difesa di un diritto in sede giudiziaria;
- all’obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell’autorità giudiziaria o della polizia giudiziaria.

In questi casi, il trattamento dei dati personali (tenendo conto, con riguardo ai dati sensibili, delle prescrizioni contenute nelle autorizzazioni generali nn.1/2005 e 5/2005 adottate dal Garante) deve essere limitato alle sole informazioni indispensabili per perseguire finalità preventivamente determinate ed essere effettuato con logiche e forme di organizzazione strettamente correlate agli obblighi, compiti e finalità già esplicitati.

[*Tutto ciò premesso il Garante*]

1) prescrive ai datori di lavoro privati e pubblici, ai sensi dell’*art.154, comma 1, lett.c)*, del Codice, di adottare la misura necessaria a garanzia degli interessati, nei termini di cui in motivazione, riguardante l’onere di specificare le modalità di utilizzo della posta elettronica e della rete Internet da parte dei lavoratori (p.to 3.1.), indicando chiaramente le modalità di uso degli strumenti messi a disposizione e se, in che misura e con quali modalità vengano effettuati controlli;

2) indica inoltre, ai medesimi datori di lavoro, le seguenti linee guida a garanzia degli interessati, nei termini di cui in motivazione, per ciò che riguarda:

- l’adozione e la pubblicizzazione di un disciplinare interno (p.to 3.2.);
- si proceda ad un’attenta valutazione dell’impatto sui diritti dei lavoratori;
- si individui preventivamente (anche per tipologie) a quali lavoratori è accordato l’utilizzo della posta elettronica e dell’accesso a Internet;
- si individui quale ubicazione è riservata alle postazioni di lavoro per ridurre il rischio di impieghi abusivi;

   c) l’adozione di misure di tipo tecnologico, e segnatamente:

   I. rispetto alla “navigazione” in Internet (p.to 5.2., a):
   - l’individuazione di categorie di siti considerati correlati o non correlati con la prestazione lavorativa;
   - la configurazione di sistemi o l’utilizzo di filtri che prevengano determinate operazioni;
   - il trattamento di dati in forma anonima o tale da precludere l’immediata identificazione degli utenti mediante opportune aggregazioni;
   - l’eventuale conservazione di dati per il tempo strettamente limitato al perseguimento di finalità organizzative, produttive e di sicurezza;
   - la graduazione dei controlli (p.to 6.1.);

   II. rispetto all’utilizzo della posta elettronica (p.to 5.2., b):
   - la messa a disposizione di indirizzi di posta elettronica condivisi tra più lavoratori, eventualmente affiancandoli a quelli individuali;
   - l’eventuale attribuzione al lavoratore di un diverso indirizzo destinato ad uso privato;
   - la messa a disposizione di ciascun lavoratore, con modalità di agevole esecuzione, di apposite funzionalità di sistema che consentano di inviare automaticamente, in caso di assenze programmate, messaggi di risposta che contengano le “coordinate” di altro
soggetto o altre utili modalità di contatto dell'istituzione presso la quale opera il lavoratore assente;
- consentire che, qualora si debba conoscere il contenuto dei messaggi di posta elettronica in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, l'interessato sia messo in grado di delegare un altro lavoratore (fiduciario) a verificare il contenuto di messaggi e a inoltrare al titolare del trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. Di tale attività dovrebbe essere redatto apposito verbale e informato il lavoratore interessato alla prima occasione utile;
- l'inserzione nei messaggi di un avvertimento ai destinatari nel quale sia dichiarata l'eventuale natura non personale del messaggio e sia specificato se le risposte potranno essere conosciute nell'organizzazione di appartenenza del mittente;
- la graduazione dei controlli (p.to 6.1.);
  3) vieta ai datori di lavoro privati e pubblici, ai sensi dell'art.154, comma 1, lett.d), del Codice, di effettuare trattamenti di dati personali mediante sistemi hardware e software che mirano al controllo a distanza di lavoratori (p.to 4), svolti in particolare mediante:
   a) la lettura e la registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio e-mail;
   b) la riproduzione e l'eventuale memorizzazione sistematica delle pagine web visualizzate dal lavoratore;
   c) la lettura e la registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo;
   d) l'analisi occulta di computer portatili affidati in uso;
  4) individua, ai sensi dell'art.24, comma 1, lett.g), del Codice, nei termini di cui in motivazione (p.to 7), i casi nei quali il trattamento dei dati personali di natura non sensibile possono essere effettuati per perseguire un legittimo interesse del datore di lavoro anche senza il consenso degli interessati;

[...]

*****

DISCUSSIONE

1. **Quali sono gli interessi in potenziale conflitto che il provvedimento del Garante cerca di conciliare?**

2. **Quali sono i principi generali del d.lgs. n.196/2003 che devono essere comunque rispettati?**

3. **Quale è il contenuto suggerito per il “disciplinare interno” previsto dal provvedimento del Garante?**

4. **Quale è il rapporto tra d.lgs. n.196/2003 e Statuto dei lavoratori in merito ai controlli a distanza riguardanti l’uso di Internet?**

5. **Quali sono le misure, distinte per navigazione web e uso della posta elettronica, suggerite dal Garante? Quali sono a vostro avviso i lati positivi ed i lati negativi di tali misure?**

6. **Che caratteristiche devono avere i controlli sull’attività in Internet del lavoratore?**
12.4. Pubblici dipendenti e uso di posta elettronica ed Internet

Presidenza del Consiglio dei Ministri, direttiva n.2/2009 del 26 maggio 2009

Oggetto: Utilizzo di Internet e della casella di posta elettronica istituzionale sul luogo di lavoro.

Premessa
Le risorse ICT costituiscono, ormai da tempo, il principale strumento di lavoro posto a disposizione dei dipendenti delle pubbliche amministrazioni.

L'ampia distribuzione di tali risorse tra i dipendenti ne favorisce il diffuso utilizzo anche per finalità diverse da quelle lavorative. La prassi, ancorché ben conosciuta dalle amministrazioni, è difficile da monitorare, sia per il costo dell'eventuale attività di monitoraggio, sia per le implicazioni relative alla tutela della riservatezza e dei dati personali.

D'altronde, tale utilizzo non istituzionale non provoca, di norma, costi aggiuntivi, tenuto conto della modalità di pagamento "flat" (non riferita, pertanto, al consumo) utilizzata nella generalità dei casi dalle amministrazioni per l'utilizzo di quasi tutte le risorse ICT (postazioni di lavoro, connessioni di rete e posta elettronica).

In considerazione della delicatezza della materia, che tocca i diritti individuali (quale il diritto alla segretezza della corrispondenza) e richiede, pertanto, un giusto bilanciamento con il potere di controllo dell'amministrazione, si ritiene opportuno fornire indicazioni utili a facilitare, da un lato, il corretto utilizzo degli strumenti ICT da parte dei dipendenti e, dall'altro, il proporzionato esercizio del potere datori di controllo da parte delle amministrazioni in indirizzo.

1. Esercizio del potere di controllo e doveri di comportamento dei dipendenti delle pubbliche amministrazioni

Le pubbliche amministrazioni, in quanto datori di lavoro, sono tenute ad assicurare la funzionalità ed il corretto impiego degli strumenti ICT da parte dei propri dipendenti, definendo le modalità di utilizzo nell'organizzazione dell'attività lavorativa ed adottando le misure necessarie a garantire la sicurezza, la disponibilità e l'integrità dei sistemi informativi.

Nell'esercizio del potere di controllo, le amministrazioni devono attenersi ad alcune regole e principi generali:
• innanzitutto deve essere rispettato il principio di proporzionalità, che si concreta nella pertinenza e non eccedenza delle attività di controllo. Le limitazioni della libertà e dei diritti individuali devono, infatti, essere proporzionate allo scopo perseguito; è in ogni caso esclusa l'ammissibilità di controlli prolungati, costanti e indiscriminati;
• inoltre, l'introduzione di tecnologie e di strumenti per il controllo sull'uso della rete e della posta elettronica deve essere fatto rispettando le procedure di informazione/consultazione delle rappresentanze dei lavoratori previste dai contratti collettivi;
• infine, i lavoratori devono essere preventivamente informati dell'esistenza di dispositivi di controllo atti a raccogliere i dati personali.

A fronte del potere di controllo dell'amministrazione datore di lavoro, esiste in capo ai dipendenti l'obbligo, sancito da norme di legge (anche di rilevanza penale) e di contratto, di adottare comportamenti conformi al corretto espletamento della prestazione lavorativa ed idonei a non causare danni o pericoli ai beni mobili ed agli strumenti ad essi affidati, tra i quali vi sono le attrezzature ICT ed i sistemi informativi messi a disposizione dall'amministrazione.

Al riguardo, si ritiene opportuno ricordare, oltre alle disposizioni del Codice disciplinare contenuto nei contratti collettivi di comparto (che dispongono sanzioni in caso di "negligenza nella cura dei locali e dei beni mobili o strumenti a lui affidati o sui quali, in relazione alle sue responsabilità, debba espletare azione di vigilanza"), anche il dettato del Codice di comportamento dei dipendenti delle pubbliche amministrazioni di cui al decreto del Ministro per la funzione pubblica del 28 novembre 2000 che, ove richiamato dal Codice disciplinare dei CCNL dei diversi comparti, costituisce, oltre che norma di valenza etico-comportamentale, anche vero e proprio obbligo la cui inosservanza da parte dei dipendenti è passibile di sanzione.

In particolare, l'art.10, comma 3, del Codice di comportamento dispone che "Il dipendente non utilizza a fini privati materiale o attrezzature di cui dispone per ragioni di ufficio". Pertanto,
l'utilizzo delle risorse ICT da parte dei dipendenti, oltre a non dover compromettere la sicurezza e la riservatezza del sistema informativo, non deve pregiudicare ed ostacolare le attività dell'amministrazione od essere destinato al perseguimento di interessi privati in contrasto con quelli pubblici.

Anche la giurisprudenza, in particolare quella della Corte dei conti (tra le altre, sez. giurisd. Piemonte, sent. 1856/2003, e sez. giurisd. Basilicata, sent. n.83/2006), ha sanzionato l'indebito utilizzo della connessione ad Internet da parte di un dipendente, statuendo che essa configura profili di responsabilità a carico del medesimo per il danno patrimoniale cagionato all'amministrazione, consistente nel mancato svolgimento della prestazione lavorativa durante le ore di connessione. Con riferimento al potere di controllo, la Corte ha, inoltre, osservato come, a seguito di ripetute e significative anomalie (rilevate, ad esempio, per la presenza di virus provenienti da siti non istituzionali), l'amministrazione possa svolgere verifiche ex post sui dati inerenti l'accesso alla rete dei propri dipendenti.

Per adempiere il proprio dovere di diligenza e vigilanza nell'utilizzo dei beni e strumenti ad esso affidati, il dipendente ha, pertanto, anche l'obbligo di impedire ad altri indetti utilizzazioni della propria apparecchiatura informatica, non rilevando, al fine del difetto di responsabilità, il fatto che altri, in sua assenza, abbia potuto usare la postazione lavorativa. In difetto, il comportamento del dipendente si configura come negligente, inescusabile e gravemente colposo.

2. I principi contenuti nelle linee guida del Garante della protezione dei dati personali

Con deliberazione del 1° marzo 2007, n.13 [...], il Garante della protezione dei dati personali ha fornito le linee guida per l'utilizzo nei luoghi di lavoro della posta elettronica e di Internet.

Allo stato, lasciando da parte i profili di illecito penale e/o disciplinare sopra richiamati, tale deliberazione costituisce, in particolare per quanto attiene alla disciplina del trattamento dei dati, sicuro punto di riferimento e regolamentazione delle modalità di utilizzo del Sistema informativo delle pubbliche amministrazioni da parte dei dipendenti nell'ambito del rapporto di lavoro.

La deliberazione, nel definire, per i datori di lavoro, le regole in materia di trattamento dei dati personali raccolti in occasione delle attività di verifica del corretto utilizzo della rete Internet e del sistema di posta elettronica da parte dei lavoratori, fissa dei principi che non riguardano esclusivamente la tutela della privacy ma riprendono anche le disposizioni contenute nel "Codice dell'amministrazione digitale" (d.lgs. 7 marzo 2005, n.82 [...], aggiornato dal d.lgs. n.159 del 4 aprile 2006, [...], recante "Disposizioni integrative e correttive al d.lgs. 7 marzo 2005, n.82 recante Codice dell'amministrazione digitale").

In particolare, come definito anche dalle linee guida del Garante, il datore di lavoro (secondo i poteri a lui affidati dalle norme del codice civile, artt.2086, 2087 e 2104), può riservarsi di controllare l'effettivo adempimento della prestazione lavorativa ed il corretto utilizzo degli strumenti di lavoro. Nell'esercizio di tali prerogative, tuttavia, deve rispettare la libertà e la dignità dei lavoratori, tenendo presente, al riguardo, quanto disposto dalle norme poste a tutela del lavoratore (ci si riferisce, in particolare, al divieto di installare "apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori" di cui all'art.4 della legge 300/1970). Inoltre, secondo i richiamati principi di pertinenza e non eccedenza, i mezzi e l'ampiezza del controllo devono essere proporzionati allo scopo: in base a tale considerazione il datore di lavoro potrebbe, ad esempio, verificare se vi è stato indebito utilizzo della connessione ad Internet da parte del dipendente attraverso il controllo degli accessi e dei tempi di connessione, senza però indagare sul contenuto dei siti visitati.

I lavoratori devono essere posti in grado di conoscere quali sono le attività consentite, a quali controlli sono sottoposti, le modalità del trattamento dei dati e in quali sanzioni possono incorrere nel caso di abusi. Al riguardo, viene raccomandata l'adozione di un disciplinare interno adeguatamente pubblicizzato e di idonee misure di tipo organizzativo.

3. Utilizzo della rete Internet

In capo all'amministrazione datore di lavoro, alla cui proprietà è riconducibile il Sistema informativo (ivi inclusi le apparecchiature, i programmi ed i dati inviati, ricevuti e salvati), è posto l'obbligo di predisporre misure per ridurre il rischio di usi impropri di Internet, consistenti in attività non correlate alla prestazione lavorativa, quali la visione di siti non pertinenti, l'"upload e il download di file, l'uso di servizi di rete con finalità ludiche o comunque estranee all'attività lavorativa.

A tale proposito, si raccomanda alle amministrazioni di dotarsi di software idonei ad impedire l'accesso a siti Internet aventi contenuti e/o finalità vietati dalla legge. Inoltre, l'amministrazione, tenendo conto delle peculiarità proprie di ciascuna organizzazione produttiva ed, eventualmente,
anche dei diversi profili professionali autorizzati all'uso della rete, potrà adottare una o più delle misure indicate dalla citata deliberazione del Garante della privacy che, a mero titolo riepilogativo, si riportano di seguito:

- individuazione di categorie di siti considerati correlati o meno con la prestazione lavorativa;
- configurazione di sistemi o utilizzo di filtri che prevengano determinate operazioni – reputate inconferenti con l'attività lavorativa - quali l'upload o l'accesso a determinati siti ( inseriti in una sorta di blacklist) e/o il download di files o software aventi particolari caratteristiche (dimensionali o di tipologia di dato);
- trattamento di dati in forma anonima o tale da precludere l'immedia identificazione di utenti mediante loro opportune aggregazioni (ad es., con riguardo ai file di log riferiti al traffico web, su base collettiva o per gruppi sufficientemente ampi di lavoratori);
- eventuale conservazione nel tempo dei dati strettamente limitata al perseguimento di finalità organizzative, produttive e di sicurezza.

Tuttavia, l'utilizzo di Internet per svolgere attività che non rientrano tra i compiti istituzionali potrebbe essere regolamentato e, quindi, consentito ai dipendenti per assolvere incombenze amministrative e burocratiche senza allontanarsi dal luogo di lavoro (ad esempio, per effettuare adempimenti on-line nei confronti di pubbliche amministrazioni e di concessionari di servizi pubblici, ovvero per tenere rapporti con istituti bancari e assicurativi). Tale modalità, purché contenuta nei tempi strettamente necessari allo svolgimento delle transazioni, avrebbe, inoltre, il vantaggio di contribuire a ridurre gli spostamenti delle persone e gli oneri logistici e di personale per l'amministrazione che eroga il servizio, favorendo, altresì, la dematerializzazione dei processi produttivi.

4. Utilizzo della posta elettronica istituzionale

Con riferimento all'utilizzo della casella di posta elettronica istituzionale deve osservarsi che il contenuto dei messaggi, come pure i file allegati e i dati esteriori delle comunicazioni, riguardano forme di corrispondenza assistite da garanzie di segretezza tutelate anche costituzionalmente, la cui ratio risiede nel proteggere il nucleo essenziale della dignità umana e il pieno sviluppo della personalità nelle formazioni sociali (qual è anche il luogo di lavoro); un'ulteriore protezione deriva dalle norme penali a tutela dell'inviolabilità dei segreti (artt.2 e 15 Cost.; Corte cost. 17 luglio 1998, n.281 e 11 marzo 1993, n.81; art.616, comma 4, c.p., art.49, Codice dell'amministrazione digitale).

Al fine di contemperare le esigenze di corretto ed ordinato svolgimento della vita lavorativa e di prevenzione di inutili intrusioni nella sfera personale dei lavoratori e di violazioni della segretezza della corrispondenza, sarebbe, pertanto, opportuno che le amministrazioni esplicitassero regole e strumenti per l'utilizzo della posta elettronica.

Ciò consentirebbe, infatti, di evitare, ovvero almeno limitare, l'insorgere di difficoltà in ordine all'utilizzo della posta elettronica poiché, per la configurazione stessa dell'indirizzo e-mail, nei singoli casi, può risultare dubbio se il lavoratore, in qualità di destinatario o mittente, utilizzi la posta operando quale espressione dell'amministrazione o ne faccia, invece, un uso personale pur restando nell'ambito lavorativo istituzionale.

Si invitano, pertanto, le amministrazioni in indirizzo, attraverso i dirigenti responsabili, ad attuare tutte le misure di informazione, controllo e verifica consentite al fine regolamentare la fruizione delle risorse ICT e responsabilizzare i dipendenti nei confronti di eventuali utilizzi non coerenti con la prestazione lavorativa e non conformi alle norme che disciplinano il lavoro alle dipendenze delle pubbliche amministrazioni.

*****

DISCUSSIONE

1. Nel caso di pubblici dipendenti, quali ulteriori interessi sono presenti?
2. Ritenete che la direttiva in esame abbia tenuto conto in maniera razionale e corretta di tali interessi? Ci sono punti che non ritenete convincenti?
3. Quali sono gli elementi di novità rispetto al provvedimento generale del Garante?